Documenta Mathematica

Journal der
Deutschen Mathematiker-Vereinigung
Gegründet 1996
Extra Volume

A Collection of Manuscripts Written in Honour of John H. Coates on the Occasion of His Sixtieth Birthday

Editors:
I. Fesenko, S. Lichtenbaum,
B. Perrin-Riou, P. Schneider

DOCUMENTA MATHEMATICA, Journal der Deutschen Mathematiker-Vereinigung, veröffentlicht Forschungsarbeiten aus allen mathematischen Gebieten und wird in traditioneller Weise referiert. Es wird indiziert durch Mathematical Reviews, Science Citation Index Expanded, Zentralblatt für Mathematik.

Artikel können als TEX-Dateien per E-Mail bei einem der Herausgeber eingereicht werden. Hinweise für die Vorbereitung der Artikel können unter der unten angegebenen WWW-Adresse gefunden werden.

DOCUMENTA MATHEMATICA, Journal der Deutschen Mathematiker-Vereinigung, publishes research manuscripts out of all mathematical fields and is refereed in the traditional manner. It is indexed in Mathematical Reviews, Science Citation Index Expanded, Zentralblatt für Mathematik.

Manuscripts should be submitted as TEX -files by e-mail to one of the editors. Hints for manuscript preparation can be found under the following WWW-address.

`http://www.math.uni-bielefeld.de/documenta`

ISBN 978-3-936609-28-8, ISSN 1431-0635 (Print), ISSN 1431-0643 (Internet)

DOCUMENTA MATHEMATICA is a Leading Edge Partner of SPARC, the Scholarly Publishing and Academic Resource Coalition of the Association of Research Libraries (ARL), Washington DC, USA.

Address of Technical Managing Editor: Ulf Rehmann, Fakultät für Mathematik, Universität Bielefeld, Postfach 100131, D-33501 Bielefeld, Copyright © 2003 for Layout: Ulf Rehmann. Typesetting in TEX.

Documenta Mathematica

Extra Volume: John H. Coates' Sixtieth Birthday, 2006

Preface

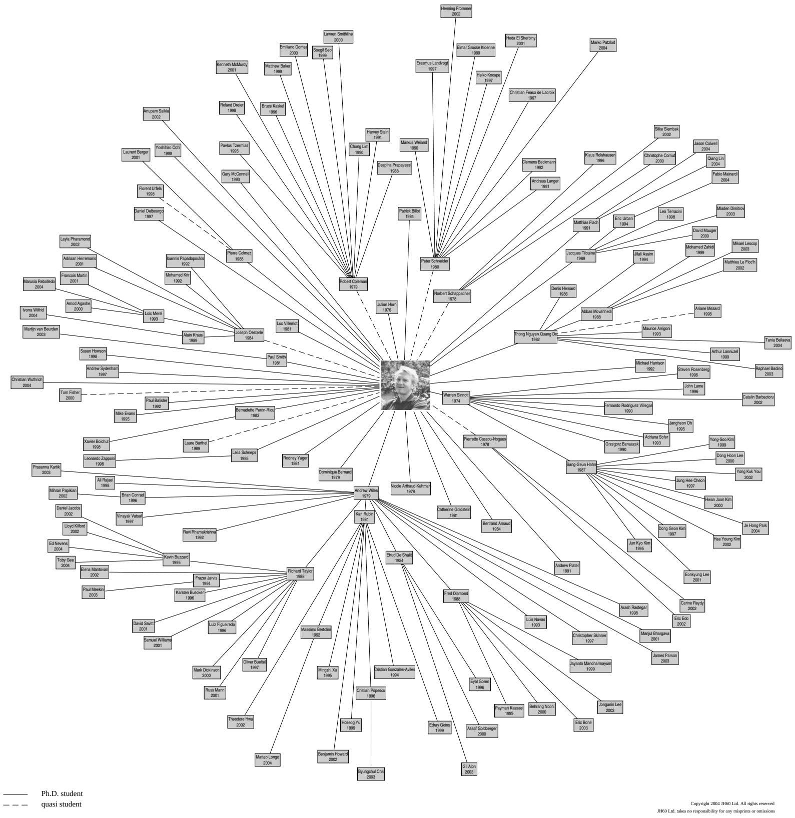
This volume is dedicated to Professor John Coates, an outstanding collaborator, colleague, author, teacher, and friend. He has greatly contributed to number theory, both through his fundamental mathematical works and through his impressive mathematical school. He is a continuous source of tremendous inspiration to students and colleagues. John Coates has been one of the leading proponents of and contributors to Iwasawa theory and he is the founding father of its recent development in the form of non-commutative Iwasawa theory.
We included in the volume the Japanese tanka ”Samegai’s Waters” which was selected by John upon our request.
Prior to the Cambridge conference

http://www.maths.nott.ac.uk/personal/ibf/jhc.html

to mark the 60th birthday of John Coates, Sarah Zerbes and Vladimir Dokchitser had produced a diagramme of his mathematical family tree which is included in the volume (next page).

I. Fesenko, S. Lichtenbaum, B. Perrin-Riou, P. Schneider

Oh, what a tangled web we weave...



We would like to thank

Andrew Aitchison for technical support,
Julie Coates for providing the pictures,

and also Jilali Assim, Matthew Baker, Grzegorz Banaszak, Laure Barthel, Massimo Bertolini, Karsten Buecker, Oliver Bueltel, Kevin Buzzard, Pierrette Cassou-Nogues, Jung-Hee Cheon, Robert Coleman, Pierre Colmez, Brian Conrad, Christophe Cornut, Daniel Delbourgo, Ehud de Shalit, Fred Diamond, Mike Evans, Ivan Fesenko, Matthias Flach, Edray Goins, Catherine Goldstein, Eyal Goren, Sang-Geun Hahn, Michael Harrison, Susan Howson, Frazer Jarvis, Bruce Kaskel, Payman Kassaei, Alain Kraus, Andreas Langer, Gary McConnell, Loic Merel, Ariane Mezard, Abbas Movahhedi, Thong Nguyen Quang Do, Yoshihiro Ochi, Joseph Oesterle, Bernadette Perrin-Riou, Andrew Plater, Arash Rastegar, Karl Rubin, Anupam Saikia, Norbert Schappacher, Peter Schneider, Leila Schneps, Tony Scholl, Sir Walter Scott, Warren Sinnott, Christopher Skinner, Paul Smith, Vic Snaith, Harvey Stein, Richard Taylor, Jacques Tilouine, Pavlos Tzermias, Vinayak Vatsal, Andrew Wiles and Rodney Yager.

Tim Dokchitser
Vladimir Dokchitser
Sarah Livia Zerbes

The John Coates mathematical family tree is reproduced here with the kind permission of its authors.

Foreword

Andrew Wiles

I first met John Coates during my first year as a graduate student at Cambridge. John was about to move back to Cambridge where he had been a graduate student himself. It was at a point in his career when he was starting a whirlwind of moves. Coming from Stanford he spent two years in Cambridge, and one in Australia before making a longer stop in Paris at Orsay. Mathematically however he was just settling down to what has become his most serious and dedicated study of the last thirty years, the arithmetic of elliptic curves. Needless to say for those who have devoted some time to this subject, it is so full of fascinating problems that it is hard to turn from this to anything else. The conjecture of Birch and Swinnerton-Dyer, by then fifteen years old, had made the old subject irresistible.

In the two years he was at Cambridge we wrote four papers on elliptic curves, culminating in the proof of a part of the conjecture for elliptic curves with complex multiplication which are defined over the rationals. When John had been at Cambridge previously as a graduate student of Alan Baker he had worked on questions about the bounding of integral points on curves. Siegel's proof of the finiteness of the number of integral points on curves of genus at least one was not effective. Work of John's, in collaboration with Baker, had given the first proof of an effective bound on the size of the integral solutions of a genus one curve. During his time in the U.S. John had been much influenced by the work of Tate and of Iwasawa. The key insight of Iwasawa had been to see how to translate the theorems of Weil, which related the characteristic polynomial of Frobenius in certain l-adic representations to the zeta function, from the function field case to the number field case. Of course this involved the p-adic zeta function and not the classical one and even then only became a translation from a theorem to a conjecture, but it became a guiding principle in the study of the special values of the zeta function and has remained so to this day. Tate had been studying the relation of K_2 of the ring of integers of a number field to Galois cohomology groups. Together with Lichtenbaum and Sinnott John had developed and examined these conjectures about K-groups using some of the ideas of Iwasawa.

When he returned to Cambridge John and I set about exploring how Iwasawa's approach would work in the case of elliptic curves with complex multiplication. It worked wonderfully well! Although at that time Iwasawa's main conjecture seemed quite out of reach, even in the basic cyclotomic case, one could develop enough using the methods of Iwasawa to get the first real theorems on the Birch and Swinnerton-Dyer conjecture. Of course the search for a solution to this conjecture remains elusive to this day but the progress has been enormous. The theory of complex multiplication has to a large extent ceded its place to the theory of modular forms but the basic idea has largely remained intact, namely to relate the special values of L-functions to the points on the elliptic curve via the class field theory of the division fields of those points.

The original work was all in the context of ordinary primes, these being primes where the reduction of the elliptic curve is ordinary. Subsequently John and his students have extended the study to try to understand first the supersingular case, but still assuming the curve has complex multiplication, and then the more general case where no complex multiplication is assumed. Meanwhile the new ideas of Kolyvagin and of Gross and Zagier have to a large extent brought the general case into line with the complex multiplication case. In the general case where the curves are not assumed to have complex multiplication the fields of division points are no longer abelian over a finite extension of the rationals. To study these fields John and his coauthors have developed a non-abelian version of Iwasawa theory.

This volume contains many papers on these and related topics. However no tribute to John Coates could be complete without a testament to his continuing generosity and skill as a teacher. Cambridge number theory seemed strongest in bringing out the problem solver but one had a sense that in terms of modern developments it was a little isolated. John's arrival brought these two worlds together, and made Cambridge and my own arrival in mathematics more exciting than I could ever have anticipated. John's return to Cambridge in 1986 has cemented his role as a teacher and inspiration to many more generations of Cambridge number theorists, many of whom were present at his 60th birthday celebrations in January of 2005.

結ぶ手ににごる心をすすぎなば浮世の夢やさめが井の水

（阿仏尼『十六夜日記』）

Samegai's Waters

Samegai's waters:
Were I to cup them in my hands
And cleanse my impure heart,
Might I awaken from the dream
Of this transitory world?

musubu te ni
nigoru kokoro wo
susuginaba
ukiyo no yume ya
samegai no mizu.

Alphabetic transcription

Ring-Theoretic Properties of Iwasawa Algebras: A Survey[1]

K. Ardakov and K. A. Brown

Received: November 7, 2005
Revised: January 22, 2006

Abstract. This is a survey of the known properties of Iwasawa algebras, i.e., completed group rings of compact p-adic analytic groups with coefficients the ring $\mathbb{Z}_p$ of p-adic integers or the field $\mathbb{F}_p$ of p elements. A number of open questions are also stated.

2000 Mathematics Subject Classification: 16L30, 16P40, 20C07, 11R23
Keywords and Phrases: Iwasawa algebra; compact p-adic analytic group; complete noetherian semilocal ring; Auslander-Gorenstein condition

1. Introduction

Noncommutative Iwasawa algebras form a large and interesting class of complete semilocal noetherian algebras, constructed as completed group algebras of compact p-adic analytic groups. They were defined and their fundamental properties were derived in M. Lazard's monumental 1965 paper [23], but in the twenty years from 1970 they were little studied. Interest in them has been revived by developments in number theory over the past fifteen years, see for example [17],[19] and [37]. Prompted by this renewed interest, and helped of course by the better understanding of noncommutative noetherian algebra gained since 1965, a number of recent papers have built on Lazard's initial work. The emerging picture is of a class of rings which in some ways look similar to the classical commutative Iwasawa algebras, (which are rings of formal power series in finitely many commuting variables over the p-adic integers), but which in other respects are very different from their commutative counterparts. And while some progress has been made in understanding these rings, many aspects of their structure and representation theory remain mysterious.

It is the purpose of this article to provide a report of what is known about Iwasawa algebras at the present time, and to make some tentative suggestions for

[1] Some of the work for this article was done in June 2005, when Ardakov was visiting the University of Glasgow with the support of the Edinburgh Mathematical Society Research Support Fund and the Glasgow Mathematical Journal Learning and Research Support Fund.

future research directions. We approach the latter objective through the listing of a series of open questions, scattered throughout the text. In an attempt to make the paper accessible to readers from as wide a range of backgrounds as possible, we have tried to give fairly complete definitions of all terminology; on the other hand, most proofs are omitted, although we have tried to give some short indication of their key points where possible. An exception to the omission of proofs occurs in the discussion of maximal orders in (4.4)-(4.7) as well as in the discussion of the canonical dimension in (5.4), where we include some original material. These paragraphs can be omitted by a reader who simply wants a quick overview of the subject; moreover, after Sections 2 and 3 the remaining sections are reasonably independent of each other.

Fundamental definitions and examples are given in Section 2; in particular we recall the definition of a *uniform* pro-p group in (2.4), and make the important observation (2.3)(1) that every Iwasawa algebra can be viewed as a crossed product of the Iwasawa algebra of a uniform group by a finite group. This has the effect of focusing attention on the Iwasawa algebra of a uniform group - this is filtered by the powers of its Jacobson radical, and the associated graded algebra is a (commutative) polynomial algebra. This fact and its consequences for the structure of the Iwasawa algebras of uniform groups are explored in Section 3; then in Section 4 we examine how properties of general Iwasawa algebras can be deduced from the uniform case using (2.3)(1). Section 5 concerns dimensions: first, the global (projective) dimension and the injective dimension, whose importance is enhanced because Iwasawa algebras satisfy the *Auslander-Gorenstein condition*, whose definition and properties we recall. In particular, Auslander-Gorenstein rings possess a so-called *canonical dimension function*; we explain this and describe some of the properties of the canonical dimension of an Iwasawa algebra in (5.3)-(5.5). The Krull-Gabriel-Rentschler dimension is discussed in (5.7). Finally, our very sparse knowledge of the two-sided ideals of Iwasawa algebras is summarised in Section 6.

2. Key definitions

Iwasawa algebras are completed group algebras. We begin by recalling which groups are involved, then give the definition of the algebras.

2.1. Compact p-adic analytic groups. Let p be a prime integer and let $\mathbb{Z}_p$ denote the ring of p-adic integers. A group G is *compact p-adic analytic* if it is a topological group which has the structure of a p-adic analytic manifold - that is, it has an atlas of open subsets of $\mathbb{Z}_p^n$, for some $n \geq 0$. Such groups can be characterised in a more intrinsic way, thanks to theorems due to Lazard, dating from his seminal 1965 paper [23]. Namely, a topological group G is compact p-adic analytic if and only if G is profinite, with an open subgroup which is pro-p of finite rank, if and only if G is a closed subgroup of $GL_d(\mathbb{Z}_p)$ for some $d \geq 1$. Nowadays, these equivalences are usually viewed as being consequences of deep properties of finite p-groups; a detailed account from this perspective can be found in [20, Part II].

Examples: (1) Every finite group is p-adic analytic, for every prime p.
(2) The abelian p-adic analytic groups are the direct products of finitely many copies of the additive group of $\mathbb{Z}_p$ with a finite abelian group [20, page 36].
(3) For any positive integer d the groups $GL_d(\mathbb{Z}_p)$ and $SL_d(\mathbb{Z}_p)$ are compact p-adic analytic. More generally, given any root system X_ℓ one can form the *universal Chevalley group* $\mathcal{G}_{\mathbb{Z}_p}(X_\ell)$, [20, page 353]. This is a compact p-adic analytic group. For more information about Chevalley groups, see [13].
(4) Let d and t be positive integers. The *t-th congruence subgroup in $SL_d(\mathbb{Z}_p)$* is the kernel $\Gamma_t(SL_d(\mathbb{Z}_p))$ of the canonical epimorphism from $SL_d(\mathbb{Z}_p)$ to $SL_d(\mathbb{Z}_p/p^t\mathbb{Z}_p)$. One sees at once from the equivalences above that $\Gamma_t(SL_d(\mathbb{Z}_p))$ is compact p-adic analytic, as indeed are $\Gamma_t(GL_d(\mathbb{Z}_p))$ and $\Gamma_t(\mathcal{G}_{\mathbb{Z}_p}(X_\ell))$ for any root system X_ℓ.

Notation: When discussing a topological group G we shall use $\overline{H}$ to denote the closure of a subset H of G in G; and when we refer to, say, G as being *generated by* elements $\{g_1, \dots, g_d\}$ we mean that $G = \overline{\langle g_1, \dots, g_d \rangle}$. In particular, G is *finitely generated* if $G = \overline{\langle X \rangle}$ for a finite subset X of G. For a subset X of G, X^p denotes the subgroup of G generated by the subset $\{x^p : x \in X\}$ of G.

2.2. Iwasawa algebras. Let G be a compact p-adic analytic group. The *Iwasawa algebra of* G is

$$\Lambda_G \quad := \quad \varprojlim \mathbb{Z}_p[G/N],$$

where the inverse limit is taken over the open normal subgroups N of G. Closely related to Λ_G is its epimorphic image Ω_G, defined as

$$\Omega_G \quad := \quad \varprojlim \mathbb{F}_p[G/N],$$

where $\mathbb{F}_p$ is the field of p elements. Often, a property of Λ_G can easily be deduced from the corresponding property of Ω_G, and vice versa; where this is routine we will frequently save space by stating only one of the two variants.

2.3. Crossed products. Recall [29, 1.5.8] that a *crossed product* of a ring R by a group A is an associative ring $R * A$ which contains R as a subring and contains a set of units $\overline{A} = \{\overline{a} : a \in A\}$, isomorphic as a set to A, such that

- $R * A$ is a free right R-module with basis $\overline{A}$,
- for all $x, y \in A$, $\overline{x}R = R\overline{x}$ and $\overline{x} \cdot \overline{y}R = \overline{xy}R$.

Suppose that H is an open normal subgroup of the compact p-adic analytic group G. Let $\mathcal{C}_H$ denote the set of open normal subgroups of G which are contained in H; then clearly $\Lambda_G = \varprojlim \mathbb{Z}_p[G/U]$ where U runs over $\mathcal{C}_H$. It follows at once that Λ_G is a crossed product of Λ_H by the finite group G/H and similarly that Ω_G is a crossed product of Ω_H by G/H:

$$(1) \qquad \begin{array}{lcl} \Lambda_G & \cong & \Lambda_H * (G/H), \\ \Omega_G & \cong & \Omega_H * (G/H). \end{array}$$

We shall see that, combined with a judicious choice of the subgroup H, the isomorphism (1) reduces many questions about Λ_G and Ω_G to the analysis of certain crossed products of finite groups. Usually, the right subgroup H to choose is a *uniform* one, defined as follows.

2.4. Uniform groups. Let G be a pro-p group. Define $P_1(G) = G$ and $P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}$ for $i \geq 1$. The decreasing chain of characteristic subgroups

$$G = P_1(G) \supseteq P_2(G) \supseteq \cdots \supseteq P_i(G) \supseteq \cdots \supseteq \cap_{i=1}^{\infty} P_i(G) = 1$$

is called the *lower p-series* of G. The group G is *powerful* if $G/\overline{G^p}$ is abelian (for p odd), or $G/\overline{G^4}$ is abelian (when $p = 2$). Finally, G is *uniform* if it is powerful, finitely generated, and

$$|G : P_2(G)| = |P_i(G) : P_{i+1}(G)|$$

for all $i \geq 1$.
Now we can add one further characterisation, also essentially due to Lazard, to those given in (2.1): a topological group G is compact p-adic analytic if and only if it has an open normal uniform pro-p subgroup of finite index, [20, Corollary 8.34].

Examples: (1) Of course, $(\mathbb{Z}_p)^{\oplus d}$ is uniform for all $d \geq 1$.
(2)The groups $\Gamma_1(GL_d(\mathbb{Z}_p))$ (for p odd) and $\Gamma_2(GL_d(\mathbb{Z}_2))$ are uniform [20, Theorem 5.2].

Let G be uniform, with $|G : P_2(G)| = p^d$. The non-negative integer d is called the *dimension* of G; it is equal to the cardinality of a minimal set of (topological) generators of G, [20, Definition 4.7 and Theorem 3.6]. More generally, we can define the dimension of an arbitrary compact p-adic analytic group to be the dimension of any open uniform subgroup; this is unambiguous [20, Lemma 4.6], and coincides with the dimension of G as a p-adic analytic manifold, [20, Definition 8.6 and Theorem 8.36].

2.5. Completed group algebras. In fact Λ_G and Ω_G are I-adic completions of the ordinary group algebras $\mathbb{Z}_p[G]$ and $\mathbb{F}_p[G]$, for suitable choices of ideals I. It is most convenient for us to state the result for uniform groups, although it can obviously be extended to the general case using (2.3)(1).

Theorem. *Let G be a uniform pro-p group, and let I denote the augmentation ideal of $\mathbb{F}_p[G]$. Then Ω_G is isomorphic to the I-adic completion of $\mathbb{F}_p[G]$. There is a similar result for $\mathbb{Z}_p[G]$.*

Indeed the theorem follows quite easily from the observations that the lower p-series $P_i(G)$ is coterminal with the family of all open normal subgroups of G, and that the powers of I are coterminal with the ideals of $\mathbb{F}_p[G]$ generated by the augmentation ideals of the subgroups $P_i(G)$, [20, §7.1].

3. The case when G is uniform

Throughout this section, we assume that G is a uniform pro-p group of dimension d. We fix a topological generating set $\{a_1, \ldots, a_d\}$ for G.

3.1. The "PBW" Theorem. It follows at once from Theorem 2.5 that the usual group algebra $\mathbb{F}_p[G]$ embeds into Ω_G. For $i = 1, \dots, d$, let $b_i = a_i - 1 \in \mathbb{F}_p[G] \subseteq \Omega_G$. Then we can form various monomials in the b_i: if $\alpha = (\alpha_1, \dots, \alpha_d)$ is a d-tuple of nonnegative integers, we define

$$\mathbf{b}^\alpha = b_1^{\alpha_1} \cdots b_d^{\alpha_d} \in \Omega_G.$$

Note that this depends on our choice of ordering of the b_i's, because Ω_G is noncommutative unless G is abelian. The following basic result shows that Ω_G is a "noncommutative formal power series ring"; it follows from the strong constraints which the hypothesis of uniformity imposes on the quotients $P_i(G)/P_{i+1}(G)$ of G, [20, Theorem 7.23].

Theorem. *Every element c of Ω_G is equal to the sum of a uniquely determined convergent series*

$$c = \sum_{\alpha \in \mathbb{N}^d} c_\alpha \mathbf{b}^\alpha$$

where $c_\alpha \in \mathbb{F}_p$ for all $\alpha \in \mathbb{N}^d$.

We record an immediate consequence of both this result and of Theorem 2.5:

Corollary. *The Jacobson radical J of Ω_G is equal to*

$$J = b_1\Omega_G + \cdots + b_d\Omega_G = \Omega_G b_1 + \cdots + \Omega_G b_d.$$

Hence $\Omega_G/J \cong \mathbb{F}_p$, so in the language of (4.1), Ω_G is a scalar local ring.

Proof. If $c \in \Omega_G$ is such that $c_0 \neq 0$, then $1 - c$ is invertible with inverse $1 + c + c^2 + \cdots \in \Omega_G$. □

Theorem 3.1 says that the monomials $\{\mathbf{b}^\alpha : \alpha \in \mathbb{N}^d\}$ form a topological basis for Ω_G, and is thus analogous to the classical Poincaré-Birkhoff-Witt theorem for Lie algebras $\mathfrak{g}$ over a field k which gives a vector space basis for the universal enveloping algebra $\mathcal{U}(\mathfrak{g})$ in terms of monomials in a fixed basis for $\mathfrak{g}$ [21]. Nevertheless we should bear in mind that explicit computations in Ω_G are often much more difficult than those in $\mathcal{U}(\mathfrak{g})$, since the Lie bracket of two generators b_i, b_j for Ω_G is in general an infinite power series with obscure coefficients.

3.2. Example. Let p be odd for simplicity and let $G = \Gamma_1(SL_2(\mathbb{Z}_p))$ be the first congruence kernel of $SL_2(\mathbb{Z}_p)$. Then

$$a_1 = \begin{pmatrix} \exp(p) & 0 \\ 0 & \exp(-p) \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}.$$

is a topological generating set for G. Setting $b_i = a_i - 1$, elementary (but tedious) computations yield

$$\begin{array}{lcll} [b_1, b_2] & \equiv & 2b_2^p & \mod J^{p+1} \\ [b_1, b_3] & \equiv & -2b_3^p & \mod J^{p+1} \\ [b_2, b_3] & \equiv & b_1^p & \mod J^{p+1}. \end{array}$$

Here $J = b_1\Omega_G + b_2\Omega_G + b_3\Omega_G$ denotes the Jacobson radical of Ω_G. Using Proposition 3.3 it is possible to produce more terms in the power series expansion of $[b_1, b_2]$ and $[b_1, b_3]$. However, we consider $[b_2, b_3]$ to be inaccessible to computation.

3.3. Skew power series rings. It is well known that if $\mathfrak{g}$ is a finite dimensional soluble Lie algebra over a field k, then its universal enveloping algebra $\mathcal{U}(\mathfrak{g})$ can be thought of as an "iterated skew polynomial ring":

$$\mathcal{U}(\mathfrak{g}) \cong k[x_1; \sigma_1, \delta_1][x_2; \sigma_2, \delta_2] \cdots [x_n; \sigma_n, \delta_n]$$

for some appropriate automorphisms σ_i and derivations δ_i (in fact, the σ_is can be chosen to be trivial). This is because any such Lie algebra $\mathfrak{g}$ has a chain of subalgebras

$$0 = \mathfrak{h}_0 \subset \mathfrak{h}_1 \subset \mathfrak{h}_2 \subset \cdots \subset \mathfrak{h}_n = \mathfrak{g}$$

with $\mathfrak{h}_{i-1}$ an ideal in $\mathfrak{h}_i$, so choosing some $x_i \in \mathfrak{h}_i \backslash \mathfrak{h}_{i-1}$ ensures that

$$\mathcal{U}(\mathfrak{h}_i) \cong \mathcal{U}(\mathfrak{h}_{i-1})[x_i; \delta_i]$$

where δ_i is the derivation on $\mathcal{U}(\mathfrak{h}_{i-1})$ defined by $\delta_i(y) = x_i y - y x_i$.
An analogous result holds for Iwasawa algebras. More precisely, we have the

Proposition. *Suppose that G has closed normal subgroup H such that $G/H \cong \mathbb{Z}_p$. Then Ω_G is a skew power series ring with coefficients in Ω_H:*

$$\Omega_G \cong \Omega_H[[t; \sigma, \delta]].$$

Proof. See [41, §4]. □

Schneider and Venjakob [41] establish a general theory of skew power series rings $S = R[[t; \sigma, \delta]]$ over a pseudocompact ring R. Here σ can be any topological automorphism of R and δ is a σ-derivation in the sense of [29, 1.2.1], satisfying some extra conditions which are required to make the relation

$$ta = \sigma(a)t + \delta(a)$$

extend to a well-defined multiplication on S.
Consequently, the Iwasawa algebra Ω_G of any soluble uniform pro-p group G can be thought of as an iterated skew power series ring over $\mathbb{F}_p$.
For example, in Example 3.2, the topological subring of Ω_G generated by b_1 and b_2 is actually the Iwasawa algebra Ω_B where $B = \overline{\langle a_1, a_2 \rangle}$ is a Borel subgroup of G. Since B is soluble with closed normal subgroup $\overline{\langle a_2 \rangle}$, Ω_B is isomorphic to the skew power series ring $\mathbb{F}_p[[b_2]][[b_1; \sigma, \delta]]$ for some appropriate σ and δ. This justifies the claim that the commutator of b_1 and b_2 is at least partially accessible to computation.
There is surely considerable scope to develop further the "abstract" theory of skew power series algebras initiated in [41] - for instance, one could easily pose skew power series versions of a number of the questions we list later, in Section 6. As a prompt for more work, here are two "general" questions:

Question A. *(1) Are there conditions on R, σ and δ such that $S = R[[t;\sigma,\delta]]$ can be described without involving a derivation - that is, as $S = R'[[t';\sigma']]$, possibly after some Ore localisation?*[1]
(2) Are there conditions on R, σ and δ such that every two-sided ideal of the skew power series ring $S = R[[t;\sigma,\delta]]$ is generated by central elements and "polynomial" elements[2]*?*

3.4. The J-adic filtration. We remind the reader that a *filtration* on a ring R is an ascending sequence

$$\cdots \subseteq F_iR \subseteq F_{i+1}R \subseteq \cdots$$

of additive subgroups such that $1 \in F_0R$, $F_iR.F_jR \subseteq F_{i+j}R$ for all $i,j \in \mathbb{Z}$, and $\cup_{i\in\mathbb{Z}} F_iR = R$.
Let J denote the Jacobson radical of Ω_G. The J-adic filtration on Ω_G is defined as follows: $F_i\Omega_G = J^{-i}$ for $i \leq 0$ and $F_i\Omega_G = \Omega_G$ f or $i \geq 0$; this is an example of a *negative* filtration. The basic tool which allows one to deduce many ring-theoretic properties of Iwasawa algebras is the following result, which can be deduced from Theorem 3.1, see [20, Theorem 7.24 and remarks on page 160]. We denote the associated graded ring $\bigoplus_{i\in\mathbb{Z}} F_{i+1}\Omega_G/F_i\Omega_G$ by $\operatorname{gr}_J \Omega_G$.

Theorem. *The graded ring of Ω_G with respect to the J-adic filtration is isomorphic to a polynomial ring in $d = \dim G$ variables:*

$$\operatorname{gr}_J \Omega_G \cong \mathbb{F}_p[X_1, \ldots, X_d].$$

Moreover, Ω_G is complete with respect to this filtration.

The J-adic filtration is quite different from the filtrations encountered when studying algebras like universal enveloping algebras and Weyl algebras, which are nearly always *positive* (that is, $F_{-1}R = 0$) and often satisfy the finiteness condition $\dim_k F_iR < \infty$ for all $i \in \mathbb{Z}$. In particular, there is no well-behaved notion of the Gel'fand-Kirillov dimension for Iwasawa algebras, a theme we will return to in §5.
However, we are still able to lift many properties of the graded ring back to Ω_G, because the J-adic filtration is *complete*, meaning that Cauchy sequences of elements in Ω_G converge to unique limits. More precisely, recall [26, page 83] that a filtration on a ring R is said to be *Zariskian*, whenever

- The Jacobson radical of F_0R contains $F_{-1}R$, and
- The Rees ring $\widetilde{R} := \bigoplus_{i\in\mathbb{Z}} F_iR \cdot t^i \subseteq R[t,t^{-1}]$ is noetherian.

Many filtrations are Zariskian. For example, by [26, Chapter II, Proposition 2.2.1], any complete filtration whose associated graded ring is noetherian is necessarily Zariskian. Since any positive filtration is complete, it follows that if a filtration is positive and has noetherian associated graded ring, then it is Zariskian. More importantly for us, for any uniform pro-p group G, the J-adic filtration on Ω_G is clearly complete, thanks to Theorem 2.5; and $\operatorname{gr}_J \Omega_G$ is

[1] Compare with [14].

[2] By the latter, we mean elements of $R[t;\sigma,\delta]$.

noetherian by Theorem 3.4 and Hilbert's basis theorem, so the J-adic filtration is Zariskian.

3.5. The $\mathfrak{m}$-adic filtration on Λ_G. There is an analogue of Theorem 3.4 for the $\mathbb{Z}_p-$version of Iwasawa algebras Λ_G. Recall from (2.3) the lower p-series $P_1(G) \supseteq P_2(G) \supseteq \cdots \supseteq \cap_{i=1}^{\infty} P_i(G) = 1$ of G and define an abelian group

$$\operatorname{gr} G := \bigoplus_{i=1}^{\infty} \frac{P_i(G)}{P_{i+1}(G)}.$$

There is a natural way of turning $\operatorname{gr} G$ into a Lie algebra over $\mathbb{F}_p[t]$, the polynomial ring in one variable over $\mathbb{F}_p$: the Lie bracket on $\operatorname{gr} G$ is induced from the Lie bracket on G described in [20, §4.5], and the action of t is induced from the p-power map. Then $\operatorname{gr} G$ is a free $\mathbb{F}_p[t]$-module of rank equal to $\dim G$. Let $\mathfrak{m} = \ker(\Lambda_G \to \mathbb{F}_p)$ be the $\mathbb{F}_p$-augmentation ideal of Λ_G, or equivalently, the Jacobson radical of Λ_G.

Theorem. *The graded ring of Λ_G with respect to the $\mathfrak{m}$-adic filtration is isomorphic to the universal enveloping algebra of the $\mathbb{F}_p[t]$-Lie algebra $\operatorname{gr} G$:*

$$\operatorname{gr}_{\mathfrak{m}} \Lambda_G \cong \mathcal{U}(\operatorname{gr} G).$$

Moreover, Λ_G is complete with respect to this filtration.

Proof. See [39, §3.3] and [23, Chapter III, Theorem 2.3.3]. □

3.6. Lifting information from the graded ring. We recall here some standard properties of a ring R. First, we say that R is *prime* if the product of any two non-zero ideals of R is again non-zero. By Goldie's theorem [29, Theorem 2.3.6], if R is prime and (right) noetherian then it has a simple artinian classical (right) quotient ring $Q(R)$. If S is another ring with classical right quotient ring $Q(R)$, so that $Q(R) = Q(S)$, we say that R and S are *equivalent* if there are units a, b, c and d in $Q(R)$ such that $aRb \subseteq S$ and $cSd \subseteq R$. Now R is a *maximal (right) order* if it is maximal (with respect to inclusion) within its equivalence class, [29, 5.1.1]. (The adjective right is omitted if R is both a maximal right order and a maximal left order.) The commutative noetherian maximal orders are just the noetherian integrally closed domains [29, Lemma 5.3.3].

Let R_R denote the right R-module R. The *Krull dimension* $\mathcal{K}(M)$ of a finitely generated (right) module M over a noetherian ring R is a well-defined ordinal, bounded above by $\mathcal{K}(R_R)$; the precise definition can be found at [29, 6.2.2]. This concept generalises the classical commutative definition; like it, it measures the "size" of a module and is 0 if and only if the module is non-zero and artinian.

The *(right) global dimension* of R is defined to be the supremum of the projective dimensions (denoted $\operatorname{pd}(-)$) of the right R-modules, [29, 7.1.8]. When R is noetherian, its right and left global dimensions are always equal, [29, 7.1.11]. We say that R has *finite (right) injective dimension d* if there is an injective resolution of R_R of length d, but none shorter. If R is noetherian and has finite right and left injective dimensions, then these numbers are equal by [45, Lemma A]. It is also well known [39, Remark 6.4] that if the (right) global dimension of the noetherian ring R is finite, then it equals the (right) injective dimension of R.

It has become apparent over the past 40 years that, when R is noncommutative and noetherian, finiteness of the injective dimension of R is a much less stringent condition than is the case for commutative noetherian rings - the structure of (commutative) Gorenstein rings is rich and beautiful. An additional hypothesis which, when coupled with finite injective dimension, has proved very useful in the noncommutative world is the *Auslander-Gorenstein condition.* To recall the definition, note first that, for every left R-module M and every non-negative integer i, $\mathrm{Ext}^i(M,R)$ is a right R-module through the right action on R. The Auslander-Gorenstein condition on a noetherian ring R requires that, when M is a finitely generated left R-module, i is a non-negative integer and N is a finitely generated submodule of $\mathrm{Ext}^i(M,R)$, then $\mathrm{Ext}^j(N,R)$ is zero for all j strictly less than i; and similarly with "right" and "left" interchanged. We say that R is *Auslander-Gorenstein* if it is noetherian, has finite right and left injective dimensions, and satisfies the Auslander condition. Commutative noetherian rings of finite injective dimension are Auslander-Gorenstein. When R is noetherian of finite global dimension and satisfies the Auslander-Gorenstein condition it is called *Auslander-regular.*

Theorem. *Let R be a ring endowed with a Zariskian filtration FR; then R is necessarily noetherian. Also, R inherits the following properties from* $\mathrm{gr}\, R$*:*

(1) *being a domain,*
(2) *being prime,*
(3) *being a maximal order,*
(4) *being Auslander-Gorenstein,*
(5) *having finite global dimension,*
(6) *having finite Krull dimension.*

Proof. See [26]. □

We immediately obtain from Theorem 3.4, Theorem 3.6 and Corollary 3.1, the

Corollary. *If G is a uniform pro-p group, then Ω_G is a noetherian, Auslander-regular, scalar local domain which is a maximal order in its quotient division ring of fractions.*

4. Extensions over finite index

For an arbitrary p-adic analytic group G, many fundamental properties of Ω_G (and of Λ_G) can be analysed using Corollary 3.6 and (2.3)(1).

4.1. Complete noetherian (semi)local rings. Recall that a ring R is *semilocal* if the factor of R by its Jacobson radical $J(R)$ is semisimple artinian. It is *local* if $R/J(R)$ is simple artinian, and *scalar local* if $R/J(R)$ is a division ring. For a crossed product $R = S * H$ of a finite group H, like that in (2.3)(1), it's not hard to show that $J(S) \subseteq J(R)$, [31, Theorem 1.4.2]. From this, Theorem 2.5 and Corollary 3.6, and their analogues for Λ_G, we deduce (1) of the following. Both it and (2) were known to Lazard.

Theorem. *Let G be a compact p-adic analytic group.*

(1) Ω_G and Λ_G are complete noetherian semilocal rings.
(2) Ω_G and Λ_G are (scalar) local rings if and only if G is a pro-p group.

4.2. Primeness and semiprimeness. Recall that a ring R is *prime* if the product of two nonzero ideals is again nonzero and that R is *semiprime* if it has no nonzero nilpotent ideals. A prime ring is always semiprime, but not necessarily conversely.

The characterisations of these properties for Iwasawa algebras given in the theorem below exactly parallel the results for ordinary group algebras proved in the early 1960s by I.G. Connell and D.S. Passman [32, Theorems 4.2.10 and 4.2.14]. However, the proofs here are quite different from the classical setting; that the stated conditions are necessary is easy to see, but sufficiency in (1) and (2) depends on Corollary 3.6 to handle the uniform case, together with non-trivial results on crossed products of finite groups. Part (3) is much easier - one can simply appeal to the fact (a consequence of Maschke's theorem) that the group ring of a finite group over a commutative coefficient domain of characteristic zero is semiprime, together with the fact that, by definition, Λ_G is an inverse limit of such group rings.

Theorem. *Let G be a compact p-adic analytic group.*

(1) [5] *Ω_G and Λ_G are prime if and only if G has no non-trivial finite normal subgroups.*
(2) [5] *Ω_G is semiprime if and only if G has no non-trivial finite normal subgroups of order divisible by p.*
(3) (Neumann, [30]) *Λ_G is always semiprime.*

4.3. Zero divisors. There is a method, familiar from the treatment of ordinary group rings, which allows one to use homological properties to deduce results about the non-existence of zero divisors in certain noetherian rings. In its simplest form, which is all that is needed here, the statement is due to Walker [42]: *if R is a scalar local noetherian semiprime ring of finite global dimension, then R is a domain.*[3] This yields the following result; it was proved by Neumann [30] for Λ_G, but for Ω_G it was necessary to wait first for semiprimeness to be settled, as in Theorem 4.2(2).

Theorem. *Let G be a compact p-adic analytic group. Then Ω_G and Λ_G are domains if and only if G is torsion free.*

Proof. If $1 \neq x \in G$ with $x^n = 1$, then $(1-x)(1+x+\cdots x^{n-1}) = 0$, so the absence of torsion is clearly necessary. Suppose that G is torsion free. Since G

[3] It is a famous and long-standing open question in ring theory whether "semiprime" is necessary in Walker's theorem.

has a pro-p subgroup of finite index by (2.4), its Sylow q-subgroups are finite for primes q not equal to p. Since G is torsion free these subgroups are trivial, so G is a pro-p group. Therefore Ω_G and Λ_G are scalar local and noetherian by Theorem 4.1. The other conditions needed for Walker's theorem are given by Theorems 4.2(2) and (3) and Theorem 5.1. □

4.4. Maximal orders. It might seem natural to suppose, in the light of Theorem 3.6(3), that whenever Λ_G or Ω_G are prime then they are maximal orders. This guess is wrong, though, as the following example shows. First, recall from [29, 5.1.7] that if R is a ring and M is an R-module, then M is said to be *reflexive* if the natural map $M \to M^{**} = \mathrm{Hom}(\mathrm{Hom}(M,R),R)$ is an isomorphism. Also, recall [29, Chapter 4] that the ideal I of R is said to be *localisable* if the set $\mathcal{C}_R(I)$ of elements of R which are regular modulo I is an Ore set in R.

Example: Let $D := A \rtimes \langle\gamma\rangle$, where A is a copy of $\mathbb{Z}_2$ and γ is the automorphism of order 2 sending each 2-adic integer to its negative. Since D is a pro-2 group with no non-trivial finite normal subgroups, Theorems 4.1 and 4.2 show that Ω_D and Λ_D are prime noetherian scalar local rings. But it's not hard to see that neither of these algebras is a maximal order: for Ω_D, observe that it is local with reflexive Jacobson radical J which is not principal, impossible for a prime noetherian maximal order by [28, Théorème IV.2.15]; for Λ_D, the kernel of the canonical map to $\mathbb{Z}_p$ is a reflexive prime ideal which is not localisable by [4, Theorem A and Lemma 4.1], impossible in a maximal order by [28, Corollaire IV.2.14]. We therefore ask:

Question B. *When are Ω_G and Λ_G maximal orders?*

Since the powerful structural results [15], which can be obtained for certain quotient categories of the category of finitely generated modules over a noetherian maximal order, are potentially important tools in arithmetic applications [18], this question is of more than passing interest.

In the next three paragraphs we offer a conjecture for the answer to Question B, and give some evidence in its support.

4.5. Conjectured answer to Question B. We will need some group-theoretic notions. Let H be a closed subgroup of a compact p-adic analytic group G. We say that H is *orbital* if H has finitely many G-conjugates, or equivalently if its normaliser $N = N_G(H)$ has finite index in G. We say that an orbital subgroup H is *isolated* if N/H has no non-trivial finite normal subgroups.

We will say that G is *dihedral-free* if, whenever H is an orbital closed subgroup of G with $\dim H = 1$, H is isomorphic to $\mathbb{Z}_p$. This seems to be the correct generalisation of the definition in [9].

Conjecture. *Let G be a compact p-adic analytic group, and suppose Ω_G is prime. Then Ω_G is a maximal order if and only if G is dihedral-free.*

4.6. Necessary conditions on G. We fix a prime p and assume throughout this paragraph that G is a compact p-adic analytic group.

Proposition. *Suppose Ω_G is a prime maximal order and let H be a closed* normal *subgroup of G with* $\dim H = 1$. *Then H is pro-p.*

Proof. We may assume that H is isolated, so G/H has no non-trivial finite normal subgroups. Hence, by Theorem 4.2(1), $w_H = \ker(\Omega_G \to \Omega_{G/H})$ is a prime ideal of Ω_G, and it is not hard to see that it is also a reflexive ideal.[4] Now because Ω_G is a maximal order and w_H is a prime reflexive ideal, it must be localisable [28, Corollaire IV.2.14].
But the conditions needed for augmentation ideals to be localisable are known [5, Theorem E]: H/F must be pro-p, where F is the largest finite normal p'-subgroup of H. Since H is normal in G and G has no non-trivial finite normal subgroups by Theorem 4.2(1), $F = 1$ and H is pro-p as required. □

We need the following group-theoretic lemma. We first set ϵ to be 1 for p odd, and $\epsilon = 2$ if $p = 2$, and define, for a closed normal uniform subgroup N of G, $E_G(N)$ to be the centraliser in G of N/N^{p^ϵ}, [5, (2.2)].

Lemma. *Suppose that G is a pro-p group of finite rank with no non-trivial finite normal subgroups. Let N be a maximal open normal uniform subgroup of G. Then*

$$E_G(N) = N.$$

Proof. Recall that $E = E_G(N)$ is an open normal subgroup of G containing N. If E strictly contains N then E/N must meet the centre $Z(G/N)$ non-trivially since G/N is a finite p-group by [20, Proposition 1.11(ii)]. Pick $x \in E\backslash N$ such that $xN \in Z(G/N)$; then $H = \langle N, x\rangle$ is normal in G by the choice of x, and also H is uniform by [5, Lemma 2.3]. This contradicts the maximality of N. □

Recall from Example 4.4 that D denotes the pro-2 completion of the infinite dihedral group.

Corollary. *Let H be a pro-p group of finite rank with no non-trivial finite normal subgroups. Suppose that* $\dim H = 1$. *Then $H \cong \mathbb{Z}_p$, unless $p = 2$ and H is isomorphic to D.*

Proof. Choose a maximal open normal uniform subgroup N of H. By the lemma, $H/N \hookrightarrow \mathrm{Aut}(N/N^{p^\epsilon})$. If p is odd, $|N : N^{p^\epsilon}| = p$, so the latter automorphism group is just $\mathbb{F}_p^\times$. Since H/N is a p-group by [20, Proposition 1.11(ii)] again, $H = N \cong \mathbb{Z}_p$. If $p = 2$ and $H > N$, $H \cong D$. □

This gives us the following weak version of one half of the conjecture. To improve the result from "normal" to "orbital" will presumably require some technical work on induced ideals.

[4] One quick way to see this uses the canonical dimension from (5.4): since $\mathrm{Cdim}(\Omega_G/w_H) = \dim(G/H) = \dim G - 1$ and since Ω_G is Auslander-Gorenstein, w_H is reflexive by Gabber's Maximality Principle [36, Theorem 2.2].

Corollary. *Suppose Ω_G is a prime maximal order. Then any closed normal subgroup H of G of dimension 1 is isomorphic to $\mathbb{Z}_p$.*

Proof. When p is odd the statement is immediate from the proposition and corollary above. So suppose that $p = 2$. We have to rule out the possibility that $H \cong D$, so suppose for a contradiction that this is the case. Then, as in the proof of the proposition, w_H is a prime reflexive, and hence localisable, ideal of Ω_G. Let R denote the local ring $(\Omega_G)_{w_H}$, which has global dimension one by [28, Théorème IV.2.15]. Let $C = \langle c \rangle$ be a copy of the cyclic group of order 2 in H. Then $\mathbb{F}_2 C \subseteq \Omega_G$ and Ω_G is a projective $\mathbb{F}_2 C$-module by [11, Lemma 4.5]. Thus R is a flat $\mathbb{F}_2 C$-module. Since $c+1 \in J(R)$, the $\mathbb{F}_2 C$-module $R/J(R)$ is a sum of copies of the trivial module, so

$$\infty = \mathrm{pd}_{\mathbb{F}_2 C}(\mathbb{F}_2) = \mathrm{pd}_{\mathbb{F}_2 C}(R/J(R)) \leq \mathrm{pd}_R(R/J(R)) = 1.$$

This contradiction shows that the only possibility for H is $\mathbb{Z}_2$. □

4.7. Sufficient conditions on G. We use the following result, essentially due to R. Martin:

Proposition. [27] *Let R be a prime noetherian maximal order and let F be a finite group. Let $S = R * F$ be a prime crossed product. Then S is a maximal order if and only if*

(a) every reflexive height 1 prime P of S is localisable, and
(b) $\mathrm{gld}(S_P) < \infty$ for all such P.

Proof. Conditions (a) and (b) hold in any prime noetherian maximal order, [28, Théorème IV.2.15]. Conversely, suppose that (a) and (b) hold. We use the Test Theorem [27, Theorem 3.2]. Condition (i) of the Test Theorem is just condition (a). We claim that if P is as in the theorem, then $\mathrm{gld}(S_P) = 1$. It's easy to check that $P \cap R$ is a semiprime reflexive ideal of R, so that the localisation $R_{P \cap R}$ exists and is hereditary by [28, Théorème IV.2.15]. Thus $R_{P\cap R} * F$ has injective dimension 1 by [5, Corollary 5.4]. But S_P is a localisation of $R_{P\cap R} * F$, so - given (b) and the comments in (3.6) - $\mathrm{gld}(S_P) \leq 1$. The reverse inequality is obvious, so our claim follows. Condition (ii) now follows from [27, Proposition 2.7]. Condition (iii) follows from the proof of [27, Lemma 3.5] and condition (iv) follows from [27, Remark 3.6 and Lemma 3.7]. □

Lemma. *Let G be a pro-p group of finite rank with no non-trivial finite normal subgroups. Then every reflexive height 1 prime of Ω_G is localisable.*

Proof. Let P be a reflexive height 1 prime of Ω_G. Choose an open normal uniform subgroup N of G. Then Ω_N is a maximal order by Corollary 3.6. Set $\overline{G} := G/N$. Now let $Q = P \cap \Omega_N$ - it is easy to see [27, Remark 3.6] that this is a height 1 reflexive $\overline{G}$-prime ideal of Ω_N. Indeed, Q is the intersection of a $\overline{G}$-orbit of reflexive prime ideals $\{P_1, \ldots, P_n\}$ of Ω_N.

Since each P_i is localisable by [28, Théorème IV.2.15], Q is localisable. In other words, the subset $\mathcal{C} := \mathcal{C}_{\Omega_N}(Q) = \cap_{i=1}^n \mathcal{C}_{\Omega_N}(P_i)$ is a $\overline{G}$-invariant Ore set in Ω_N. An easy calculation [32, proof of Lemma 13.3.5(ii)] shows that $\mathcal{C}$ is an Ore set in Ω_G. In other words, the semiprime ideal $A = \sqrt{Q\Omega_G}$ is localisable in Ω_G and

$$(\Omega_N)_Q * \overline{G} \cong (\Omega_G)_A.$$

Since $\overline{G}$ is a p-group, $A = P$ by [31, Proposition 16.4] and the result follows. □

Corollary. *Let G be a torsion free compact p-adic analytic group. Then Ω_G is a prime maximal order.*

Proof. Suppose that G is as stated. Since G has a pro-p open subgroup, the Sylow q-subgroups of G are finite, and hence trivial, for all primes q not equal to p. That is, G is a pro-p group. Thus the corollary follows from the lemma and the proposition, since $\operatorname{gld}\Omega_G$ is finite by Theorem 5.1. □

5. Dimensions

5.1. Global dimension. The situation as regards the global dimension of Ω_G and Λ_G is completely understood, and depends fundamentally on properties of the cohomology of profinite groups - in particular behaviour under finite extensions - due to Serre [34]. The result is due to Brumer [11, Theorem 4.1] who computed the global dimension of the completed group algebra of an arbitrary profinite group G with coefficients in a pseudo-compact ring R. As a consequence of his work, we have

Theorem. *Let G be a compact p-adic analytic group of dimension d. Then Ω_G and Λ_G have finite global dimension if and only if G has no elements of order p, and in this case*

$$\operatorname{gld}(\Omega_G) = d \quad \textit{and} \quad \operatorname{gld}(\Lambda_G) = d + 1.$$

5.2. Auslander-Gorenstein rings. Recall that the group algebra of an arbitrary finite group over any field is a Frobenius algebra [44, Proposition 4.2.6], and thus is self-injective. It should therefore come as no surprise that injective dimension is well-behaved for Iwasawa algebras. In fact, much more is true:

Theorem. [5, Theorem J] *Let G be a compact p-adic analytic group of dimension d. Then Ω_G and Λ_G are Auslander-Gorenstein rings of dimensions d and $d+1$ respectively.*

This result was first proved by O. Venjakob [39] and is easy to deduce from Theorem 3.6(4) and Theorem 5.1, as follows. Let H be an open uniform normal subgroup of G. Then Ω_H and Λ_H are Auslander-Gorenstein by Theorem 3.6(4), and the dimensions are given by Theorem 5.1. Now apply (2.3)(1): a simple lemma [5, Lemma 5.4] shows that

$$\operatorname{Ext}^i_{\Omega_G}(M, \Omega_G) \cong \operatorname{Ext}^i_{\Omega_H}(M, \Omega_H) \tag{1}$$

for all $i \geq 0$ and all Ω_G-modules M, with a similar isomorphism for Λ_G, and the result follows.

5.3. Dimension functions for Auslander-Gorenstein rings. We recall from [24] the basics of dimension theory over an Auslander-Gorenstein ring R. Write d for the injective dimension of R. The *grade* $j(M)$ of a finitely generated R-module M is defined as follows:

$$j(M) = \min\{j : \operatorname{Ext}^j_R(M,R) \neq 0\}.$$

Thus $j(M)$ exists and belongs to the set $\{0,\dots,d\} \cup \{+\infty\}$. The *canonical dimension* of M, $\operatorname{Cdim}(M)$ is defined to be

$$\operatorname{Cdim}(M) = d - j(M).$$

It is known [24, Proposition 4.5] that Cdim is an exact, finitely partitive dimension function on finitely generated R-modules in the sense of [29, §6.8.4]. That is,

- $\operatorname{Cdim}(0) = -\infty$;
- if $0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$ is an exact sequence of finitely generated modules, then $\operatorname{Cdim}(M) = \max\{\operatorname{Cdim}(N), \operatorname{Cdim}(T)\}$;
- if $MP = 0$ for a prime ideal P of R, and M is a torsion R/P-module, then $\operatorname{Cdim}(M) \leq \operatorname{Cdim}(R/P) - 1$;
- if $\operatorname{Cdim}(M) = t$ then there is an integer n such that every descending chain $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_i \supseteq M_{i+1} \cdots$ of submodules of M has at most n factors M_i/M_{i+1} with $\operatorname{Cdim}(M_i/M_{i+1}) = t$.

The ring R is said to be *grade symmetric* if

$$\operatorname{Cdim}({}_R M) = \operatorname{Cdim}(M_R)$$

for any R−R-bimodule M which is finitely generated on both sides.[5] The triangular matrix ring $\begin{pmatrix} k & k \\ 0 & k \end{pmatrix}$ over a field k gives an easy example of an Auslander Gorenstein ring which is *not* grade symmetric.

The existence of an exact, finitely partitive, symmetric dimension function for the finitely generated modules over a noncommutative noetherian ring R is a very valuable tool which is often not available: the Gel'fand-Kirillov dimension [29, §8.1] - although symmetric - is often not defined; and although the Krull dimension is always defined [29, §6.2], it is a long-standing open question whether it is symmetric in general. As we shall see in the next paragraph, the canonical dimension function fulfils these requirements for an Iwasawa algebra.

If δ is a dimension function on finitely generated R-modules, we say that R is *Cohen-Macaulay with respect to* δ if $\delta(M) = \operatorname{Cdim}(M)$ for all finitely generated R-modules M.

This definition is consistent with, and therefore generalises, the definition from commutative algebra. To see this, suppose that R is a commutative noetherian ring of dimension d. Suppose that R is Cohen-Macaulay [12, Definition 2.1.1], and let M be a finitely generated R-module with Krull dimension $\mathcal{K}(M)$. Note

[5] Alternatively, we can say in these circumstances that the dimension function Cdim is *symmetric*.

that if R is an *affine* (i.e. finitely generated) k-algebra, this equals the Gel'fand-Kirillov dimension of M. Then

$$j(M) + \mathcal{K}(M) = d, \tag{1}$$

[12, Corollary 2.1.4 and Theorem 1.2.10(e)]. And conversely, if (1) holds for all simple R-modules M, then R is Cohen-Macaulay [12, Theorem 1.2.5].

5.4. Canonical dimension for Ω_G. We continue in this paragraph to assume that G is a compact p-adic analytic group of dimension d. Fix an open uniform normal subgroup H of G, and let M be a finitely generated Ω_G-module. By Theorem 5.2 and paragraph (5.3), and with the obvious notation, $\mathrm{Cdim}_G(-)$ and $\mathrm{Cdim}_H(-)$ are well-defined dimension functions, and in fact (5.2)(1) shows that

$$\mathrm{Cdim}_H(M) = \mathrm{Cdim}_G(M). \tag{1}$$

In particular, in studying the canonical dimension we may as well assume that $G = H$ is uniform, which we now do. Hence, by Theorem 3.4, the graded ring of Ω_G is a polynomial $\mathbb{F}_p$-algebra in d variables.

Choose a good filtration for M ($F_n M = MJ^{-n}$ for $n \leq 0$ will do) and form the associated graded module $\mathrm{gr}\, M$. Because the J-adic filtration is Zariskian, it follows from [8, Remark 5.8] that

$$j(\mathrm{gr}\, M) = j(M). \tag{2}$$

Moreover, from this and the concluding remarks of (5.3) we see that

$$\mathcal{K}(\mathrm{gr}\, M) = \mathrm{Cdim}(\mathrm{gr}\, M) = d - j(M). \tag{3}$$

(This shows, incidentally, that $\mathcal{K}(\mathrm{gr}\, M)$ is actually independent of the choice of good filtration on M.)[6] Combining (2) and (3), we find that

$$\mathrm{Cdim}(M) = d - j(M) = \mathrm{Cdim}(\mathrm{gr}\, M) = \mathcal{K}(\mathrm{gr}\, M) = \mathrm{GK}(\mathrm{gr}\, M)$$

for any choice of good filtration on M. This proves the last part of the

Proposition. *Let G be a compact p-adic analytic group.*

(1) Ω_G is grade-symmetric.

(2) Ω_G is ideal-invariant with respect to Cdim.

(3) Suppose that G is uniform. Then for all finitely generated Ω_G-modules M,

$$\mathrm{Cdim}(M) \quad = \quad \mathrm{GK}(\mathrm{gr}\, M).$$

Proof. (1) In view of (5.4)(1) we can and do assume that G is uniform. Write J for the Jacobson radical of Ω_G and let M be a finitely generated Ω_G-module. Then by the definition of the Gel'fand Kirillov dimension [29, §8.1.11], $\mathrm{GK}(\mathrm{gr}\, M)$ is the growth rate $\gamma(f)$ of the function

$$f(n) = \dim \frac{M}{MJ^n};$$

[6] Consider (3) with M the trivial Ω_G-module $\mathbb{F}_p$. Then $\mathcal{K}(\mathrm{gr}\, M) = 0$, so $j(M) = d$ and therefore the injective dimension of Ω_G actually equals d, providing another proof of the numerical part of Theorem 5.1.

note that this function is eventually polynomial because the finitely generated $\operatorname{gr}\Omega_G$-module $\operatorname{gr} M$ has a Hilbert polynomial.

Now let N be an Ω_G-bimodule, finitely generated on both sides. Then NJ is a sub-bimodule, and N/NJ is finite dimensional over $\mathbb{F}_p$ because N is a finitely generated right Ω_G-module. Hence N/NJ is also a finite dimensional *left* Ω_G-module and as such is killed by some power of J, J^a say. Thus $J^aN \subseteq NJ$ and similarly there exists an integer $b \geq 1$ such that $NJ^b \subseteq JN$. An easy induction on n shows that

$$J^{abn}N \subseteq NJ^{bn} \subseteq J^nN \tag{1}$$

for all $n \geq 0$. Letting $f(n) = \dim \frac{N}{NJ^n}$ and $g(n) = \dim \frac{N}{J^nN}$, we obtain

$$g(n) \leq f(bn) \leq g(abn)$$

for all $n \geq 0$. It follows that $\operatorname{Cdim}(N_{|\Omega_G}) = \gamma(f) = \gamma(g) = \operatorname{Cdim}({}_{\Omega_G|}N)$, proving part (1).

For part (2), recall [29, 6.8.13] that a ring R is said to be *ideal-invariant* with respect to a dimension function δ if $\delta(M \otimes_R I) \leq \delta(M)$ for all finitely generated right R-modules M and all two-sided ideals I of R and if the left-hand version of this statement also holds.

In fact, we will show that

$$\operatorname{Cdim}(M \otimes_{\Omega_G} N) \leq \operatorname{Cdim}(M) \tag{4}$$

for any finitely generated Ω_G-module M and any Ω_G-bimodule N, finitely generated on both sides.[7] Let M and N be as above, and let H be an open uniform normal subgroup of G. Since there is an Ω_H-epimorphism $M \otimes_{\Omega_H} N \twoheadrightarrow M \otimes_{\Omega_G} N$, (5.2)(1) shows that we can replace G by H in proving (4); that is, we now assume that G is uniform.

Choose the integer a as above so that $J^{an}N \subseteq NJ^n$ for all $n \geq 0$. Fix n and let

$$f(n) = \dim \frac{M}{MJ^n} \quad \text{and} \quad g(n) = \dim \left(\frac{M \otimes_{\Omega_G} N}{(M \otimes_{\Omega_G} N).J^n} \right).$$

Note that $(M \otimes_{\Omega_G} N).J^n$ equals the image of $M \otimes_{\Omega_G} NJ^n$ in $M \otimes_{\Omega_G} N$ so the right-exactness of tensor product gives

$$M \otimes_{\Omega_G} \left(\frac{N}{J^{an}N} \right) \twoheadrightarrow M \otimes_{\Omega_G} \left(\frac{N}{NJ^n} \right) \cong \frac{M \otimes_{\Omega_G} N}{(M \otimes_{\Omega_G} N).J^n}.$$

Now we have a natural isomorphism of right Ω_G-modules

$$M \otimes_{\Omega_G} \frac{N}{J^{an}N} \cong \frac{M}{MJ^{an}} \otimes_{\Omega_G} N$$

and picking a finite generating set of size t for the left Ω_G-module N shows that

$$\dim \left(\frac{M}{MJ^{an}} \otimes_{\Omega_G} N \right) \leq \left(\dim \frac{M}{MJ^{an}} \right) \cdot t.$$

[7] Compare this with [29, Proposition 8.3.14].

Hence

$$g(n) = \dim\left(\frac{M \otimes_{\Omega_G} N}{(M \otimes_{\Omega_G} N).J^n}\right) \leq \dim\left(M \otimes_{\Omega_G} \left(\frac{N}{J^{an}N}\right)\right) \leq f(an) \cdot t$$

for all $n \geq 0$, so $\mathrm{Cdim}(M \otimes_{\Omega_G} N) = \gamma(g) \leq \gamma(f) = \mathrm{Cdim}(M)$ as required. □

The above proposition is due to the first author; it was inspired by a result of S. J. Wadsley [43, Lemma 3.1].

5.5. Characteristic varieties. Assume in this paragraph that G is uniform. Let M be a finitely generated Ω_G-module. There is another way of seeing that $\mathcal{K}(\mathrm{gr}\, M)$ does not depend on the choice of good filtration for M, as follows. It is well known [26, Chapter III, Lemma 4.1.9] that

$$J(M) := \sqrt{\mathrm{Ann}_{\mathrm{gr}\,\Omega_G}(\mathrm{gr}\, M)}$$

is independent of this choice. Standard commutative algebra now gives

$$\mathcal{K}(\mathrm{gr}\, M) = \mathcal{K}\left(\frac{\mathrm{gr}\,\Omega_G}{J(M)}\right),$$

as claimed.

The graded ideal $J(M)$ is called the *characteristic ideal* of M, and the affine variety $\mathrm{Ch}(M)$ defined by it is called the *characteristic variety* of M. Thus we obtain yet another expression for the canonical dimension of M:

$$\mathrm{Cdim}(M) = \dim \mathrm{Ch}(M). \tag{2}$$

The characteristic variety is defined in an entirely analogous fashion for finitely generated modules over enveloping algebras and Weyl algebras $A_n(\mathbb{C})$. In that setting it enjoys many pleasant properties, in addition to the simple formula (2). In particular, there exists a *Poisson structure* on $\mathrm{Ch}(M)$, which gives more information about M through the geometric properties of the characteristic variety. For example, the fact that the characteristic variety of a finitely generated $A_n(\mathbb{C})$-module is integrable can be used to prove the Bernstein inequality.

Question C. *Is there a way of capturing more information about M in the characteristic variety* $\mathrm{Ch}(M)$*?*

The naive method (mimicking the construction of the Poisson structure in the enveloping algebra case) seems to fail because derivations are not sufficient when studying algebras in positive characteristic: they kill too much. Presumably, if the answer to the above question is affirmative, then differential operators in characteristic p will play a role.

5.6. No GK-dimension. The theory outlined in the previous sections will sound very familiar to the experts. However, Iwasawa algebras are *not* Cohen Macaulay with respect to the GK dimension. This is easily seen by decoding the definition of GK dimension in the case when $G \cong \mathbb{Z}_p$: in this case, Ω_G is isomorphic to the one-dimensional power series ring $\mathbb{F}_p[[t]]$, which (being uncountable) contains polynomial algebras over $\mathbb{F}_p$ of arbitrarily large dimension.

Thus $GK(\Omega_G) = \infty$ for any infinite G, since any such G will contain a closed subgroup isomorphic to $\mathbb{Z}_p$.

If one tries to brush this problem away by replacing the GK dimension by the canonical dimension, then one has to be careful not to fall into the following trap.

Recall [29, Lemma 8.1.13(ii)] that if $R \subseteq S$ are affine k-algebras over a field k, then for any finitely generated S-module M,

$$\mathrm{GK}(N) \leq \mathrm{GK}(M) \tag{3}$$

whenever N is a finitely generated R-submodule of M. This enables one to "pass to subalgebras of smaller dimension" and use inductive arguments on the GK dimension - a ploy used, for example, in the computation of the Krull dimension of $\mathcal{U}(\mathfrak{sl}_2(\mathbb{C}))$ by S.P. Smith [29, Theorem 8.5.16]. Another consequence of this property of GK dimension is that it is impossible to find an embedding $R \hookrightarrow S$ of k-algebras such that $\mathrm{GK}(R) > \mathrm{GK}(S)$.

Unfortunately, (3) fails for Iwasawa algebras, if one tries to replace the GK dimension by the canonical dimension. This is due to the following pathological example:

Example. [38, Chapter VII, page 219] *There exists a continuous embedding of $\mathbb{F}_p$-algebras*

$$\Omega_G \hookrightarrow \Omega_H$$

where $\dim G = 3$ *and* $\dim H = 2$*.*

Proof. Let $G = \mathbb{Z}_p^3$ and $H = \mathbb{Z}_p^2$. By Theorem 3.1 we can identify Ω_G with the three-dimensional power series ring $\mathbb{F}_p[[x, y, z]]$ and Ω_H with the two-dimensional power series ring $\mathbb{F}_p[[a, b]]$.

Because $\mathbb{F}_p[[a]]$ is uncountable, we can find an element $u = u(a) \in a\mathbb{F}_p[[a]]$ such that the $\mathbb{F}_p$-algebra generated by a and u is isomorphic to the two-dimensional polynomial ring $\mathbb{F}_p[a, u]$. Define $\theta : \mathbb{F}_p[[x, y, z]] \to \mathbb{F}_p[[a, b]]$ to be the unique continuous $\mathbb{F}_p$-algebra map such that

$$\theta(x) = b, \quad \theta(y) = ab, \quad \theta(z) = ub.$$

We have

$$\theta\left(\sum_{\lambda,\mu,\nu\in\mathbb{N}} r_{\lambda,\mu,\nu} x^\lambda y^\mu z^\nu\right) = \sum_{n=0}^{\infty} b^n \left(\sum_{\lambda+\mu+\nu=n} r_{\lambda,\mu,\nu} a^\mu u^\nu\right).$$

This shows that θ is an injection, as required. □

One can of course concatenate these embeddings and produce a continuous embedding of Ω_G into $\mathbb{F}_p[[a, b]]$ for abelian uniform pro-p groups G of arbitrarily large dimension. Here is the actual counterexample to the analogue of (3).

Example. *There exist uniform pro-p groups $H \subset G$, a finitely generated Ω_G-module M and a finitely generated Ω_H-submodule N of M such that* $\mathrm{Cdim}(M) = 2$*, but* $\mathrm{Cdim}(N) = 3$.

Proof. Let $R = \mathbb{F}_p[[a,b,c,d]]$ and $S = \mathbb{F}_p[[b,c,d]]$. Let I be the ideal of R generated by $c - ab$ and $d - u(a)b$ where $u(a)$ is chosen as in the previous example and let $M = R/I$. By construction, the graded ideal $\operatorname{gr} I$ is generated by the symbols of c and d, so

$$\operatorname{Cdim}(M) = \mathcal{K}(\operatorname{gr} M) = 2.$$

Now if $r \in I \cap S$, then $\theta(r) = 0$, letting $\theta : \mathbb{F}_p[[b,c,d]] \hookrightarrow \mathbb{F}_p[[a,b]]$ be as above. Hence $r = 0$, so $S \hookrightarrow R/I = M$. Therefore the cyclic S-submodule N of M generated by $1 + I$ is actually free, so $\operatorname{Cdim}(N) = 3$. □

5.7. Krull dimension. The Krull-(Gabriel-Rentschler) dimension of Ω_G was first studied by one of the authors in [1]. An immediate upper bound of $\dim G$ can be obtained using Theorem 3.6, or if one prefers, using [7, Corollary 1.3]. Here is a result covering a large number of cases.

Theorem. [1, Theorem A and Corollary C] *Let G be a compact p-adic analytic group, and let $\mathfrak{g}$ be the $\mathbb{Q}_p$-Lie algebra of an open uniform subgroup of G. Let $\mathfrak{r}$ denote the soluble radical of $\mathfrak{g}$ and suppose that the semisimple part $\mathfrak{g}/\mathfrak{r}$ of $\mathfrak{g}$ is a direct sum of some number of copies of $\mathfrak{sl}_2(\mathbb{Q}_p)$. Then*

$$\mathcal{K}(\Omega_G) = \dim G.$$

In particular, $\mathcal{K}(\Omega_G)$ equals $\dim G$ whenever G is soluble-by-finite. The main idea in the proof is to obtain a lower bound on the Krull dimension of Ω_G for *any* compact p-adic analytic group G. Namely, with $\mathfrak{g}$ as in the theorem, and writing $\lambda(\mathfrak{g})$ for the length of the longest chain of subalgebras of $\mathfrak{g}$, we have

$$\lambda(\mathfrak{g}) \leq \mathcal{K}(\Omega_G).$$

Question D. *With the above notation, is $\mathcal{K}(\Omega_G) = \lambda(\mathfrak{g})$ in general?*

It is easy to see that $\lambda(\mathfrak{g}) = \lambda(\mathfrak{n}) + \lambda(\mathfrak{g}/\mathfrak{n})$ whenever $\mathfrak{n}$ is an ideal of $\mathfrak{g}$. Let N be a closed uniform subgroup of G with Lie algebra $\mathfrak{n}$.

Question E. *Is $\mathcal{K}(\Omega_G) = \mathcal{K}(\Omega_N) + \mathcal{K}(\Omega_{G/N})$?*

Aside from its intrinsic interest, an affirmative answer to Question E would obviously reduce Question D to the study of *almost simple* groups G, (where we say that a uniform pro-p group G is *almost simple* provided its Lie algebra has no non-trivial ideals).

The classical split simple Lie algebras are the first examples to study. Given such a Lie algebra $\mathfrak{g}$, choose a Borel subalgebra $\mathfrak{b}$ and a Cartan subalgebra $\mathfrak{t}$. Then it is easy to produce a chain of subalgebras of $\mathfrak{g}$ of length $\dim \mathfrak{b} + \dim \mathfrak{t}$.

Question F. *For G almost simple and split, is $\mathcal{K}(\Omega_G) = \dim \mathfrak{b} + \dim \mathfrak{t}$?*

Question F has an affirmative answer in the two smallest cases: $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{Q}_p)$ and $\mathfrak{g} = \mathfrak{sl}_3(\mathbb{Q}_p)$. In particular,

Theorem. [1, Theorem B]. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{sl}_3(\mathbb{Q}_p)$. Then Ω_G is a scalar local complete noetherian domain of global dimension 8, with*

$$\mathcal{K}(\Omega_G) = 7.$$

The main idea of the proof of this last result is to show that Ω_G has no finitely generated modules whose canonical dimension equals precisely 1; that is, there is a "gap" at Cdim $= 1$.[8] The extra $\dim \mathfrak{t}$ term in our conjectured formula for $\mathcal{K}(\Omega_G)$ comes from the fact that Ω_G is scalar local - this fact is used crucially in the proof of the lower bound for the Krull dimension of Ω_G.

6. Two-sided ideal structure

6.1. One of the first questions asked when studying a noetherian algebra R is "what are its two-sided ideals?" It is usually sensible to focus first on the *prime* ideals of R.

One way of answering the above question is to give a reduction to the commutative case. This is a recurring theme in noncommutative algebra. For example, if $R = k[G]$ is the group algebra of a polycyclic group G over a field k, the paper [33] by J. E. Roseblade achieves this, "to within a finite group".[9] Similar results hold for universal enveloping algebras $\mathcal{U}(\mathfrak{g})$ of finite dimensional soluble Lie algebras over a field k: see [21] and [29, Chapter 13]. As for the case when $\mathfrak{g}$ is semisimple, one can view the huge body of research on the primitive ideals of $\mathcal{U}(\mathfrak{g})$ as an analysis of the failure of the naive hope that these primitive ideals should be generated by their intersection with the centre of $\mathcal{U}(\mathfrak{g})$, [21]. And for quantised function algebras of semisimple groups, and many related quantum algebras, there are "stratification theorems" which describe their prime and primitive spectra as finite disjoint unions of affine commutative pieces, [10, Theorem II.2.13].

Unfortunately, no such results are currently known for Iwasawa algebras - see below for a summary of what little *is* known. Alleviation of this state of gross ignorance would seem to be the most pressing problem in the subject.

Because of the crossed product decomposition (2.3)(1) and the going up and down theorems for crossed products of finite groups [31, Theorem 16.6], one should naturally first concentrate on the case when G is uniform.

6.2. Ideals arising from subgroups and from centres. Since centrally generated one-sided ideals are necessarily two-sided, it helps to know the centre of the ring in question. However the centre of Iwasawa algebras is not very big:

Theorem. [2, Corollary A] *Let G be a uniform pro-p group and let Z be its centre. Then the centre of Ω_G equals Ω_Z and the centre of Λ_G equals Λ_Z.*

Thus when the centre of G is trivial (and this happens frequently), Ω_G has no non-trivial centrally generated ideals. This is one place where the analogy with enveloping algebras of semisimple Lie algebras breaks down.

[8] A similar idea was used by Smith [35] in giving an upper bound for the Krull dimension of $\mathcal{U}(\mathfrak{g})$ when $\mathfrak{g}$ is a complex semisimple Lie algebra. We note in passing that $\mathcal{K}(\mathcal{U}(\mathfrak{g}))$ when $\mathfrak{g}$ is complex semisimple has been recently proved to be equal to $\dim \mathfrak{b}$ by Levasseur [25], answering a long-standing question in the affirmative.

[9] See [31, Chapter 5] for more details.

One can also produce two-sided ideals by using normal subgroups. Certainly when H is a closed normal subgroup of G, the augmentation ideal

$$w_H := \ker(\Omega_G \to \Omega_{G/H})$$

is a two-sided ideal of Ω_G and we can tell whether it is prime or semiprime using Theorem 4.2. As for Λ_G, H yields two augmentation ideals: the inverse image v_H of w_H under the natural projection $\Lambda_G \twoheadrightarrow \Omega_G$ and "the" augmentation ideal

$$I_H = \ker(\Lambda_G \to \Lambda_{G/H}).$$

The behaviour of these ideals regarding localisation is quite well understood:

Theorem. *Let H be a closed normal subgroup of the compact p-adic analytic group G and let F be the largest finite normal subgroup of H of order coprime to p. Then*

(1) [5] *w_H and v_H are localisable if and only if H/F is pro-p,*
(2) [4] *I_H is localisable if and only if H is finite-by-nilpotent.*

These results were prompted by the formulation of the Iwasawa Main Conjecture by Coates *et al* in [19]. Localisation techniques play an important role in the construction of *characteristic elements* for suitable Λ_G-modules. For number-theoretic reasons, it is assumed in [19] that the subgroup H actually satisfies $G/H \cong \mathbb{Z}_p$: in arithmetic applications, G arises as the Galois group of a certain extension K of $\mathbb{Q}$ containing the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{\text{cyc}}$, and H is taken to be $\text{Gal}(K/\mathbb{Q}^{\text{cyc}})$. The characteristic elements all lie inside the K_1-group of the localisation of Λ_G at the Ore set

$$\mathcal{C}_{\Lambda_G}(v_N) \times \{1, p, p^2, \ldots\},$$

where N is the largest closed normal pro-p subgroup of G which is open in H. For more details, see [19, §2], [6] and [5, Theorem G].

Notwithstanding the above, the most embarrassing aspect of the state of our knowledge about ideals of Iwasawa algebras is the lack of examples. In particular, we've noted that central elements and closed normal subgroups give rise to ideals. This suggests the following improperly-posed question, for which we'll suggest more precise special cases in the succeeding paragraphs.

Question G. *Is there a mechanism for constructing ideals of Iwasawa algebras which involves neither central elements nor closed normal subgroups?*

One way to begin the study of prime ideals is to look first at the smallest non-zero ones - that is, the prime ideals of height one. With one eye on the commutative case and another on the results of (4.4) on maximal orders, one can ask when they are all principal. Here are two slightly more precise ways to ask this question:

Question H. *When is Ω_G a unique factorisation ring in the sense of* [16]*?*

Question I. *When G is uniform, is every reflexive prime ideal of Ω_G principal?*

6.3. The case when G is almost simple. Recall that the compact p-adic analytic group G is *almost simple* if every non-trivial closed normal subgroup of G is open (5.7). For such groups the constructions of (6.2) do not produce anything interesting because Ω_G/w_H is artinian and hence finite dimensional over $\mathbb{F}_p$ for any closed normal subgroup $H \neq 1$. So Question G specialises here to

Question J. *Let G be an almost simple uniform pro-p group and let P be a nonzero prime ideal of Ω_G. Must P be the unique maximal ideal of Ω_G?*

We remind the reader that $x \in \Omega_G$ is *normal* if $x\Omega_G = \Omega_G x$. Another closely related question is

Question K. *Let G be as in Question J, with $G \ncong \mathbb{Z}_p$. Must any nonzero normal element of Ω_G be a unit?*

In [22], M. Harris claimed that, for G as in Question J, any closed subgroup H of G with $2\dim H > \dim G$ gives rise to a non-zero two-sided ideal in Ω_G, namely the annihilator of the "Verma module" constructed by induction from the simple Ω_H-module. Unfortunately his paper contains a gap, so Question J remains open. Some slight evidence towards a positive answer is provided by

Theorem. [3, Theorem A] *Suppose that G is an almost simple uniform pro-p group and that the Lie algebra of G contains a copy of the two-dimensional non-abelian Lie algebra. Then for any two-sided ideal I of Ω_G,*

$$\mathcal{K}(\Omega_G/I) \neq 1.$$

Recall [29, §6.4.4] that if R is a noetherian ring with $\mathcal{K}(R) < \infty$, the *classical Krull dimension* $\dim R$ of R is the largest length of a chain of prime ideals of R. We always have $\dim R \leq \mathcal{K}(R)$; an easy consequence of the above result is

$$\dim(\Omega_G) < \dim G$$

whenever G satisfies conditions of the Theorem.

6.4. The case when G is nilpotent. Towards the opposite end of the "spectrum of commutativity" from the almost simple groups lie the nilpotent groups. Motivated by analogous results for enveloping algebras of nilpotent Lie algebras [21, Chapter 4] and for group algebras $k[G]$ of finitely generated nilpotent groups G [33, Theorem E], we ask

Question L. *Let G be a nilpotent uniform pro-p group with centre Z and let I be a nonzero ideal of Ω_G. Does I contain a non-zero central element? That is, is $I \cap \Omega_Z$ nonzero?*

S. J. Wadsley has shown that Question L has an affirmative answer in the case when G is one of the simplest possible nonabelian nilpotent uniform pro-p groups:

Theorem. [43, Theorem 4.10] *Let G be a uniform Heisenberg pro-p group with centre Z and let I be a nonzero two-sided ideal of Ω_G. Then $I \cap \Omega_Z \neq 0$.*

A uniform pro-p group G is said to be *Heisenberg* provided its centre Z is isomorphic to $\mathbb{Z}_p$ and G/Z is abelian. The main idea of the proof of the above result is to show that for any integer t, any finitely generated Ω_G-module M satisfying $\mathrm{Cdim}(M) \leq \dim G/Z - t$ is actually finitely generated over "most" subalgebras Ω_H satisfying $Z \leq H$ and $\dim G/H = t$ [43, Theorem 3.10].

In a more precise version of Question L, one might also hope that, when G is nilpotent, "small" prime ideals I in Ω_G are *controlled* by Ω_Z; that is

$$I = (I \cap \Omega_Z)\Omega_G.$$

Question O suggests a more general version of this.

Moreover, one might even hope that arbitrary ideals of these Iwasawa algebras of nilpotent groups are constructed by means of a sequence of centrally generated ideals - that is, one can ask:

Question M. *Suppose that G is a nilpotent uniform pro-p group. If I is an ideal of Ω_G strictly contained in $J(\Omega_G)$, is there a non-zero central element in $J(\Omega_G)/I$?* [10]

6.5. The case when G is soluble. Given the parallels pointed out in (3.3) between the Iwasawa algebras of uniform soluble groups and the enveloping algebras of finite dimensional complex soluble Lie algebras, it is natural to wonder whether properties known for the latter case might also be valid in the former. We give two sample questions of this sort. Recall for the first that a prime ideal P of the ring R is *completely prime* if R/P is a domain.

Question N. *Let G be a soluble uniform pro-p group.*

(i) Is every prime ideal of Ω_G completely prime? [11]

(ii) Is the prime spectrum of Ω_G the disjoint union of finitely many commutative strata (along the lines of [10, Theorem II.2.13]*, but with necessarily non-affine strata)?*

The simple possible nonabelian soluble case has been studied by O. Venjakob:

Theorem. [40, Theorem 7.1] *Let $G = X \rtimes Y$ be a nonabelian semidirect product of two copies of $\mathbb{Z}_p$. Then the only prime ideals of Ω_G are $0, w_X$ and $J(\Omega_G)$, and each one is completely prime. Moreover, w_X is generated by a normal element.*

An example of such a nonabelian semidirect product is provided by the group $B = \overline{\langle a_1, a_2 \rangle}$ considered in Example 3.2.

Following J. E. Roseblade and D. S. Passman [33, §1.5], we define the *Zalesskii subgroup* A of the soluble uniform pro-p group G to be the centre of the largest nilpotent closed normal subgroup H of G. We say that an ideal I of Ω_G is *faithful* if G acts faithfully on the quotient Ω_G/I. If Question L has a positive answer, then it's possible that a more general statement is true:

[10] Compare with [21, Proposition 4.7.1(i)].

[11] Compare with [21, Theorem 3.7.2].

Question O. *Let G be a soluble uniform pro-p group. Is every faithful prime ideal of Ω_G controlled by the Zalesskii subgroup A of G?*

References

[1] K. Ardakov, *Krull dimension of Iwasawa Algebras*, J. Algebra 280 (2004), 190-206.

[2] K. Ardakov, *The centre of completed group algebras of pro-p groups*, Doc. Math 9 (2004), 599-606.

[3] K. Ardakov, *Prime ideals in noncommutative Iwasawa algebras*, Math. Proc. Camb. Phil. Soc. 141(2) (2006), 197-203.

[4] K. Ardakov, *Localisation at augmentation ideals in Iwasawa algebras*, Glasgow Mathematical Journal 48(2) (2006), 251-267.

[5] K. Ardakov and K. A. Brown, *Primeness, semiprimeness and localisation in Iwasawa algebras*, Transactions of the Amer. Math. Soc., to appear.

[6] K. Ardakov and S. J. Wadsley, *Characteristic elements for p-torsion Iwasawa modules*, Journal of Algebraic Geometry 15 (2006), 339-377.

[7] K. Ajitabh, S. P. Smith, J. J. Zhang, *Auslander-Gorenstein rings*, Comm. Algebra 26 (1998), 2159-2180.

[8] J.-E. Bjork and E.K. Ekstrom, *Filtered Auslander-Gorenstein rings*, in "Colloque en l'honneur de J. Dixmier," Birkhauser, Bosel, 1990.

[9] K. A. Brown, *Height one primes of polycyclic group rings*, J. London Math. Soc. 32 (1985) 426-438; corrigendum J. London Math. Soc. .

[10] K. A. Brown and K.R. Goodearl, *Lectures on Algebraic Quantum groups*, Birkhauser, 2002.

[11] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra 4 (1966), 442-470.

[12] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics, CUP, (1993).

[13] R. Carter, *Simple groups of Lie type*, J. Wiley, London (1989).

[14] G. Cauchon, *Effacement des dérivations et spectres premiers des algèbres quantiques*, J. Algebra 260 (2003), no. 2, 476-518.

[15] M. Chamarie, *Modules sur les anneaux de Krull non commutatifs*, Paul Dubreil and Marie-Paule Malliavin algebra seminar, Lecture Notes in Math. vol. 1029, Springer, (1982), 283-310.

[16] A.W. Chatters and D.A. Jordan, *Non-commutative unique factorisation rings*, J. London Math. Soc. (2) 33 (1986), no. 1, 22–32.

[17] J. Coates, Iwasawa algebras and arithmetic, Séminaire Bourbaki 2001/2002 Astérisque 290 (2003), 37–52.

[18] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu 2, (2003) 73-108.

[19] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES 101 (2005), 163-208.

[20] J.D.Dixon, M.P.F. Du Sautoy, A.Mann, D.Segal, *Analytic pro-p groups*, 2nd edition, CUP (1999).

[21] J. Dixmier, *Enveloping Algebras*, Graduate Studies in Mathematics 11, Amer. Math. Soc. (1996).

[22] M. Harris, *The annihilators of p-Adic Induced Modules*, J.Algebra 67, 68-71 (1980).

[23] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHES 26 (1965), 389-603.

[24] T. Levasseur, *Some properties of noncommutative regular graded rings*, *Glasgow J. Math*, 34, (1992) 277-300.

[25] T. Levasseur, *Krull dimension of the enveloping algebra of a semisimple Lie algebra*, Proc. Amer. Math. Soc. 130 (2002), no. 12, 3519-3523.

[26] L. Huishi and F. van Oystaeyen, *Zariskian filtrations*, Kluwer Academic Publishers, K-monographs in Mathematics, vol. 2 (1996).

[27] R. Martin, *Skew group rings and maximal orders*, Glasgow Math. J. 37 (1995), no. 2, 249-263.

[28] G. Maury and J. Raynaud, *Ordres Maximaux au Sens de K. Asano* Lecture Notes in Math. vol. *808*, Springer, 1980.

[29] J.C. McConnell, J.C. Robson, *Noncommutative Noetherian rings*, AMS Graduate Studies in Mathematics, vol. 30 (2001).

[30] A. Neumann, *Completed group algebras without zero divisors*, Arch. Math. (Basel) 51, (1988) 496-499.

[31] D.S. Passman, *Infinite Crossed Products*, Pure and Applied Mathematics vol. 135, Academic press, San Diego (1989).

[32] D.S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, (1977).

[33] J. E. Roseblade, *Prime ideals in group rings of polycyclic groups*, Proc. London Math. Soc (3) 36, (1978) 385-447.

[34] J.-P. Serre, *Sur la dimension homologique des groupes profinis*, Topology 3, (1965) 413-420.

[35] S. P. Smith, *Krull dimension of factor rings of the enveloping algebra of a semisimple Lie algebra*, Math. Proc. Camb. Phil. Soc. 93 (1983), no. 3, 459-466.

[36] J. T. Stafford, *Auslander-regular algebras and maximal orders*, J. London Math. Soc. (2) 50 (1994), no. 2, 276-292.

[37] P. Schneider and J. Teitelbaum, *Banach space representations and Iwasawa theory*, Israel J. Math. 127 (2002), 359-380.

[38] P. Samuel, O. Zariski, *Commutative algebra*, Graduate Texts in Mathematics vol.29, Springer, 1975.

[39] O. Venjakob, *On the structure theory of the Iwasawa algebra of a compact p-adic Lie group*, J. Eur. Math. Soc. (JEMS) 4 (2002), no. 3, 271-311.

[40] O. Venjakob, *A noncommutative Weierstrass Preparation Theorem and applications to Iwasawa Theory*, J. Reine Angew. Math. 559 (2003), 153-191.

[41] O. Venjakob and P. Schneider, *On the codimension of modules over skew power series rings with applications to Iwasawa algebras*, J. Pure Appl. Algebra 204(2) (2006), 349-367.

[42] R. Walker, *Local rings and normalising sets of elements*, Proc. London Math. Soc. 24 (1972), 27-45.

[43] S. J. Wadsley, *A Bernstein-type inequality for Heisenberg pro-p groups*, to appear in the Quarterly Journal of Mathematics.

[44] C. A. Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics 38, CUP, (1994).

[45] A. Zaks, *Injective dimension of semiprimary rings*, J. Algebra 13 (1969), 73-89.

K. Ardakov
DPMMS
University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB, UK
K.Ardakov@dpmms.cam.ac.uk

K. A. Brown
Department of Mathematics
University of Glasgow
Glasgow G12 8QW
UK
kab@maths.gla.ac.uk

On the Image of l-Adic Galois Representations for Abelian Varieties of Type I and II

Dedicated to John Coates on the occasion of his 60-th birthday

G. Banaszak, W. Gajda, P. Krasoń

Received: August 9, 2005
Revised: August 10, 2006

Abstract. In this paper we investigate the image of the l-adic representation attached to the Tate module of an abelian variety over a number field with endomorphism algebra of type I or II in the Albert classification. We compute the image explicitly and verify the classical conjectures of Mumford-Tate, Hodge, Lang and Tate for a large family of abelian varieties of type I and II. In addition, for this family, we prove an analogue of the open image theorem of Serre.

2000 Mathematics Subject Classification: 11F80, 11G10
Keywords and Phrases: abelian varieties, l-adic representations

1. Introduction.

Let A be an abelian variety defined over a number field F. Let l be an odd prime number. In this paper we study the images of the l-adic representation $\rho_l : G_F \longrightarrow GL(T_l(A))$ and the *mod l* representation $\overline{\rho}_l : G_F \longrightarrow GL(A[l])$ of the absolute Galois group $G_F = G(\bar{F}/F)$ of the field F, associated with the Tate module, for A of type I or II in the Albert classification list cf. [M]. In our previous paper on the subject cf. [BGK], we computed the images of the Galois representations for some abelian varieties with real (type I) and complex multiplications (type IV) by the field $E{=}End_F(A) \otimes \mathbb{Q}$ and for l which splits completely in the field E *loc. cit.*, Theorem 2.1 and Theorem 5.3.

In the present paper we extend results proven in [BGK] to a larger class (cf. Definition of class $\mathcal{A}$ below) of abelian varieties which includes some varieties with non-commutative algebras of endomorphisms, and to almost all prime numbers l. In order to get these results, we had to implement the Weil restriction functor $R_{L/K}$ for a finite extension of fields L/K. In section 2 of the paper we give an explicit description of the Weil restriction functor for affine group schemes which we use in the following sections. In a very short section 3 we prove two general lemmas about bilinear forms which we apply to Weil pairing in the following section. Further in section 4, we collect some auxiliary facts about abelian varieties. In section 5 we obtain the integral versions of the results of Chi cf. [C2], for abelian varieties of type II and compute Lie algebras and endomorphism algebras corresponding to the λ-adic representations related to the Tate module of A. In section 6 we prove the main results of the paper which concern images of Galois representations ρ_l, $\rho_l \otimes \mathbb{Q}_l : G_F \rightarrow GL(V_l(A))$, the mod l-representation $\overline{\rho}_l$ and the associated group schemes $\mathcal{G}_l^{alg}$, G_l^{alg} and $G(l)^{alg}$, respectively.

The main results proven in this paper concern the following class of abelian varieties:

Definition of class $\mathcal{A}$.
We say that an abelian variety A/F, defined over a number field F is of class $\mathcal{A}$, if the following conditions hold:

(i) *A is a simple, principally polarized abelian variety of dimension g*
(ii) *$\mathcal{R} = End_{\bar{F}}(A) = End_F(A)$ and the endomorphism algebra $D = \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q}$, is of type I or II in the Albert list of division algebras with involution (cf. [M], p. 201).*
(iii) *the field F is such that for every l the Zariski closure G_l^{alg} of $\rho_l(G_F)$ in $GL_{2g}/\mathbb{Q}_l$ is a connected algebraic group*
(iv) *$g = hed$, where h is an odd integer, $e = [E : \mathbb{Q}]$ is the degree of the center E of D and $d^2 = [D : E]$.*

Let us recall the definition of abelian varieties of type I and II in the Albert's classification list of division algebras with involution [M], p. 201. Let $E \subset D = End_{\bar{F}}(A) \otimes_Z \mathbb{Q}$ be the center of D and E be a totally real extension of $\mathbb{Q}$ of degree e. Abelian varieties of type I are such that $D = E$. Abelian varieties of type II are those for which D is an indefinite quaternion algebra with the center E, such that $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i=1}^{e} M_{2,2}(\mathbb{R})$.

We have chosen to work with principal polarizations, however the main results of this paper have their analogs for any simple abelian variety A with a fixed polarization, provided A satisfies the above conditions (ii), (iii) and (iv). The most restrictive of the conditions in the definition of class $\mathcal{A}$ is condition (iv) on the dimension of the variety A. We need this condition to perform computations with Lie algebras in the proof of Lemma 5.33, which are based on an application of the minuscule conjecture cf. [P]. Note that due to results of Serre, the assumption (iii) is not very restrictive. It follows by [Se1] and [Se4] that for an abelian variety A defined over a number field K, there exists a finite extension

K^{conn}/K for which the Zariski closure of the group $\rho_l(G_{K^{conn}})$ in GL is a connected variety for any prime l. Hence, to make A meet the condition (iii), it is enough to enlarge the base field, if necessary. Note that the field K^{conn} can be determined in purely algebraic terms, as the intersection of a family of fields of division points on the abelian variety A cf. [LP2], Theorem 0.1.

Main results

Theorem A. *[Theorem 6.9]*
If A is an abelian variety of class $\mathcal{A}$, then for $l \gg 0$, we have equalities of group schemes:

$$(G_l^{alg})' \;=\; \prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(Sp_{2h})$$

$$(G(l)^{alg})' \;=\; \prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(Sp_{2h}),$$

where G' stands for the commutator subgroup of an algebraic group G, and $R_{L/K}(-)$ denotes the Weil restriction functor.

Theorem B. *[Theorem 6.16]*
If A is an abelian variety of class $\mathcal{A}$, then for $l \gg 0$, we have:

$$\overline{\rho_l}(G_F') \;=\; \prod_{\lambda | l} Sp_{2h}(k_\lambda) \;=\; Sp_{2h}(\mathcal{O}_E/l\mathcal{O}_E)$$

$$\rho_l(\,\overline{G_F'}\,) \;=\; \prod_{\lambda | l} Sp_{2h}(\mathcal{O}_\lambda) \;=\; Sp_{2h}(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_l),$$

where $\overline{G_F'}$ is the closure of G_F' in the profinite topology in G_F.

As an application of Theorem A we obtain:

Theorem C. *[Theorem 7.12]*
If A is an abelian variety of class $\mathcal{A}$, then

$$G_l^{alg} = MT(A) \otimes \mathbb{Q}_l,$$

for every prime number l, where $MT(A)$ denotes the Mumford-Tate group of A, i.e., the Mumford -Tate conjecture holds true for A.

Using the approach initiated by Tankeev [Ta5] and Ribet [R2], futher developed by V.K. Murty [Mu] combined with some extra work on the Hodge groups in section 7, we obtain:

Theorem D. *[Theorems 7.34, 7.35]*
If A is an abelian variety of class $\mathcal{A}$, then the Hodge conjecture and the Tate conjecture on the algebraic cycle maps hold true for the abelian variety A.

In the past there has been an extensive work on the Mumford-Tate, Tate and Hodge conjectures for abelian varieties. Special cases of the conjectures were verified for some classes of abelian varieties, see for example papers: [Ab], [C2], [Mu], [P], [Po], [R2], [Se1], [Se5], [Ta1], [Ta2], [Ta3]. For an abelian variety A of type I or II the above mentioned papers consider the cases where A is such that $End(A) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or has center $\mathbb{Q}$. The papers [Ta4], [C1] and [BGK] considered some cases with the center larger than $\mathbb{Q}$. For more complete list of results concerning the Hodge conjecture see [G]. In the current work we prove the conjectures in the case when the center of $End(A) \otimes \mathbb{Q}$ is an arbitrary totally real extension of $\mathbb{Q}$. To prove the conjectures for such abelian varieties we needed to do careful computations using the Weil restriction functor.

Moreover, using a result of Wintenberger (cf. [Wi], Cor. 1, p.5), we were able to verify that for A of class $\mathcal{A}$, the group $\rho_l(G_F)$ contains the group of all the homotheties in $GL_{T_l(A)}(\mathbb{Z}_l)$ for $l \gg 0$, i.e., the Lang conjecture holds true for A cf. Theorem 7.38.

As a final application of the method developed in this paper, we prove an analogue of the open image theorem of Serre cf. [Se1] for the class of abelian varieties we work with.

Theorem E. *[Theorem 7.42]*
If A is an abelian variety of class $\mathcal{A}$, then for every prime number l, the image $\rho_l(G_F)$ is open in the group $C_{\mathcal{R}}(GSp_{(\Lambda,\, \psi)})(\mathbb{Z}_l)$ of $\mathbb{Z}_l$-points of the commutant of $\mathcal{R}{=}End\, A$ in the group $GSp_{(\Lambda,\, \psi)}$ of symplectic similitudes of the bilinear form $\psi : \Lambda \times \Lambda \longrightarrow \mathbb{Z}$ associated with the polarization of A. In addition, for $l \gg 0$ we have:

$$\rho_l(\overline{G_F'}) \;=\; C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)})(\mathbb{Z}_l).$$

As an immediate corollary of Theorem E we obtain that for any A of class $\mathcal{A}$ and for every l, the group $\rho_l(G_F)$ is open in $\mathcal{G}_l^{alg}(\mathbb{Z}_l)$ (in the l-adic topology), where $\mathcal{G}_l^{alg}$ is the Zariski closure of $\rho_l(G_F)$ in $GL_{2g}/\mathbb{Z}_l$. cf. Theorem 7.48. Recently, the images of Galois representations coming from abelian varieties have also been considered by A.Vasiu (cf. [Va1],[Va2]).

2. Weil restriction functor $R_{E/K}$ for affine schemes and Lie algebras.

In this section we describe the Weil restriction functor and its basic properties which will be used in the paper c.f. [BLR], [V1], [V2, pp. 37-40], [W1] and [W2, pp. 4-9]. For the completeness of the exposition and convenience of the reader we decided to include the results although some of them might be known to specialists. Let E/K be a separable field extension of degree n. Let $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ denote the set of all imbeddings $E \to E^{\sigma_i} \subset \overline{K}$ fixing K. Define M to be the composite of the fields E^{σ_i}

$$M = E^{\sigma_1} \ldots E^{\sigma_n}.$$

Let $X = [x_1, x_2, \ldots x_r]$ denote a multivariable. For polynomials $f_k = f_k(X) \in E[X]$, $1 \leq k \leq s$, we denote by $I = (f_1, f_2, \ldots, f_s)$ the ideal generated by the f_k's and put $I^{\sigma_i} = (f_1^{\sigma_i}(X), f_2^{\sigma_i}(X), \ldots, f_s^{\sigma_i}(X))$ for any $1 \leq i \leq n$. Let $A = E[X]/I$. Define E-algebras A^{σ_i} and $\overline{A}$ as follows:

$$A^{\sigma_i} = A \otimes_{E,\sigma_i} M \;\cong\; M[X]/\, I^{\sigma_i} M[X],$$

$$\overline{A} = A^{\sigma_1} \otimes_M \cdots \otimes_M A^{\sigma_n}.$$

Let $X^{\sigma_1}, \ldots, X^{\sigma_n}$ denote the multivariables

$$X^{\sigma_i} = [x_{i,1}, x_{i,2}, \ldots, x_{i,r}]$$

on which the Galois group $G = G(M/K)$ acts naturally on the right. Indeed for any imbedding σ_i and any $\sigma \in G$ the composition $\sigma_i \circ \sigma$, applied to E on the right, gives uniquely determined imbedding σ_j of E into $\overline{K}$, for some $1 \leq j \leq n$. Hence we define the action of $G(M/K)$ on the elements X^{σ_i} in the following way:

$$(X^{\sigma_i})^{\sigma} = X^{\sigma_j}.$$

We see that

$$\overline{A} \;\cong\; M[X^{\sigma_1}, \ldots, X^{\sigma_n}]/\, (I_1 + \cdots + I_n),$$

where $I_k = M[X^{\sigma_1}, \ldots, X^{\sigma_n}]I_{(k)}$ and $I_{(k)} = (f_1^{\sigma_k}(X^{\sigma_k}), \ldots, f_s^{\sigma_k}(X^{\sigma_k}))$, for any $1 \leq k \leq n$.

Lemma 2.1.

$$\overline{A}^G \otimes_K M \cong \overline{A}.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis of E over K. It is clear that

$$\sum_{i=1}^{n} \alpha_j^{\sigma_i} X^{\sigma_i} \;\in\; \overline{A}^G.$$

Since $[\alpha_j^{\sigma_i}]_{i,j}$ is an invertible matrix with coefficients in M, we observe that $X^{\sigma_1}, \ldots, X^{\sigma_n}$ are in the subalgebra of $\overline{A}$ generated by M and $\overline{A}^G$. But $X^{\sigma_1}, \ldots, X^{\sigma_n}$ and M generate $\overline{A}$ as an algebra. $\square$

Remark 2.2. Notice that the elements $\sum_{i=1}^{n} \alpha_j^{\sigma_i} X^{\sigma_i}$ for $j = 1, \ldots, n$ generate $\overline{A}^G$ as a K-algebra. Indeed if C denotes the K-subalgebra of $\overline{A}^G$ generated by these elements and if C were smaller than $\overline{A}^G$, then $C \otimes_K M$ would be smaller than $\overline{A}^G \otimes_K M$, contrary to Lemma 2.1.

Definition 2.3. *Put $V = spec\, A$, and $W = spec\, \overline{A}^G$. Weil's restriction functor $R_{E/K}$ is defined by the following formula:*

$$R_{E/K}(V) = W.$$

Note that we have the following isomorphisms:

$$W \otimes_K M \; = \; spec\,(\overline{A}^G \otimes_K M) \; \cong \; spec\,\overline{A} \cong$$

$$spec\,(A^{\sigma_1} \otimes_M \cdots \otimes_M A^{\sigma_n}) \; \cong \; (V \otimes_{E,\sigma_1} M) \otimes_M \cdots \otimes_M (V \otimes_{E,\sigma_n} M),$$

hence

$$R_{E/K}(V) \otimes_K M \cong (V \otimes_{E,\sigma_1} M) \otimes_M \cdots \otimes_M (V \otimes_{E,\sigma_n} M).$$

Lemma 2.4. *Let $V' \subset V$ be a closed imbedding of affine schemes over E. Then $R_{E/K}(V') \subset R_{E/K}(V)$ is a closed imbedding of affine schemes over K.*

Proof. We can assume that $V = spec\,(E[X]/I)$ and $V' = spec\,(E[X]/J)$ for two ideals $I \subset J$ of $E[X]$. Put $A = E[X]/I$ and $B = E[X]/J$ and let $\phi : A \rightarrow B$ be the natural surjective ring homomorphism. The homomorphism ϕ induces the surjective E-algebra homomorphism

$$\overline{\phi} : \overline{A} \rightarrow \overline{B}$$

which upon taking fix points induces the K-algebra homomorphism

$$\overline{\phi}^G : \overline{A}^G \rightarrow \overline{B}^G. \tag{2.5}$$

By Remark 2.2 we see that $\overline{B}^G$ is generated as a K-algebra by elements $\sum_{i=1}^n \alpha_j^{\sigma_i} X^{\sigma_i}$ (more precisely their images in $\overline{B}^G$). Similarly $\overline{A}^G$ is generated as a K-algebra by elements $\sum_{i=1}^n \alpha_j^{\sigma_i} X^{\sigma_i}$ (more precisely their images in $\overline{A}^G$). It is clear that $\overline{\phi}^G$ sends the element $\sum_{i=1}^n \alpha_j^{\sigma_i} X^{\sigma_i} \in \overline{A}^G$ into $\sum_{i=1}^n \alpha_j^{\sigma_i} X^{\sigma_i} \in \overline{B}^G$. Hence $\overline{\phi}^G$ is onto. □

Let $\alpha_1, \ldots, \alpha_n$ be a basis of E over K and let $\beta_1, \ldots, \beta_n$ be the corresponding dual basis with respect to $Tr_{E/K}$. Define block matrices:

$$\mathbb{A} = \begin{pmatrix} \alpha_1^{\sigma_1} I_r & \alpha_1^{\sigma_2} I_r & \ldots & \alpha_1^{\sigma_n} I_r \\ \alpha_2^{\sigma_1} I_r & \alpha_2^{\sigma_2} I_r & \ldots & \alpha_2^{\sigma_n} I_r \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_n^{\sigma_1} I_r & \alpha_n^{\sigma_2} I_r & \ldots & \alpha_n^{\sigma_n} I_r \end{pmatrix}, \quad \mathbb{B} = \begin{pmatrix} \beta_1^{\sigma_1} I_r & \beta_2^{\sigma_1} I_r & \ldots & \beta_n^{\sigma_1} I_r \\ \beta_1^{\sigma_2} I_r & \beta_2^{\sigma_2} I_r & \ldots & \beta_n^{\sigma_2} I_r \\ \vdots & \vdots & \ldots & \vdots \\ \beta_1^{\sigma_n} I_r & \beta_2^{\sigma_n} I_r & \ldots & \beta_n^{\sigma_n} I_r \end{pmatrix}$$

Notice that by definition of the dual basis $\mathbb{A}\mathbb{B} = \mathbb{B}\mathbb{A} = I_{rn}$. Define block diagonal matrices:

$$\mathbb{X} = \begin{pmatrix} X^{\sigma_1} & 0I_r & \dots & 0I_r \\ 0I_r & X^{\sigma_2} & \dots & 0I_r \\ \vdots & \vdots & \dots & \vdots \\ 0I_r & 0I_r & \dots & X^{\sigma_n} \end{pmatrix}, \quad \mathbb{Y} = \begin{pmatrix} Y^{\sigma_1} & 0I_r & \dots & 0I_r \\ 0I_r & Y^{\sigma_2} & \dots & 0I_r \\ \vdots & \vdots & \dots & \vdots \\ 0I_r & 0I_r & \dots & Y^{\sigma_n} \end{pmatrix},$$

where $Y^{\sigma_1}, \dots, Y^{\sigma_n}$ and $X^{\sigma_1}, \dots, X^{\sigma_n}$, are multivariables written now in a form of $r \times r$ matrices indexed by $\sigma_1, \dots, \sigma_n$. Let T_{ij} and S_{ij}, for all $1 \leq i \leq n$, $1 \leq j \leq n$, be $r \times r$ multivariable matrices. Define block matrices of multivariables:

$$\mathbb{T} = \begin{pmatrix} T_{11} & T_{12} & \dots & T_{1n} \\ T_{21} & T_{22} & \dots & T_{2n} \\ \vdots & \vdots & \dots & \vdots \\ T_{n1} & T_{n2} & \dots & T_{nn} \end{pmatrix}, \quad \mathbb{S} = \begin{pmatrix} S_{11} & S_{12} & \dots & S_{1n} \\ S_{21} & S_{22} & \dots & S_{2n} \\ \vdots & \vdots & \dots & \vdots \\ S_{n1} & S_{n2} & \dots & S_{nn} \end{pmatrix}$$

Notice that:

$$\mathbb{A}\mathbb{X}\mathbb{B} = \begin{pmatrix} \sum_{j=1}^n (\alpha_1\beta_1)^{\sigma_j} X^{\sigma_j} & \sum_{j=1}^n (\alpha_1\beta_2)^{\sigma_j} X^{\sigma_j} & \dots & \sum_{j=1}^n (\alpha_1\beta_n)^{\sigma_j} X^{\sigma_j} \\ \sum_{j=1}^n (\alpha_2\beta_1)^{\sigma_j} X^{\sigma_j} & \sum_{j=1}^n (\alpha_2\beta_2)^{\sigma_j} X^{\sigma_j} & \dots & \sum_{j=1}^n (\alpha_2\beta_n)^{\sigma_j} X^{\sigma_j} \\ \vdots & \vdots & \dots & \vdots \\ \sum_{j=1}^n (\alpha_n\beta_1)^{\sigma_j} X^{\sigma_j} & \sum_{j=1}^n (\alpha_n\beta_2)^{\sigma_j} X^{\sigma_j} & \dots & \sum_{j=1}^n (\alpha_n\beta_n)^{\sigma_j} X^{\sigma_j} \end{pmatrix}$$

$$\mathbb{A}\mathbb{Y}\mathbb{B} = \begin{pmatrix} \sum_{j=1}^n (\alpha_1\beta_1)^{\sigma_j} Y^{\sigma_j} & \sum_{j=1}^n (\alpha_1\beta_2)^{\sigma_j} Y^{\sigma_j} & \dots & \sum_{j=1}^n (\alpha_1\beta_n)^{\sigma_j} Y^{\sigma_j} \\ \sum_{j=1}^n (\alpha_2\beta_1)^{\sigma_j} Y^{\sigma_j} & \sum_{j=1}^n (\alpha_2\beta_2)^{\sigma_j} Y^{\sigma_j} & \dots & \sum_{j=1}^n (\alpha_2\beta_n)^{\sigma_j} Y^{\sigma_j} \\ \vdots & \vdots & \dots & \vdots \\ \sum_{j=1}^n (\alpha_n\beta_1)^{\sigma_j} Y^{\sigma_j} & \sum_{j=1}^n (\alpha_n\beta_2)^{\sigma_j} Y^{\sigma_j} & \dots & \sum_{j=1}^n (\alpha_n\beta_n)^{\sigma_j} Y^{\sigma_j} \end{pmatrix}.$$

Observe that the entries of $\mathbb{A}\mathbb{X}\mathbb{B}$ and $\mathbb{A}\mathbb{Y}\mathbb{B}$ are G-equivariant. Hence, there is a well defined homomorphism of K-algebras

$$(2.6)\ \Phi \ :\ K[\mathbb{T}, \mathbb{S}]/(\mathbb{T}\mathbb{S} - I_{rn},\, \mathbb{S}\mathbb{T} - I_{rn}) \ \rightarrow\ \big(M[\mathbb{X}, \mathbb{Y}]/(\mathbb{X}\mathbb{Y} - I_{rn},\, \mathbb{Y}\mathbb{X} - I_{rn})\big)^G$$

$$\mathbb{T} \rightarrow \mathbb{A}\mathbb{X}\mathbb{B}$$

$$\mathbb{S} \rightarrow \mathbb{A}\mathbb{Y}\mathbb{B}$$

The definition of Φ and the form of the entries of matrices $\mathbb{A}\mathbb{X}\mathbb{B}$ and $\mathbb{A}\mathbb{Y}\mathbb{B}$ show (by the same argument as in Lemma 2.4) that the map Φ is surjective. Observe that

$$GL_{rn}/K = spec\ K[\mathbb{T}, \mathbb{S}]/(\mathbb{T}\mathbb{S} - I_{rn},\, \mathbb{S}\mathbb{T} - I_{rn}),$$

$$GL_r/E \ =\ spec\ E[X, Y]/(XY - I_r,\, YX - I_r),$$

where X and Y are $r \times r$ multivariable matrices.

Lemma 2.7. *Consider the group scheme GL_r/E. The map Φ induces a natural isomorphism $R_{E/K}(GL_r) \cong C_E(GL_{rn}/K)$ of closed group subschemes of GL_{rn}/K, where $C_E(GL_{rn}/K)$ is the commutant of E in GL_{rn}/K.*

Proof. Observe that there is a natural M-algebra isomorphism

$$M[\mathbb{X}, \mathbb{Y}]/(\mathbb{X}\mathbb{Y} - I_{rn},\, \mathbb{Y}\mathbb{X} - I_{rn}) \cong A^{\sigma_1} \otimes_M \cdots \otimes_M A^{\sigma_n},$$

where in this case

$$A^{\sigma_j} = M[X,Y]/(XY - I_r,\, YX - I_r) \cong M[X^{\sigma_j}, Y^{\sigma_j}]/(X^{\sigma_j}Y^{\sigma_j} - I_r,\, Y^{\sigma_j}X^{\sigma_j} - I_r).$$

Hence, by Definition 2.3 we get a natural isomorphism of schemes over K :

$$R_{E/K}(GL_r) \cong spec\left(M[\mathbb{X}, \mathbb{Y}]/(\mathbb{X}\mathbb{Y} - I_{rn},\, \mathbb{Y}\mathbb{X} - I_{rn})\right)^G$$

and it follows that Φ induces a closed imbedding of schemes $R_{E/K}(GL_r) \rightarrow GL_{rn}$ over K. Moreover we easily check that $Ker\,\Phi$ is generated by elements $\alpha \circ \mathbb{T} - \mathbb{T} \circ \alpha$ and $\alpha \circ \mathbb{S} - \mathbb{S} \circ \alpha$ for all $\alpha \in E$, where $\circ$ denotes the multiplication in GL_{rn}/K. Note that $C_E(GL_{rn}/K)$ is equal to

$$spec\ K[\mathbb{T}, \mathbb{S}]/(\mathbb{T}\mathbb{S} - I_{rn},\ \mathbb{S}\mathbb{T} - I_{rn},\ \alpha \circ \mathbb{T} - \mathbb{T} \circ \alpha,\ \alpha \circ \mathbb{S} - \mathbb{S} \circ \alpha,\ \forall_{\alpha \in E}). \qquad \Box$$

Remark 2.8. Let E/K be an unramified extension of two local fields. Hence the extension of rings of integers $\mathcal{O}_E/\mathcal{O}_K$ has an integral basis $\alpha_1, \dots, \alpha_n$ of $\mathcal{O}_E$ over $\mathcal{O}_K$ such that the corresponding dual basis $\beta_1, \dots, \beta_n$ with respect to $Tr_{E/K}$ is also a basis of $\mathcal{O}_E$ over $\mathcal{O}_K$ see [A], Chapter 7. Let $R_{\mathcal{O}_E/\mathcal{O}_K}$ be the Weil restriction functor defined analogously to the Weil restriction functor for the extension E/K. Under these assumptions the following Lemmas 2.9 and 2.10 are proven in precisely the same way as Lemmas 2.4 and 2.6.

Lemma 2.9. *Let $V' \subset V$ be a closed imbedding of affine schemes over $\mathcal{O}_E$. Under the assumptions of Remark 2.8 $R_{\mathcal{O}_E/\mathcal{O}_K}(V') \subset R_{\mathcal{O}_E/\mathcal{O}_K}(V)$ is a closed imbedding of affine schemes over $\mathcal{O}_K$.*

Lemma 2.10. *Consider the group scheme $GL_r/\mathcal{O}_E$. Under the assumptions of Remark 2.8 there is a natural isomorphism $R_{\mathcal{O}_E/\mathcal{O}_K}(GL_r) \cong C_{\mathcal{O}_E}(GL_{rn}/\mathcal{O}_K)$ of closed group subschemes of $GL_{rn}/\mathcal{O}_K$, where $C_{\mathcal{O}_E}(GL_{rn}/\mathcal{O}_K)$ is the commutant of $\mathcal{O}_E$ in $GL_{rn}/\mathcal{O}_K$.*

We return to the case of the arbitrary separable field extension E/K of degree n. Every point of $X_0 \in GL_r(E)$ is uniquely determined by the ring homomorphism

$$h_{X_0}\ :\ E[X,Y]/(XY - I_r,\, YX - I_r)\ \rightarrow\ E$$

$$X \mapsto X_0, \quad Y \mapsto Y_0,$$

where Y_0 is the inverse of X_0. This gives immediately the homomorphism

$$h_{\mathbb{T}_0} : K[\mathbb{T}, \mathbb{S}]/(\mathbb{T}\mathbb{S} - I_{rn}, \mathbb{S}\mathbb{T} - I_{rn}) \to K$$

$$\mathbb{T} \mapsto \mathbb{T}_0 = \mathbb{A}\mathbb{X}_0\mathbb{B},$$

$$\mathbb{S} \mapsto \mathbb{S}_0 = \mathbb{A}\mathbb{Y}_0\mathbb{B}$$

where

$$\mathbb{X}_0 = \begin{pmatrix} X_0^{\sigma_1} & 0I_r & \dots & 0I_r \\ 0I_r & X_0^{\sigma_2} & \dots & 0I_r \\ \vdots & \vdots & \dots & \vdots \\ 0I_r & 0I_r & \dots & X_0^{\sigma_n} \end{pmatrix}, \quad \mathbb{Y}_0 = \begin{pmatrix} Y_0^{\sigma_1} & 0I_r & \dots & 0I_r \\ 0I_r & Y_0^{\sigma_2} & \dots & 0I_r \\ \vdots & \vdots & \dots & \vdots \\ 0I_r & 0I_r & \dots & Y_0^{\sigma_n} \end{pmatrix},$$

and the action of σ_i on X_0 and Y_0 is the genuine action on the entries of X_0 and Y_0. Obviously $h_{\mathbb{T}_0}$ determines uniquely the point $\mathbb{T}_0 \in GL_{rn}(K)$ with the inverse $\mathbb{S}_0$.

Definition 2.11. *Assume that $Z = \{X_t;\ t \in T\} \subset GL_r(E)$ is a set of points. We define the corresponding set of points:*

$$Z_\Phi \quad = \quad \{\mathbb{T}_t = \mathbb{A}\mathbb{X}_t\mathbb{B};\ t \in T\} \quad \subset \quad GL_{rn}(K),$$

where

$$\mathbb{X}_t = \begin{pmatrix} X_t^{\sigma_1} & 0I_r & \dots & 0I_r \\ 0I_r & X_t^{\sigma_2} & \dots & 0I_r \\ \vdots & \vdots & \dots & \vdots \\ 0I_r & 0I_r & \dots & X_t^{\sigma_n} \end{pmatrix}.$$

We denote by Z^{alg} the Zariski closure of Z in GL_r/E and by Z_Φ^{alg} the Zariski closure of Z_Φ in GL_{rn}/K.

Proposition 2.12. *We have a natural isomorphism of schemes over K :*

$$R_{E/K}(Z^{alg}) \ \cong \ Z_\Phi^{alg}.$$

Proof. Let

$$J_t = (XY - I_r, YX - I_r, X - X_t, Y - Y_t)$$

be the prime ideal of $E[X, Y]$ corresponding to the point $X_t \in GL_r(E)$. Let

$$J = \bigcap_{t \in T} J_t.$$

By definition $Z^{alg} = spec\,(E[X,Y]/J)$. Let

$$\mathbb{J}_t = (\mathbb{T}\mathbb{S} - I_{rn},\, \mathbb{S}\mathbb{T} - I_{rn},\, \mathbb{T} - \mathbb{A}\mathbb{X}_t\mathbb{B},\, \mathbb{S} - \mathbb{A}\mathbb{Y}_t\mathbb{B})$$

be the prime ideal in $K[\mathbb{T},\mathbb{S}]/(\mathbb{T}\mathbb{S} - I_{rn},\, \mathbb{S}\mathbb{T} - I_{rn})$ corresponding to the point $\mathbb{A}\mathbb{X}_t\mathbb{B} \in GL_{rn}(K)$. Define

$$\mathbb{J} = \bigcap_{t\in T} \mathbb{J}_t.$$

By definition $Z_{\Phi}^{alg} = spec\,(K[\mathbb{T},\mathbb{S}]/\mathbb{J})$. Put $A = E[X,Y]/(XY - I_r,\, YX - I_r)$. Observe that the ring $\overline{A}^G$ is generated as a K-algebra by $\mathbb{A}\mathbb{X}\mathbb{B}$ and $\mathbb{A}\mathbb{Y}\mathbb{B}$, since $\overline{A}$ is generated by $\mathbb{X}$ and $\mathbb{Y}$ as an M-algebra. Define

$$\mathbb{J}'_t = (\mathbb{A}\mathbb{X}\mathbb{B} - \mathbb{A}\mathbb{X}_t\mathbb{B},\, \mathbb{A}\mathbb{Y}\mathbb{B} - \mathbb{A}\mathbb{Y}_t\mathbb{B})$$

which is an ideal of $\overline{A}^G$. Put

$$\mathbb{J}' = \bigcap_{t\in T} \mathbb{J}'_t.$$

We have the following isomorphism induced by Φ.

$$K[\mathbb{T},\mathbb{S}]/\mathbb{J}_t \;\cong\; \overline{A}^G/\,\mathbb{J}'_t \;\cong\; K. \tag{2.13}$$

Hence, $\Phi^{-1}(\mathbb{J}'_t) \;=\; \mathbb{J}_t$ and $\Phi^{-1}(\mathbb{J}') \;=\; \mathbb{J}$. This gives the isomorphism

$$K[\mathbb{T},\mathbb{S}]/\mathbb{J} \;\cong\; \overline{A}^G/\,\mathbb{J}'. \tag{2.14}$$

Let $B = E[X,Y]/J$. There is a natural surjective homomorphism of K-algebras coming from the construction in the proof of Lemma 2.4 (see (2.5)):

$$\overline{A}^G/\,\mathbb{J}' \to \overline{B}^G \tag{2.15}$$

induced by the quotient map $A \to B$. We want to prove that (2.15) is an isomorphism. Observe that there is natural isomorphism of K-algebras:

$$\overline{A}^G/\,\mathbb{J}'_t \;\cong\; \overline{A/J_t}^G \;\cong\; K. \tag{2.16}$$

Consider the following commutative diagram of homomorphisms of K-algebras:

$$\begin{tikzcd} \overline{A}^G/\,\mathbb{J}' \arrow[r] \arrow[d] & \overline{B}^G \arrow[d] \\ \prod_{t\in T} \overline{A}^G/\,\mathbb{J}'_t \arrow[r, "\cong"] & \prod_{t\in T} \overline{A/J_t}^G \end{tikzcd} \tag{2.17}$$

The left vertical arrow is an imbedding by definition of $\mathbb{J}'$ and the bottom horizontal arrow is an isomorphism by (2.16). Hence the top horizontal arrow is an imbedding, i.e., the map (2.15) is an isomorphism. The composition of maps (2.14) and (2.15) gives a natural isomorphism of K-algebras

$$K[\mathbb{T},\mathbb{S}]/\mathbb{J} \;\cong\; \overline{B}^G. \tag{2.18}$$

But $Z_{\Phi}^{alg} = spec\,(K[\mathbb{T},\mathbb{S}]/\mathbb{J})$. In addition, $Z^{alg} = spec\,B$, hence $R_{E/K}(Z^{alg}) = spec\,\overline{B}^G$ and Proposition 2.12 follows by (2.18). □

Remark 2.19. If Z is a subgroup of $GL_r(E)$, then Z_{Φ} is a subgroup of $GL_{rn}(K)$. In this case Z^{alg} is a closed algebraic subgroup of GL_r/E and Z_{Φ}^{alg} is a closed algebraic subgroup of GL_{rn}/K.

Definition 2.20. *Let $H = spec\,A$ be an affine algebraic group scheme defined over E and $\mathfrak{h}$ its Lie algebra. We define $\mathfrak{g} = R_{E/K}\mathfrak{h}$ to be the Lie algebra obtained from $\mathfrak{h}$ by considering it over K with the same bracket.*

Lemma 2.21. *There is the following equality of Lie algebras*

$$\mathcal{L}ie(R_{E/K}H) = R_{E/K}\mathfrak{h}.$$

Proof. Let $n = [E : K]$ and $G = Gal(E/K)$. Since H is an algebraic group $\mathfrak{h} = \mathcal{D}er(A)$ is the Lie algebra of derivations of the algebra A of functions on H [H1]. Let $\phi : Der(A) \rightarrow Der(\bar{A})$ be the homomorphism of Lie algebras (considered over E) given by the following formula:

$$\phi(\delta) = \Sigma_{i=1}^{n} id \otimes \cdots \otimes id \otimes \delta_i \otimes id \otimes \cdots \otimes id,$$

where $\delta_i = \delta \otimes 1$ as an element of $Der(A^{\sigma_i})$. Recall that $A^{\sigma_i} = A \otimes_{E,\sigma_i} M$. If $\sigma \in G$ and $\sigma(a_1 \otimes \cdots \otimes a_n) = \sigma(a_{k_1}) \otimes \cdots \otimes \sigma(a_{k_n})$ one readily sees that $\delta_j(\sigma(a_{k_j})) = \sigma(\delta_{k_j}(a_{k_j}))$ and therefore $\phi(\delta)$ is G-equivariant i.e., $\phi(\delta) \in Der(\bar{A}^G)$. It is easy to see that $\phi(\delta)$ as an element of $Der(\bar{A})$ is nontrivial if δ is nontrivial. Since $\phi(\delta)$ is M-linear and $\bar{A}^G \otimes_K M = \bar{A}$, we see that $\phi(\delta)$ is a nontrivial element of $Der(\bar{A}^G) = \mathcal{L}ie(R_{E/K}H)$. On the other hand, observe that

$$\mathcal{L}ie(R_{E/K}H) \otimes_K \bar{K} = \mathcal{L}ie(R_{E/K}H \otimes_K \bar{K}) =$$
$$= \mathcal{L}ie(\bar{H} \times_K \cdots \times_K \bar{H}) = (\oplus \mathfrak{h}) \otimes_E \bar{K} = \mathfrak{g} \otimes_K \bar{K}.$$

This shows that $\mathcal{L}ie(R_{E/K}H)$ and $R_{E/K}\mathfrak{h}$ have the same dimensions and therefore are equal. □

Lemma 2.22. *Let $\mathfrak{g}$ be a Lie algebra over E and let $\mathfrak{g}'$ be its derived algebra. Then*

$$R_{E/K}(\mathfrak{g}') = (R_{E/K}(\mathfrak{g}))'$$

Proof. This follows immediately from the fact that $R_{E/K}(\mathfrak{g})$ and $\mathfrak{g}$ have the same Lie bracket (cf. Definition 2.20) □

Lemma 2.23. *If G is a connected, algebraic group over E of characteristic 0, then*

$$R_{E/K}(G') = (R_{E/K}G)'$$

Proof. We have the following identities:

$$Lie((R_{E/K}(G))') = (Lie(R_{E/K}(G)))' = (R_{E/K}(Lie(G)))' =$$

$$= R_{E/K}((Lie(G))') = R_{E/K}(Lie(G')) = Lie(R_{E/K}(G'))$$

The first and the fourth equality follow from Corollary on p.75 of [H1]. The second and fifth equality follow from Lemma 2.21. The third equality follows from Lemma 2.22. The Lemma follows by Theorem on p. 87 of [H1] and Proposition on p. 110 of [H1]. □

3. Some remarks on bilinear forms.

Let E be a finite extension of $\mathbb{Q}$ of degree e. Let $E_l = E \otimes \mathbb{Q}_l$ and $\mathcal{O}_{E_l} = \mathcal{O}_E \otimes \mathbb{Z}_l$. Hence $E_l = \prod_{\lambda | l} E_\lambda$ and $\mathcal{O}_{E_l} = \prod_{\lambda | l} O_\lambda$. Let $\mathcal{O}'_\lambda$ be the dual to $\mathcal{O}_\lambda$ with respect to the trace $Tr_{E_\lambda/\mathbb{Q}_l}$. For $l \gg 0$ we have $\mathcal{O}'_\lambda = \mathcal{O}_\lambda$ see [A], Chapter 7. From now on we take l big enough to ensure that $\mathcal{O}'_\lambda = \mathcal{O}_\lambda$ for all primes λ in $\mathcal{O}_E$ over l and that an abelian variety A we consider, has good reduction at all primes in $\mathcal{O}_F$ over l. The following lemma is the integral version of the sublemma 4.7 of [D].

Lemma 3.1. *Let T_1 and T_2 be finitely generated, free $\mathcal{O}_{E_l}$-modules. For any $\mathbb{Z}_l$-bilinear (resp. nondegenerate $\mathbb{Z}_l$-bilinear) map*

$$\psi_l \,:\, T_1 \times T_2 \to \mathbb{Z}_l$$

such that $\psi_l(ev_1, v_2) = \psi_l(v_1, ev_2)$ for all $e \in \mathcal{O}_{E_l}, v_1 \in T_1, v_2 \in T_2$, there is a unique $\mathcal{O}_{E_l}$-bilinear (resp. nondegenerate $\mathcal{O}_{E_l}$-bilinear) map

$$\phi_l \,:\, T_1 \times T_2 \to \mathcal{O}_{E_l}$$

such that $Tr_{E_l/\mathbb{Q}_l}(\phi_l(v_1, v_2)) = \psi_l(v_1, v_2)$ for all $v_1 \in T_1$ and $v_2 \in T_2$.

Proof. Similary to Sublemma 4.7, [D] we observe that the map

$$Tr_{E_l/\mathbb{Q}_l} \,:\, Hom_{\mathcal{O}_{E_l}}(T_1 \otimes_{\mathcal{O}_{E_l}} T_2 \,; \mathcal{O}_{E_l}) \to Hom_{\mathbb{Z}_l}(T_1 \otimes_{\mathcal{O}_{E_l}} T_2 \,; \mathbb{Z}_l)$$

is an isomorphism since it is a surjective map of torsion free $\mathbb{Z}_l$-modules of the same $\mathbb{Z}_l$-rank. The surjectivity of $Tr_{E_l/\mathbb{Q}_l}$ can be seen as follows. The $\mathbb{Z}_l$-basis of the module $T_1 \otimes_{\mathcal{O}_{E_l}} T_2$ is given by

$$\mathcal{B} = \big((0, \dots, 0, \alpha_k^\lambda, 0, \dots, 0) e_i \otimes e'_j\big)$$

where $(0, \ldots, 0, \alpha_k^\lambda, 0, \ldots, 0) \in \prod_{\lambda | l} \mathcal{O}_\lambda$ and α_k^λ is an element of a basis of $\mathcal{O}_\lambda$ over $\mathbb{Z}_l$ and e_i (resp. e'_j) is an element of the standard basis of T_1 (resp. T_2) over $\mathcal{O}_{E_l}$. Let $\psi^\lambda_{k,i,j} \in Hom_{\mathbb{Z}_l}(T_1 \otimes_{\mathcal{O}_{E_l}} T_2\,;\mathbb{Z}_l)$ be the homomorphism which takes value 1 on the element $(0, \ldots, 0, \alpha_k^\lambda, 0, \ldots, 0) e_i \otimes e'_j$ of the basis $\mathcal{B}$ and takes value 0 on the remaining elements of the basis $\mathcal{B}$. Let us take $\phi_{i,j} \in Hom_{\mathcal{O}_{E_l}}(T_1 \otimes_{\mathcal{O}_{E_l}} T_2\,;\mathcal{O}_{E_l})$ such that

$$\phi_{i,j}(e_r \otimes e'_s) = \begin{cases} 1 & \text{if } i = r \text{ and } j = s \\ 0 & \text{if } i \neq r \text{ or } j \neq s \end{cases}$$

Then for each k there exist elements (the dual basis) $\beta_k^\lambda \in \mathcal{O}_\lambda$ such that $Tr_{E_\lambda/\mathbb{Q}_l}(\beta_k^\lambda \alpha_n^\lambda) = \delta_{k,n}$. If we put $\phi^\lambda_{i,j,k} = (0, \ldots, 0, \beta_k^\lambda, 0, \ldots, 0)\phi_{i,j}$ then clearly $Tr_{E_l/\mathbb{Q}_l}(\phi^\lambda_{i,j,k}(t_1, t_2)) = \psi^\lambda_{i,j,k}(t_1, t_2)$. Hence the proof is finished since the elements $\psi^\lambda_{i,j,k}(t_1, t_2)$ form a basis of $Hom_{\mathbb{Z}_l}(T_1 \otimes_{\mathcal{O}_{E_l}} T_2\,;\mathbb{Z}_l)$ over $\mathbb{Z}_l$. □

Consider the case $T_1 = T_2$ and put $T_l = T_1 = T_2$. Assume in addition that ψ_l is nondegenerate. Let

$$\overline{\psi}_l \,:\, T_l / l\, T_l \times T_l / l\, T_l \to \mathbb{Z}/l$$

be the $\mathbb{Z}/l$-bilinear pairing obtained by reducing the form ψ_l modulo l. Define

$$T_\lambda = e_\lambda T_l \cong T_l \otimes_{\mathcal{O}_{E_l}} \mathcal{O}_\lambda$$

$$V_\lambda = T_\lambda \otimes_{\mathcal{O}_\lambda} E_\lambda$$

where e_λ is the standard idempotent corresponding to the decomposition $\mathcal{O}_{E_l} = \prod_\lambda \mathcal{O}_\lambda$. Let $\pi_\lambda \,:\, \mathcal{O}_{E_l} \to \mathcal{O}_\lambda$ be the natural projection. We can define an $\mathcal{O}_\lambda$-nondegenerate bilinear form as follows:

$$\psi_\lambda \,:\, T_\lambda \times T_\lambda \to \mathcal{O}_\lambda$$

$$\psi_\lambda(e_\lambda v_1, e_\lambda v_2) = \pi_\lambda(\phi_l(v_1, v_2))$$

for any $v_1, v_2 \in T_l$. Put $k_\lambda = \mathcal{O}_\lambda / \lambda\, \mathcal{O}_\lambda$. This gives the k_λ-bilinear form $\overline{\psi}_\lambda = \psi_\lambda \otimes_{\mathcal{O}_\lambda} k_\lambda$

$$\overline{\psi}_\lambda \,:\, T_\lambda / \lambda\, T_\lambda \,\times\, T_\lambda / \lambda\, T_\lambda \to k_\lambda.$$

We also have the E_λ-bilinear form $\psi^0_\lambda := \psi_\lambda \otimes_{\mathcal{O}_\lambda} E_\lambda$

$$\psi^0_\lambda \,:\, V_\lambda \times V_\lambda \to E_\lambda.$$

Lemma 3.2. *Assume that the form $\overline{\psi}_l$ is nondegenerate. Then the forms $\overline{\psi}_\lambda$, ψ_λ and ψ_λ^0 are nondegenerate for each $\lambda | l$.*

Proof. First we prove that $\overline{\psi}_\lambda$ is nondegenerate for all $\lambda | l$. Assume that $\overline{\psi}_\lambda$ is degenerate for some λ. Without loss of generality we can assume that the left radical of $\overline{\psi}_\lambda$ is nonzero. So there is a nonzero vector $e_\lambda v_0 \in T_\lambda$ (for some $v_0 \in T_l$) which maps to a nonzero vector in $T_\lambda / \lambda T_\lambda$ such that $\psi_\lambda(e_\lambda v_0,\, e_\lambda w) \in \lambda\, \mathcal{O}_\lambda$ for all $w \in T_l$. Now use the decomposition $T_l = \oplus_\lambda T_\lambda$, Lemma 3.1 and the $\mathcal{O}_{E_l}$-linearity of ϕ_l to observe that for each $w \in T_l$

$$\psi_l(e_\lambda v_0,\, w) = Tr_{E_l/\mathbb{Q}_l}(\phi_l(e_\lambda v_0, \sum_{\lambda'} e_{\lambda'} w)) = Tr_{E_\lambda/\mathbb{Q}_l} \psi_\lambda(e_\lambda v_0,\, e_\lambda w) \in l\mathbb{Z}_l.$$

This contradicts the assumption that $\overline{\psi}_l$ is nondegenerate.
Similarly, but in an easier way, we prove that ψ_λ is nondegenerate. From this it immediately follows that ψ_λ^0 is nondegenerate. □

4. Auxiliary facts about abelian varieties.

Let A/F be a principally polarized, simple abelian variety of dimension g with the polarization defined over F. Put $\mathcal{R} = End_{\bar{F}}(A)$ We assume that $End_{\bar{F}}(A) = End_F(A)$, hence the actions of $\mathcal{R}$ and G_F on $A(\overline{F})$ commute. Put $D = End_{\bar{F}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. The ring $\mathcal{R}$ is an order in D. Let E_1 be the center of D and let

$$E := \{a \in E_1;\ a' = a\},$$

where $'$ is the Rosati involution. Let $\mathcal{R}_D$ be a maximal order in D containing $\mathcal{R}$. Put $\mathcal{O}_E^0 := \mathcal{R} \cap E$. The ring $\mathcal{O}_E^0$ is an order in E. Take l that does not divide the index $[\mathcal{R}_D : \mathcal{R}]$. Then $\mathcal{R}_D \otimes_{\mathbb{Z}} \mathbb{Z}_l = \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_l$ and $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_l = \mathcal{O}_E^0 \otimes_{\mathbb{Z}} \mathbb{Z}_l$

The polarization of A gives a $\mathbb{Z}_l$-bilinear, nondegenerate, alternating pairing

$$\psi_l \,:\, T_l(A) \times T_l(A) \to \mathbb{Z}_l. \tag{4.1}$$

Because A has the principal polarization, for any endomorphism $\alpha \in \mathcal{R}$ we get $\alpha' \in \mathcal{R}$, (see [Mi] chapter 13 and 17) where α' is the image of α by the Rosati involution. Hence for any $v, w \in T_l(A)$ we have $\psi_l(\alpha v, w) = \psi_l(v, \alpha' w)$ (see loc. cit.).

Remark 4.2. Notice that if an abelian variety were not principally polarized, one would have to assume that l does not divide the degree of the polarization of A, to get $\alpha' \otimes 1 \in \mathcal{R} \otimes \mathbb{Z}_l$ for $\alpha \in \mathcal{R}$.

By Lemma 3.1 there is a unique nondegenerate, $\mathcal{O}_{E_l}$-bilinear pairing

$$\phi_l \,:\, T_l(A) \times T_l(A) \to \mathcal{O}_{E_l} \tag{4.3}$$

such that $Tr_{E_l/\mathbb{Q}_l}(\phi_l(v_1, v_2)) = \psi_l(v_1, v_2)$. As in the general case define

$$T_\lambda(A) = e_\lambda T_l(A) \cong T_l(A) \otimes_{\mathcal{O}_{E_l}} \mathcal{O}_\lambda$$

$$V_\lambda(A) = T_\lambda(A) \otimes_{\mathcal{O}_\lambda} E_\lambda.$$

Note that $T_\lambda(A)/\lambda T_\lambda(A) \cong A[\lambda]$ as $k_\lambda[G_F]$-modules.
Again as in the general case define nondegenerate, $\mathcal{O}_\lambda$-bilinear form

$$\psi_\lambda \,:\, T_\lambda(A) \times T_\lambda(A) \to \mathcal{O}_\lambda \tag{4.4}$$

$$\psi_\lambda(e_\lambda v_1, e_\lambda v_2) = \pi_\lambda(\phi_l(v_1, v_2))$$

for any $v_1, v_2 \in T_l(A)$, where $\pi_\lambda : \mathcal{O}_{E_l} \to \mathcal{O}_\lambda$ is the natural projection. The form ψ_λ gives the forms:

$$\overline{\psi}_\lambda \,:\, A[\lambda] \times A[\lambda] \to k_\lambda. \tag{4.5}$$

$$\psi_\lambda^0 \,:\, V_\lambda(A) \times V_\lambda(A) \to E_\lambda. \tag{4.6}$$

Notice that all the bilinear forms $\psi_\lambda, \overline{\psi}_\lambda$ and ψ_λ^0 are alternating forms. For l relatively prime to the degree of polarization the form ψ_l is nondegenerate. Hence by lemma 3.2 the forms $\psi_\lambda, \overline{\psi}_\lambda$ and ψ_λ^0 are nondegenerate.

Lemma 4.7. *Let $\chi_\lambda : G_F \to \mathbb{Z}_l \subset \mathcal{O}_\lambda$ be the composition of the cyclotomic character with the natural imbedding $\mathbb{Z}_l \subset \mathcal{O}_\lambda$.*

(i) *For any $\sigma \in G_F$ and all $v_1, v_2 \in T_\lambda(A)$*

$$\psi_\lambda(\sigma v_1, \sigma v_2) = \chi_\lambda(\sigma)\psi_\lambda(v_1, v_2).$$

(ii) *For any $\alpha \in \mathcal{R}$ and all $v_1, v_2 \in T_\lambda(A)$*

$$\psi_\lambda(\alpha v_1, v_2) = \psi_\lambda(v_1, \alpha' v_2).$$

Proof. The proof is the same as the proof of Lemma 2.3 in [C2]. □

Remark 4.8. After tensoring appropriate objects with $\mathbb{Q}_l$ in lemmas 3.1 and 4.6 we obtain Lemmas 2.2 and 2.3 of [C2].

Let A/F be an abelian variety defined over a number field F such that $End_{\bar{F}}(A) = End_F(A)$. We introduce some notation. Let G_{l^∞}, G_l, $G_{l^\infty}^0$ denote the images of the corresponding representations:

$$\rho_l \,:\, G_F \to GL(T_l(A)) \cong GL_{2g}(\mathbb{Z}_l),$$

$$\overline{\rho_l} \,:\, G_F \to GL(A[l]) \cong GL_{2g}(\mathbb{F}_l),$$

$$\rho_l \otimes \mathbb{Q}_l \,:\, G_F \to GL(V_l(A)) \cong GL_{2g}(\mathbb{Q}_l).$$

Let $\mathcal{G}_l^{alg}$, (G_l^{alg} resp.) denote the Zariski closure of the image of the representation ρ_l, ($\rho_l \otimes \mathbb{Q}_l$, resp.) in $GL_{2g}/\mathbb{Z}_l$, ($GL_{2g}/\mathbb{Q}_l$, resp). We define $G(l)^{alg}$ to be the special fiber of the $\mathbb{Z}_l-$scheme $\mathcal{G}_l^{alg}$.

Due to our assumptions on the G_F-action and the properties of the forms $\psi_\lambda, \overline{\psi}_\lambda$ and ψ_λ^0 we get:

$$G_{l^\infty} \subset \mathcal{G}_l^{alg}(\mathbb{Z}_l) \subset \prod_{\lambda | l} GSp_{T_\lambda(A)}(\mathcal{O}_\lambda) \subset GL_{T_l(A)}(\mathbb{Z}_l) \tag{4.9}$$

$$G_l \subset G(l)^{alg}(\mathbb{F}_l) \subset \prod_{\lambda | l} GSp_{A[\lambda]}(k_\lambda) \subset GL_{A[l]}(\mathbb{F}_l) \tag{4.10}$$

$$G_{l^\infty}^0 \subset G_l^{alg}(\mathbb{Q}_l) \subset \prod_{\lambda | l} GSp_{V_\lambda(A)}(E_\lambda) \subset GL_{V_l(A)}(\mathbb{Q}_l). \tag{4.11}$$

Before we proceed further let us state and prove some general lemmas concerning l-adic representations. Let $K/\mathbb{Q}_l$ be a local field extension and $\mathcal{O}_K$ the ring of integers in K. Let T be a finitely generated, free $\mathcal{O}_K$-module and let $V = T \otimes_{\mathcal{O}_K} K$. Consider a continuous representation $\rho : G_F \rightarrow GL(T)$ and the induced representation $\rho^0 = \rho \otimes K : G_F \rightarrow GL(V)$. Since G_F is compact and ρ^0 is continuous, the subgroup $\rho^0(G_F)$ of $GL(V)$ is closed. By [Se7], LG. 4.5, $\rho^0(G_F)$ is an analytic subgroup of $GL(V)$.

Lemma 4.12. *Let $\mathfrak{g}$ be the Lie algebra of the group $\rho^0(G_F)$*

(i) *There is an open subgroup $U_0 \subset \rho^0(G_F)$ such that*

$$End_{U_0}(V) = End_{\mathfrak{g}}(V).$$

(ii) *For all open subgroups $U \subset \rho^0(G_F)$ we have*

$$End_U(V) \subset End_{\mathfrak{g}}(V).$$

(iii) *Taking union over all open subgroups $U \subset \rho^0(G_F)$ we get*

$$\bigcup_U End_U(V) = End_{\mathfrak{g}}(V).$$

Proof. (i) Note that for any open subgroup $\tilde{U}$ of $\mathfrak{g}$ we have

$$End_{\tilde{U}}\,(V) \;=\; End_{\mathfrak{g}}\,(V) \tag{4.13}$$

because $K\,\tilde{U} \;=\; \mathfrak{g}$. By [B], Prop. 3, III.7.2, for some open $\tilde{U} \subset \mathfrak{g}$, there is an exponential map

$$exp\,:\,\tilde{U}\,\to \rho^0(G_F)$$

which is an analytic isomorphism and such that $exp\,(\tilde{U})$ is an open subgroup of $\rho^0(G_F)$. The exponential map can be expressed by the classical power series for $exp\,(t)$. On the other hand by [B], Prop. 10, III.7.6, for some open $U \subset \rho^0(G_F)$, there is a logarithmic map

$$log\,:\,U\,\to \mathfrak{g}$$

which is an analytic isomorphism and the inverse of exp. The logarithmic map can be expressed by the classical power series for $\ln t$. Hence, we can choose $\tilde{U}_0$ such that $U_0 = exp\,(\tilde{U}_0)$ and $log\,(U_0) = \tilde{U}_0$. This gives

$$End_{U_0}\,(V) \;=\; End_{\tilde{U}_0}\,(V). \tag{4.14}$$

and (i) follows by (4.13) and (4.14).

(ii) Observe that for any open $U \subset \rho^0(G_F)$ we have

$$End_U\,(V) \;\subset\; End_{U_0 \cap U}\,(V).$$

Hence (ii) follows by (i).

(iii) Follows by (i) and (ii). □

Lemma 4.15. *Let A/F be an abelian variety over F such that $End_F\,(A) = End_{\overline{F}}\,(A)$. Then*

$$End_{G_F}\,(V_l(A)) = End_{\mathfrak{g}_l}\,(V_l(A)).$$

Proof. By the result of Faltings [Fa], Satz 4,

$$End_L\,(A) \otimes \mathbb{Q}_l = End_{G_L}\,(V_l(A))$$

for any finite extension L/F. By the assumption $End_F\,(A) = End_L\,(A)$. Hence

$$End_{G_F}\,(V_l(A)) = End_{U'}\,(V_l(A))$$

for any open subgroup U' of G_F. So the claim follows by Lemma 4.12 (iii). □

Let A be a simple abelian variety defined over F and E be the center of the algebra $D = End_F(A) \otimes \mathbb{Q}$. Let $\lambda | l$ be a prime of $\mathcal{O}_E$ over l. Consider the following representations.

$$\rho_\lambda\,:\,G_F \to GL(T_\lambda(A)),$$
$$\overline{\rho_\lambda}\,:\,G_F \to GL(A[\lambda]),$$
$$\rho_\lambda \otimes_{\mathcal{O}_\lambda} E_\lambda\,:\,G_F \to GL(V_\lambda(A)),$$

where $\lambda | l$. Let $\mathcal{G}_\lambda^{alg}$, (G_λ^{alg} resp.) denote the Zariski closure of the image of the representation ρ_λ, ($\rho_\lambda \otimes E_\lambda$ resp.) in $GL_{T_\lambda(A)}/\mathcal{O}_\lambda$, ($GL_{V_\lambda(A)}/E_\lambda$ resp.) We define $G(\lambda)^{alg}$ to be the special fiber of the $\mathcal{O}_\lambda$-scheme $\mathcal{G}_\lambda^{alg}$.

Theorem 4.16. *Let A be a simple abelian variety with the property that $\mathcal{R} = End_{\bar{F}}(A) = End_F(A)$. Let $\mathcal{R}_\lambda = \mathcal{R} \otimes_{\mathcal{O}_E^0} \mathcal{O}_\lambda$ and let $D_\lambda = D \otimes_E E_\lambda$. Then*

(i) $End_{\mathcal{O}_\lambda[G_F]}(T_\lambda(A)) \cong \mathcal{R}_\lambda$

(ii) $End_{R_\lambda[G_F]}(V_\lambda(A)) \cong D_\lambda$

(iii) $End_{k_\lambda[G_F]}(A[\lambda]) \cong \mathcal{R}_\lambda \otimes_{\mathcal{O}_\lambda} k_\lambda$ *for* $l \gg 0$.

Proof. It follows by [Fa], Satz 4 and [Za], Cor. 5.4.5. □

Lemma 4.17. *Let K be a field and let R be a unital K-algebra. Put $D = End_R(M)$ and let L be a subfield of the center of D. Assume that L/K is a finite separable extension. If M is a semisimple R-module then M is also a semisimple $R \otimes_K L$-module with the obvious action of $R \otimes_K L$ on M.*

Proof. Take $\alpha \in L$ such that $L = K(\alpha)$. Let $[L : K] = n$. Let us write $M = \oplus_i M_i$ where all M_i are simple R modules. For any i we put $\tilde{M_i} = \sum_{k=0}^{n-1} \alpha^k M_i$. Then $\tilde{M_i}$ is an $R \otimes_K L$-module. Because M_i is a simple R-module we can write

$$\tilde{M_i} = \bigoplus_{k=0}^{m-1} \alpha^k M_i,$$

for some m. Observe that if $m = 1$, then $\tilde{M_i}$ is obviously a simple $R \otimes_K L$-module. If $m{>}1$, we pick any simple R-submodule $N_i \subset \tilde{M_i}$, $N_i \neq M_i$. There is an R- isomorphism $\phi : M_i \to N_i$ by semisimplicity of $\tilde{M_i}$. We can write $M = M_i \oplus N_i \oplus M'$, where M' is an R-submodule of M. Define $\Psi \in Aut_R(M) \subset End_R(M)$ by $\Psi|_{M_i} = \phi$, $\Psi|_{N_i} = \phi^{-1}$ and $\Psi|_{M'} = Id_{M'}$. Note that

$$\Psi(\bigoplus_{k=0}^{m-1} \alpha^k M_i) = \bigoplus_{k=0}^{m-1} \alpha^k N_i \tag{4.18}$$

since α is in the center of D. Hence $\tilde{M_i} = \bigoplus_{k=0}^{m-1} \alpha^k N_i$ by the classification of semisimple R-modules. We conclude that $\tilde{M_i}$ is a simple $R \otimes_K L$-module. Indeed, if $N \subset \tilde{M_i}$ were a nonzero $R \otimes_K L$-submodule of $\tilde{M_i}$ then we could pick any simple R-submodule $N_i \subset N$. If $N_i = M_i$ then $N = \tilde{M_i}$. If $N_i \neq M_i$ then by (4.18) $\tilde{M_i} = \bigoplus_{k=0}^{m-1} \alpha^k N_i \subset N$. Since $M = \sum_i \tilde{M_i}$, we see that M is a semisimple $R \otimes_K L$-module. □

Theorem 4.19. *Let A be a simple abelian variety with the property that $\mathcal{R} = End_{\bar{F}}(A) = End_F(A)$. Let $\mathcal{R}_\lambda = \mathcal{R} \otimes_{\mathcal{O}_E^0} \mathcal{O}_\lambda$ and let $D_\lambda = D \otimes_E E_\lambda$. Then G_F acts on $V_\lambda(A)$ and $A[\lambda]$ semisimply and G_λ^{alg} and $G(\lambda)^{alg}$ are reductive algebraic groups. The scheme $\mathcal{G}_\lambda^{alg}$ is a reductive group scheme over $\mathcal{O}_\lambda$ for l big enough.*

Proof. It follows by [Fa], Theorem 3 and our Lemma 4.17. The last statement follows by [LP1], Proposition 1.3, see also [Wi], Theoreme 1. □

5. Abelian varieties of type I and II.

In this section we work with abelian varieties of type I and II in the Albert's classification list of division algebras with involution [M], p. 201, i.e. $E \subset D = End_{\bar{F}}(A) \otimes_Z \mathbb{Q}$ is the center of D and E is a totally real extension of $\mathbb{Q}$ of degree e. To be more precise D is either E (type I) or an indefinite quaternion algebra with the center E, such that $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i=1}^{e} M_{2,2}(\mathbb{R})$ (type II). In the first part of this section we prove integral versions of the results of Chi [C2] for abelian varieties of type II. Let l be a sufficiently large prime number that does not divide the index $[\mathcal{R}_D : \mathcal{R}]$ and such that $D \otimes_E E_\lambda$ splits over E_λ for any prime λ in $\mathcal{O}_E$ over l. Hence, $D_\lambda = M_{2,2}(E_\lambda)$. Then by [R, Corollary 11.2 p. 132 and Theorem 11.5 p. 133] the ring R_λ is a maximal order in D_λ. So by [R] Theorem 8.7 p. 110 we get $R_\lambda = M_{2,2}(\mathcal{O}_\lambda)$, hence $R_\lambda \otimes_{\mathcal{O}_\lambda} k_\lambda = M_{2,2}(k_\lambda)$. Similarly to [C2] we put

$$t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad u = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $e = \frac{1}{2}(1+t)$, $f = \frac{1}{2}(1+u)$, $\mathcal{X} = e\, T_\lambda(A)$, $\mathcal{Y} = (1-e)\, T_\lambda(A)$, $\mathcal{X}' = f\, T_\lambda(A)$, $\mathcal{Y}' = (1-f)\, T_\lambda(A)$. Put $X = \mathcal{X} \otimes_{\mathcal{O}_\lambda} E_\lambda$, $X' = \mathcal{X}' \otimes_{\mathcal{O}_\lambda} E_\lambda$, $Y = \mathcal{Y} \otimes_{\mathcal{O}_\lambda} E_\lambda$, $Y' = \mathcal{Y}' \otimes_{\mathcal{O}_\lambda} E_\lambda$, $\overline{\mathcal{X}} = \mathcal{X} \otimes_{\mathcal{O}_\lambda} k_\lambda$, $\overline{\mathcal{X}}' = \mathcal{X}' \otimes_{\mathcal{O}_\lambda} k_\lambda$, $\overline{\mathcal{Y}} = \mathcal{Y} \otimes_{\mathcal{O}_\lambda} k_\lambda$, $\overline{\mathcal{Y}}' = \mathcal{Y}' \otimes_{\mathcal{O}_\lambda} k_\lambda$. Because $ueu = 1-e$, the matrix u gives an $\mathcal{O}_\lambda[G_F]$-isomorphism between $\mathcal{X}$ and $\mathcal{Y}$, hence it yields an $E_\lambda[G_F]$-isomorphism between X and Y and a $k_\lambda[G_F]$-isomorphism between $\overline{\mathcal{X}}$ and $\overline{\mathcal{Y}}$. Multiplication by t gives an $\mathcal{O}_\lambda[G_F]$-isomorphism between $\mathcal{X}'$ and $\mathcal{Y}'$, hence it yields an $E_\lambda[G_F]$-isomorphism between X' and Y' and a $k_\lambda[G_F]$-isomorphism between $\overline{\mathcal{X}}'$ and $\overline{\mathcal{Y}}'$. Observe that

$$End_{\mathcal{O}_\lambda[G_F]}(\mathcal{X}) \cong End_{\mathcal{O}_\lambda[G_F]}(\mathcal{X}') \cong \mathcal{O}_\lambda \tag{5.1}$$

$$End_{E_\lambda[G_F]}(X) \cong End_{E_\lambda[G_F]}(X') \cong E_\lambda \tag{5.2}$$

$$End_{k_\lambda[G_F]}(\overline{\mathcal{X}}) \cong End_{k_\lambda[G_F]}(\overline{\mathcal{X}}') \cong k_\lambda. \tag{5.3}$$

So the representations of G_F on the spaces X, Y, X', Y' (resp. $\overline{\mathcal{X}}, \overline{\mathcal{Y}}, \overline{\mathcal{X}}', \overline{\mathcal{Y}}'$) are absolutely irreducible over E_λ (resp. over k_λ). Hence, the bilinear form ψ_λ^0 cf. (4.4) (resp. $\overline{\psi}_\lambda$ cf. (4.5)) when restricted to any of the spaces X, X', Y, Y', (resp. spaces $\overline{\mathcal{X}}, \overline{\mathcal{X}}', \overline{\mathcal{Y}}, \overline{\mathcal{Y}}'$) is either nondegenerate or isotropic.

We obtain the integral version of Theorem A of [C2].

Theorem 5.4. *If A is of type II, then there is a free $\mathcal{O}_\lambda$-module $\mathcal{W}_\lambda(A)$ of rank $2h$ such that*

(i) *we have an isomorphism of $\mathcal{O}_\lambda[G_F]$- modules $T_\lambda(A) \cong \mathcal{W}_\lambda(A) \oplus \mathcal{W}_\lambda(A)$*

(ii) *there is an alternating pairing $\psi_\lambda : \mathcal{W}_\lambda(A) \times \mathcal{W}_\lambda(A) \to \mathcal{O}_\lambda$*

(ii') *the induced alternating pairing $\psi_\lambda^0 : W_\lambda(A) \times W_\lambda(A) \to E_\lambda$ is nondegenerate, where $W_\lambda(A) = \mathcal{W}_\lambda(A) \otimes_{\mathcal{O}_\lambda} E_\lambda$*

(ii") *the induced alternating pairing $\overline{\psi}_\lambda : \overline{\mathcal{W}}_\lambda(A) \times \overline{\mathcal{W}}_\lambda(A) \to k_\lambda$ is nondegenerate, where $\overline{\mathcal{W}}_\lambda(A) = \mathcal{W}_\lambda(A) \otimes_{\mathcal{O}_\lambda} k_\lambda$.*

The pairings in (ii), (ii') and (ii") are compatible with the G_F-action in the same way as the pairing in Lemma 4.7 (i).

Proof. (ii') is proven in [C2], while (i) and (ii) are straightforward generalizations of the arguments in *loc. cit.* The bilinear pairing ϕ_l is nondegenerate, hence the bilinear pairing $\overline{\phi}_l$ is nondegenerate, since the abelian variety A is principally polarized by assumption. (Actually $\overline{\phi}_l$ is nondegenerate for any abelian variety with polarization degree prime to l). So, by Lemma 3.2 the form $\overline{\psi}_\lambda$ is nondegenerate for all λ hence simultaneously the forms ψ_λ^0 and $\overline{\psi}_\lambda$ are nondegenerate. Now we finish the proof of (ii") arguing for $A[\lambda]$ similarly as it is done for V_λ in [C2], Lemma 3.3. □

From now on we work with the abelian varieties of type either I or II. We assume that the field F of definition of A is such that G_l^{alg} is a connected algebraic group.
Let us put

$$T_\lambda = \begin{cases} T_\lambda(A) & \text{if } A \text{ is of type I} \\ \\ \mathcal{W}_\lambda(A)\,, & \text{if } A \text{ is of type II} \end{cases} \tag{5.5}$$

Let $V_\lambda = T_\lambda \otimes_{\mathcal{O}_\lambda} E_\lambda$ and $A_\lambda = V_\lambda/T_\lambda$. With this notation we have:

$$V_l(A) = \begin{cases} \bigoplus_{\lambda|l} V_\lambda & \text{if } A \text{ is of type I} \\ \\ \bigoplus_{\lambda|l} \big(V_\lambda \oplus V_\lambda\big)\,, & \text{if } A \text{ is of type II} \end{cases} \tag{5.6}$$

We put

$$V_l \;=\; \bigoplus_{\lambda|l} V_\lambda \tag{5.7}$$

Let V_{Φ_λ} be the space V_λ considered over $\mathbb{Q}_l$. We define $\rho_{\Phi_\lambda}(g) = \mathbb{T}_\lambda = \mathbb{A}_\lambda \mathbb{X}_\lambda \mathbb{B}_\lambda$, where $X_\lambda \in GL(V_\lambda)$ is such that $\rho_\lambda(g) = X_\lambda$. (cf. the definition of the map Φ in (2.6) for the choice of $\mathbb{A}_\lambda$ and $\mathbb{B}_\lambda$). Proposition 2.12 motivates the definition of ρ_{Φ_λ}. We have the following equality of $\mathbb{Q}_l$-vector spaces:

$$V_l \;=\; \bigoplus_{\lambda|l} V_{\Phi_\lambda} \tag{5.8}$$

The l-adic representation

$$\rho_l \,:\, G_F \longrightarrow GL(V_l(A)) \tag{5.9}$$

induces the following representations (note that we use the notation ρ_l for both representations (5.9) and (5.10) cf. Remark 5.13):

$$\rho_l : G_F \longrightarrow GL(V_l) \tag{5.10}$$

$$\prod \rho_\lambda : G_F \longrightarrow \prod_\lambda GL(V_\lambda) \tag{5.11}$$

$$\prod \rho_{\Phi_\lambda} : G_F \longrightarrow \prod\nolimits_{\Phi_\lambda} GL(V_{\Phi_\lambda}). \tag{5.12}$$

Remark 5.13. In the case of abelian variety of type II we have $V_l(A) = V_l \oplus V_l$ and the action of G_F on the direct sum is the diagonal one as follows from Theorem 5.4. Hence, the images of the Galois group via the representations (5.9), (5.10) and (5.12) are isomorphic. Also the Zariski closures of the images of these three representations are isomorphic as algebraic varieties over $\mathbb{Q}_l$ in the corresponding GL-groups. Similarly, $V_\lambda(A) = V_\lambda \oplus V_\lambda$ with the diagonal action of G_F on the direct sum by Theorem 5.4. Hence, the images of the representations given by G_F-actions on V_λ and $V_\lambda(A)$ are isomorphic and so are their Zariski closures in corresponding GL-groups. For this reason, in the sequel, we will identify the representation of G_F on $V_l(A)$ (respectively on $V_\lambda(A)$) with its representation on V_l (resp. V_λ).

By Remark 5.13 we can consider G_l^{alg} (resp. G_λ^{alg}) to be the Zariski closure in GL_{V_l} (resp. GL_{V_λ}) of the image of the representation ρ_l of (5.10) (resp. ρ_λ of (5.11)). Let $G_{\Phi_\lambda}^{alg}$ denote the Zariski closure in $GL_{V_{\Phi_\lambda}}$ of the image of the representation ρ_{Φ_λ} of (5.12). Let $\mathfrak{g}_l$ be the Lie algebra of G_l^{alg}, $\mathfrak{g}_\lambda$ be the Lie algebra of G_λ^{alg} and let $\mathfrak{g}_{\Phi_\lambda}$ be the Lie algebra of $G_{\Phi_\lambda}^{alg}$. By definition, we have the following inclusions:

$$G_l^{alg} \subset \prod\nolimits_{\lambda|l} G_{\Phi_\lambda}^{alg} \tag{5.14}$$

$$(G_l^{alg})' \subset \prod\nolimits_{\lambda|l} (G_{\Phi_\lambda}^{alg})' \tag{5.15}$$

$$\mathfrak{g}_l \subset \bigoplus\nolimits_{\lambda|l} \mathfrak{g}_{\Phi_\lambda} \tag{5.16}$$

$$\mathfrak{g}_l^{ss} \subset \bigoplus\nolimits_{\lambda|l} \mathfrak{g}_{\Phi_\lambda}^{ss}. \tag{5.17}$$

The map (5.14) gives a map

$$G_l^{alg} \to G_{\Phi_\lambda}^{alg}, \tag{5.18}$$

which induces the natural map of Lie algebras:

$$\mathfrak{g}_l \to \mathfrak{g}_{\Phi_\lambda}. \tag{5.19}$$

Lemma 5.20. *The map (5.19) of Lie algebras is surjective for any prime $\lambda | l$. Hence the following map of Lie algebras:*

$$\mathfrak{g}_l^{ss} \to \mathfrak{g}_{\Phi_\lambda}^{ss} \tag{5.21}$$

is surjective.

Proof. We know by the result of Tate, [T2] that the $\mathbb{Q}_l[G_F]$-module $V_l(A)$ is of Hodge-Tate type for any prime v of $\mathcal{O}_F$ dividing l. Hence by the theorem of Bogomolov cf. [Bo] we have

$$\mathfrak{g}_l = \mathcal{L}ie\,(\rho_l(G_F)).$$

Since each $\mathbb{Q}_l[G_F]$-module V_{Φ_λ} is a direct summand of the $\mathbb{Q}_l[G_F]$-module V_l, then the $\mathbb{Q}_l[G_F]$-module V_{Φ_λ} is also of Hodge-Tate type for any prime v of $\mathcal{O}_F$ dividing l. It follows by the theorem of Bogomolov, [Bo] that

$$\mathfrak{g}_{\Phi_\lambda} = \mathcal{L}ie\,(\rho_{\Phi_\lambda}(G_F)).$$

But the surjective map of l-adic Lie groups $\rho_l(G_F) \to \rho_{\Phi_\lambda}(G_F)$ induces the surjective map of l-adic Lie algebras $\mathcal{L}ie\,(\rho_l(G_F)) \to \mathcal{L}ie\,(\rho_{\Phi_\lambda}(G_F))$. □

Lemma 5.22. *Let A/F be an abelian variety over F of type I or II such that $End_F\,(A) = End_{\overline{F}}\,(A)$. Then*

$$End_{\mathfrak{g}_\lambda}\,(V_\lambda) \;\cong\; End_{E_\lambda[G_F]}\,(V_\lambda) \;\cong\; E_\lambda \tag{5.23}$$

$$End_{\mathfrak{g}_{\Phi_\lambda}}\,(V_{\Phi_\lambda}) \;\cong\; End_{\mathbb{Q}_l[G_F]}\,(V_{\Phi_\lambda}) \;\cong\; E_\lambda. \tag{5.24}$$

Proof. By [F], Theorem 4, the assumption $End_F\,(A) = End_L\,(A)$ for any finite extension L/F, Theorem 4.16 (ii), the equality (5.2) and Theorem 5.4 we get

$$E_\lambda \cong End_{E_\lambda[G_F]}\,(V_\lambda) \cong End_{E_\lambda[G_L]}\,(V_\lambda). \tag{5.25}$$

This implies the equality

$$End_{G_F}\,(V_\lambda) = End_U\,(V_\lambda)$$

for any open subgroup U of G_F. Hence, the equality (5.23) follows by Lemma 4.12 (iii). For any $F \subset L \subset \overline{F}$ we have $M_{2,2}(End_{\mathbb{Q}_l[G_L]}(V_l)) = End_{\mathbb{Q}_l[G_L]}(V_l^2) = End_{\mathbb{Q}_l[G_L]}(V_l(A))$ and

$$End_{\mathbb{Q}_l[G_L]}(V_l(A)) \cong \prod_{\lambda | l} D_\lambda \cong \prod_{\lambda | l} M_{2,2}(E_\lambda). \tag{5.26}$$

On the other hand

$$\prod_{\lambda | l} E_\lambda \cong \prod_{\lambda | l} End_{E_\lambda[G_L]}(V_\lambda) \subset End_{\mathbb{Q}_l[G_L]}(V_l). \tag{5.27}$$

Hence, comparing the dimensions over $\mathbb{Q}_l$ in (5.26) and (5.27) we get

$$\prod_{\lambda | l} End_{E_\lambda[G_L]}(V_\lambda) \cong End_{\mathbb{Q}_l[G_L]}(V_l). \tag{5.28}$$

By (5.28) we clearly have

$$\prod_{\lambda | l} End_{\mathbb{Q}_l[G_L]}(V_{\Phi_\lambda}) \subset End_{\mathbb{Q}_l[G_L]}(V_l) \cong \prod_{\lambda | l} E_\lambda, \tag{5.29}$$

and

$$End_{E_\lambda[G_L]}(V_\lambda) \subset End_{\mathbb{Q}_l[G_L]}(V_{\Phi_\lambda}). \tag{5.30}$$

It follows by (5.25), (5.29) and by (5.30) that for any finite field extension $F \subset L$ contained in $\overline{F}$ we have

$$End_{\mathbb{Q}_l[G_L]}(V_{\Phi_\lambda}) \cong End_{E_\lambda[G_L]}(V_\lambda) \cong E_\lambda. \tag{5.31}$$

The isomorphisms (5.31) imply that

$$End_{G_F}(V_{\Phi_\lambda}) \cong End_U(V_{\Phi_\lambda}) \tag{5.32}$$

for any open subgroup U of G_F. The isomorphism (5.24) follows by (5.32) and Lemma 4.12 (iii). □

Lemma 5.33. $\mathfrak{g}_\lambda^{ss} = sp_{2h}(E_\lambda)$.

Proof. In the proof we adapt to the current situation the argument from [BGK], Lemma 3.2. The only thing to check is the minuscule conjecture for the λ-adic representations $\rho_F : G_F \to GL(V_\lambda)$. By the work of Pink cf. [P], Corollary 5.11, we know that $\mathfrak{g}_l^{ss} \otimes \bar{\mathbb{Q}}_l$ may only have simple factors of types A, B, C or D. By the semisimplicity of $\mathfrak{g}_l^{ss}$ and Lemma 5.20 the simple factors of $\mathfrak{g}_{\Phi_\lambda}^{ss} \otimes \bar{\mathbb{Q}}_l$ are of the same types. By Proposition 2.12 and Lemmas 2.21, 2.22, 2.23 we get

$$\mathfrak{g}_{\Phi_\lambda}^{ss} \cong R_{E_\lambda/\mathbb{Q}_l} \mathfrak{g}_\lambda^{ss}. \tag{5.34}$$

Since

$$\mathfrak{g}_{\Phi_\lambda}^{ss} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l \;\cong\; \mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} E_\lambda \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}} \;\cong\; \bigoplus_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} \mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} \overline{\mathbb{Q}}$$

we see that the simple factors of $\mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} \overline{\mathbb{Q}}$ are of types A, B, C or D. The rest of the argument is the same as in the proof of Lemma 3.2 of [BGK]. □

Lemma 5.35. *There are natural isomorphisms of $\mathbb{Q}_l$-algebras.*

$$End_{\mathfrak{g}_{\Phi_\lambda}^{ss}}(V_{\Phi_\lambda}) \cong End_{\mathfrak{g}_\lambda^{ss}}(V_\lambda) \cong E_\lambda \tag{5.36}$$

Proof. Since $\mathfrak{g}_\lambda$ is reductive and it acts irreducibly on the module V_λ (cf. Lemma 5.33) by [H2], Prop. p. 102 we have:

$$\mathfrak{g}_\lambda = Z(\mathfrak{g}_\lambda) \oplus \mathfrak{g}_\lambda^{ss} \tag{5.37}$$

and $Z(\mathfrak{g}_\lambda) = 0$ or $Z(\mathfrak{g}_\lambda) = E_\lambda$. This gives

$$End_{\mathfrak{g}_\lambda^{ss}}(V_\lambda) \;=\; End_{\mathfrak{g}_\lambda}(V_\lambda). \tag{5.38}$$

The Weil restriction functor commutes with the operation of taking the center of a Lie algebra, hence we get $Z(\mathfrak{g}_{\Phi_\lambda}) = 0$ or E_λ and by (5.34):

$$\mathfrak{g}_{\Phi_\lambda} = Z(\mathfrak{g}_{\Phi_\lambda}) \oplus \mathfrak{g}_{\Phi_\lambda}^{ss}.$$

Since $\mathfrak{g}_{\Phi_\lambda} \cong R_{E_\lambda/\mathbb{Q}_l}\mathfrak{g}_\lambda$, it is clear that

$$End_{\mathfrak{g}_{\Phi_\lambda}^{ss}}(V_{\Phi_\lambda}) \;=\; End_{\mathfrak{g}_{\Phi_\lambda}}(V_{\Phi_\lambda}).$$

The lemma follows now from Lemma 5.22. □

Proposition 5.39. *There is an equality of Lie algebras:*

$$\mathfrak{g}_l^{ss} = \bigoplus_{\lambda | l} \mathfrak{g}_{\Phi_\lambda}^{ss} \tag{5.40}$$

Proof. Put $\overline{V}_l = V_l \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$, $\overline{V}_\lambda = V_\lambda \otimes_{E_\lambda} \overline{\mathbb{Q}}_l$, $\overline{\mathfrak{g}}_l^{ss} = \mathfrak{g}_l^{ss} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$, $\overline{\mathfrak{g}}_{\Phi_\lambda}^{ss} = \mathfrak{g}_{\Phi_\lambda}^{ss} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$. By (5.34) we get

$$\overline{\mathfrak{g}}_{\Phi_\lambda}^{ss} \;\cong\; \mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} E_\lambda \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l \;\cong\; \prod_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} \mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} \overline{\mathbb{Q}}_l \;\cong\; \prod_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} sp(\overline{V}_\lambda) \tag{5.41}$$

By Corollary 1.2.2 of [C1] we have $\mathfrak{g}_l = \mathbb{Q}_l \oplus \mathfrak{g}_l^{ss}$, hence

$$End_{\mathfrak{g}_l^{ss}}(V_l(A)) \;=\; End_{\mathfrak{g}_l}(V_l(A)).$$

By Lemmas 5.20 and 5.35

$$\prod_{\lambda|l} E_\lambda \;\cong\; \prod_{\lambda|l} End_{\mathfrak{g}_{\Phi_\lambda}^{ss}}(V_{\Phi_\lambda}) \;\cong\; \prod_{\lambda|l} End_{\mathfrak{g}_l^{ss}}(V_{\Phi_\lambda}) \subset End_{\mathfrak{g}_l^{ss}}(V_l). \tag{5.42}$$

But by assumption on l and (5.42)

$$\prod_{\lambda|l} D_\lambda \;\cong\; \prod_{\lambda|l} M_{2,2}(E_\lambda) \;\cong\; M_{2,2}(\prod_{\lambda|l} E_\lambda) \subset M_{2,2}(End_{\mathfrak{g}_l^{ss}}(V_l)) \;=$$

$$= \; End_{\mathfrak{g}_l^{ss}}(V_l(A)) \;=\; End_{\mathfrak{g}_l}(V_l(A)) \;\cong\; \prod_{\lambda|l} D_\lambda. \tag{5.43}$$

Comparing dimensions in (5.43) we get

$$End_{\mathfrak{g}_l^{ss}}(V_l) \;\cong\; \prod_{\lambda|l} E_\lambda. \tag{5.44}$$

Hence we get

$$End_{\overline{\mathfrak{g}}_l^{ss}}(\overline{V}_l) \;\cong\; End_{\mathfrak{g}_l^{ss}}(V_l) \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l \;\cong\; \prod_{\lambda|l} E_\lambda \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l \;\cong\; \prod_{\lambda|l} \prod_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} \overline{\mathbb{Q}}_l. \tag{5.45}$$

$$End_{\overline{\mathbb{Q}}_l[G_F]}(\overline{V}_\lambda) \;\cong\; End_{E_\lambda[G_F]}(V_\lambda) \otimes_{E_\lambda} \overline{\mathbb{Q}}_l \;\cong\; E_\lambda \otimes_{E_\lambda} \overline{\mathbb{Q}}_l \;\cong\; \overline{\mathbb{Q}}_l. \tag{5.46}$$

$$\overline{V}_l \;\cong\; \bigoplus_{\lambda|l} V_\lambda \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l \;\cong\; \bigoplus_{\lambda|l} \bigoplus_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} \overline{V}_\lambda. \tag{5.47}$$

By (5.21) the map of Lie algebras $\overline{\mathfrak{g}}_l^{ss} \to \overline{\mathfrak{g}}_{\Phi_\lambda}^{ss}$ is surjective. Isomorphisms (5.45), (5.46) and (5.47) show that the simple $\overline{\mathfrak{g}}_l^{ss}$ modules $\mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} \overline{\mathbb{Q}}_l$, for all $\lambda|l$ and all $E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l$, are pairwise nonisomorphic submodules of $\overline{\mathfrak{g}}_l^{ss}$. Hence by [H2], Theorem on page 23

$$\bigoplus_{\lambda|l} \bigoplus_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} \mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} \overline{\mathbb{Q}}_l \;\subset\; \overline{\mathfrak{g}}_l^{ss}. \tag{5.48}$$

Tensoring (5.17) with $\overline{\mathbb{Q}}_l$ and comparing with (5.48) we get

$$\bigoplus_{\lambda|l} \bigoplus_{E_\lambda \hookrightarrow \overline{\mathbb{Q}}_l} \mathfrak{g}_\lambda^{ss} \otimes_{E_\lambda} \overline{\mathbb{Q}}_l \;\cong\; \overline{\mathfrak{g}}_l{}^{ss}. \tag{5.49}$$

Hence for dimensional reasons (5.17), (5.41) and (5.49) imply (5.40). □

Corollary 5.50. *The representations ρ_{Φ_λ}, for $\lambda|l$ are pairwise nonisomorphic. The representations of the Lie algebra $\mathfrak{g}_l^{ss}$ on V_{Φ_λ} are pairwise nonisomorphic over $\mathbb{Q}_l$.*

Proof. It follows by Lemmas 5.20 and 5.22 and equalities (5.8), (5.36), (5.44). □

Corollary 5.51. *There is an equality of ranks of group schemes over $\mathbb{Q}_l$:*

$$rank\ (G_l^{alg})' \ = rank \prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(Sp_{2h}/E_\lambda). \tag{5.52}$$

Proof. The Corollary follows by Lemma 5.33, equality (5.40), the isomorphism (5.34) and Lemma 2.21. □

Taking into account (4.10), (4.11) and Remark 5.13 we get:

$$G(l)^{alg} \ \subset \ \prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(GSp_{A_\lambda[\lambda]}) \ \cong \ \prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(GSp_{2h}) \tag{5.53}$$

$$G_l^{alg} \ \subset \ \prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(GSp_{V_\lambda}) \ \cong \ \prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(GSp_{2h}). \tag{5.54}$$

6. Computation of the images of the Galois representations ρ_l and $\overline{\rho}_l$.

In this section we explicitly compute the images of the l-adic representations induced by the action of the absolute Galois group on the Tate module of a large class of abelian varieties of types I and II described in the definition below.

Definition of class $\mathcal{A}$. *We say that an abelian variety A/F, defined over a number field F, is of class $\mathcal{A}$, if the following conditions hold:*

(i) *A is a simple, principally polarized abelian variety of dimension g*

(ii) *$\mathcal{R} = End_{\bar{F}}(A) = End_F(A)$ and the endomorphism algebra $D = \mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Q}$, is of type I or II in the Albert list of the division algebras with involution cf. [Mu], p. 201*

(iii) *the field F is such that for every l the Zariski closure G_l^{alg} of $\rho_l(G_F)$ in $GL_{2g}/\mathbb{Q}_l$ is a connected algebraic group*

(iv) *$g = hed$, where h is an odd integer, $e = [E : Q]$ is the degree of the center E of D and $d^2 = [D : E]$.*

Let L be a local field with the ring of integers $\mathcal{O}_L$ with maximal ideal $\mathfrak{m}_L = \mathfrak{m}$ and the residue field $k = \mathcal{O}_L/\mathfrak{m}$.

Lemma 6.1. *Let*

$$\mathcal{G}_1 \hookrightarrow \mathcal{G}_2 \tag{6.2}$$

be a closed immersion of two smooth, reductive group schemes over $\mathcal{O}_L$. Let

$$G_1 \hookrightarrow G_2 \tag{6.3}$$

be the base change to L of the arrow (6.2) and let

$$G_1(\mathfrak{m}) \hookrightarrow G_2(\mathfrak{m}) \tag{6.4}$$

be the base change to k of the arrow (6.2). If $rank\, G_1 = rank\, G_2$ then $rank\, G_1(\mathfrak{m}) = rank\, G_2(\mathfrak{m})$.

Proof. By [SGA3, Th. 2.5 p. 12] applied to the special point of the scheme $spec\, \mathcal{O}_L$ there exists an étale neighborhood $S' \rightarrow spec\, \mathcal{O}_L$ of the geometric point over the special point such that the group schemes $\mathcal{G}_{1,S'} = \mathcal{G}_1 \times_{spec\, \mathcal{O}_L} S'$ and $\mathcal{G}_{2,S'} = \mathcal{G}_2 \times_{spec\, \mathcal{O}_L} S'$ have maximal tori $\mathcal{T}_{1,S'}$ and $\mathcal{T}_{1,S'}$ respectively. By [SGA3] XXII, Th. 6.2.8 p. 260 we observe (we do not need it here but in the Theorem 6.6 below) that $(\mathcal{G}_{i,S'})' \cap \mathcal{T}_{i,S'}$ is a maximal torus of $(\mathcal{G}_{i,S'})'$. By the definition of a maximal torus and by [SGA3] XIX, Th. 2.5, p. 12 applied to the special point of $spec\, \mathcal{O}_L$, we obtain that the special and generic fibers of each scheme $\mathcal{G}_{i,S'}$ have the same rank. But clearly the generic (resp. special) fibers of schemes $\mathcal{G}_{i,S'}$ and $\mathcal{G}_i$ have the same rank for $i = 1, 2$. Hence going around the diagram

$$\begin{tikzcd}
G_1 \arrow[r, hook] \arrow[d, hook] & G_2 \arrow[d, hook] \\
\mathcal{G}_1 \arrow[r, hook] & \mathcal{G}_2 \\
G_1(\mathfrak{m}) \arrow[r, hook] \arrow[u, hook] & G_2(\mathfrak{m}) \arrow[u, hook]
\end{tikzcd} \tag{6.5}$$

and taking into account the assumptions that the ranks of the upper corners are the same we get $rank\, G_1(\mathfrak{m}) = rank\, G_2(\mathfrak{m})$. □

Theorem 6.6. *Let A/F be an abelian variety of class $\mathcal{A}$. Then for all $l \gg 0$, we have equalitiy of ranks of group schemes over $\mathbb{F}_l$:*

$$rank\ (G(l)^{alg})' = rank \prod_{\lambda | l} R_{k_\lambda / \mathbb{F}_l}(Sp_{2h}) \tag{6.7}$$

Proof. By [LP1] Prop.1.3 and by [Wi], Th.1 and 2.1, for $l \gg 0$ the group scheme $\mathcal{G}_l^{alg}$ over $spec\, \mathbb{Z}_l$ is smooth and reductive. For such an l the structure morphism $(\mathcal{G}_l^{alg})' \rightarrow spec\, \mathbb{Z}_l$ is the base change of the smooth morphism

$\mathcal{G}_l^{alg} \rightarrow D_{\mathbb{Z}_l}(D_{\mathbb{Z}_l}(\mathcal{G}_l^{alg}))$ via the unit section of $D_{\mathbb{Z}_l}(D_{\mathbb{Z}_l}(\mathcal{G}_l^{alg}))$, see [SGA3] XXII, Th. 6.2.1, p. 256 where $D_S(G) = \underline{Hom}_{S-gr}(G, \mathbb{G}_{m,S})$ for a scheme S. Hence, the group scheme $(\mathcal{G}_l^{alg})'$ is also smooth over $\mathbb{Z}_l$. By [SGA3] *loc. cit*, the group scheme $(\mathcal{G}_l^{alg})'$ is semisimple. We finish the proof by taking $L = \mathbb{Q}_l$, $\mathcal{G}_1 = (\mathcal{G}_l^{alg})'$, $\mathcal{G}_2 = \prod_{\lambda | l} R_{\mathcal{O}_\lambda/\mathbb{Z}_l}(Sp_{2h})$ in Lemma 6.1 and applying Corollary 5.51. □

Remark 6.8. If G is a group scheme over S_0 then the derived subgroup G' is defined as the kernel of the natural map

$$G \rightarrow D_{S_0}(D_{S_0}(G))$$

[V], [SGA3]. Since this map is consistent with the base change, we see that for any scheme S over S_0 we get

$$G' \times_{S_0} S = (G \times_{S_0} S)'.$$

Theorem 6.9. *Let A/F be an abelian variety of class $\mathcal{A}$. Then for all $l \gg 0$, we have equalities of group schemes:*

$$(G_l^{alg})' = \prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(Sp_{2h}) \tag{6.10}$$

$$(G(l)^{alg})' = \prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(Sp_{2h}) \tag{6.11}$$

Proof. The proof is similar to the proof of Lemma 3.4 of [BGK]. We prove the equality (6.11). The proof of the equality (6.10) is analogous. Let

$$\underline{\rho}_l : G(l)^{alg} \rightarrow GL_{2g}$$

denote the representation induced by the inclusion $G(l)^{alg} \subset GL_{2g}$. By the result of Faltings cf. [Fa], the representation $\underline{\rho}_l$ is semisimple and the commutant of $\underline{\rho}_l(G(l)^{alg})$ in the matrix ring $M_{2g,2g}$ is $\underline{End}_{\bar{F}}(A) \otimes_{\mathbb{Z}} \mathbb{F}_l$. The representation $\underline{\rho}_l$ factors through the imbedding (5.53). Projecting onto the λ component in (5.53) we obtain the representation

$$\underline{\rho}_{\Phi_\lambda} : G(l)^{alg} \rightarrow R_{k_\lambda/\mathbb{F}_l}(GSp_{A[\lambda]}) \cong R_{k_\lambda/\mathbb{F}_l}(GSp_{2h}). \tag{6.12}$$

This map corresponds to the map

$$G(l)^{alg} \otimes_{\mathbb{F}_l} k_\lambda \rightarrow GSp_{2h}. \tag{6.13}$$

By Remark 6.8 restriction of the the map (6.13) to the derived subgroups gives the following map:

$$(G(l)^{alg})' \otimes_{\mathbb{F}_l} k_\lambda \to Sp_{2h} \tag{6.14}$$

which in turn gives the representation

$$\underline{\rho}_{\Phi_\lambda} : (G(l)^{alg})' \to R_{k_\lambda/\mathbb{F}_l}(Sp_{2h}).$$

Now by (5.3) we have the natural isomorphisms:

$$\prod_{k_\lambda \hookrightarrow \overline{\mathbb{F}}_l} \overline{\mathbb{F}}_l \;\cong\; k_\lambda \otimes_{\mathbb{F}_l} \overline{\mathbb{F}}_l \;\cong\; End_{k_\lambda \otimes_{\mathbb{F}_l} \overline{\mathbb{F}}_l [G_F]}(A_\lambda[\lambda] \otimes_{\mathbb{F}_l} \overline{\mathbb{F}}_l) \;\cong$$

$$\cong\; End_{k_\lambda \otimes_{\mathbb{F}_l} \overline{\mathbb{F}}_l [G_F]}(A_\lambda[\lambda] \otimes_{k_\lambda} k_\lambda \otimes_{\mathbb{F}_l} \overline{\mathbb{F}}_l) \;\cong$$

$$\cong\; \prod_{k_\lambda \hookrightarrow \overline{\mathbb{F}}_l} End_{\overline{\mathbb{F}}_l [G_F]}(A_\lambda[\lambda] \otimes_{k_\lambda} \overline{\mathbb{F}}_l). \tag{6.15}$$

Note that $Z(Sp_{2h}) \cong \mu_2$ and this isomorphism holds over any field of definition. The isomorphisms (6.15) imply by the Schur's Lemma:

$$\underline{\rho}_{\Phi_\lambda}(Z((G(l)^{alg})')) \subset R_{k_\lambda/\mathbb{F}_l}(\mu_2).$$

Hence

$$Z((G(l)^{alg})') \subset \prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(\mu_2) = Z(\prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(Sp_{2h})).$$

Observe that both groups $(G(l)^{alg})'$ and $\prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(Sp_{2h})$ are reductive. Now the proof is finished in the same way as the proof of Lemma 3.4 in [BGK]. □

Theorem 6.16. *Let A/F be an abelian variety of class $\mathcal{A}$. Then for $l \gg 0$, we have:*

$$\overline{\rho_l}(G_F') \;=\; \prod_{\lambda | l} Sp_{2h}(k_\lambda) \;=\; Sp_{2h}(\mathcal{O}_E / l\mathcal{O}_E), \tag{6.17}$$

$$\rho_l(\overline{G_F'}) \;=\; \prod_{\lambda | l} Sp_{2h}(\mathcal{O}_\lambda) \;=\; Sp_{2h}(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_l), \tag{6.18}$$

where $\overline{\rho_l}$ is the representation ρ_l mod l and $\overline{G_F'}$ is the closure of the commutator subgroup $G_F' \subset G_F$ computed with respect to the natural profinite topology of G_F.

Proof. To prove the equality (6.17), note that the group scheme $\prod_{\lambda | l} R_{k_\lambda/\mathbb{F}_l}(Sp_{2h})$ is simply connected, since its base change to $\overline{\mathbb{F}}_l$ is

$\prod_{\lambda|l}\prod_{k_\lambda\hookrightarrow\overline{\mathbb{F}}_l} Sp_{2h}/\overline{\mathbb{F}}_l$, which is clearly simply connected. From now on the argument is the same as in the proof of Theorem 3.5 in [BGK]. Namely: it follows by (6.11) that $(G(l)^{alg})'$ is simply connected. So $(G(l)^{alg})'(\mathbb{F}_l) = (G(l)^{alg})'(\mathbb{F}_l)_u$. Hence, by a theorem of Serre (cf. [Wi], Th.4) we get

$$(G(l)^{alg})'(\mathbb{F}_l) \subset (\overline{\rho_l}(G_F))' = \overline{\rho_l}(G'_F).$$

On the other hand, by definition of the group $G(l)^{alg}$, it is clear that

$$\overline{\rho_l}(G'_F) = (\overline{\rho_l}(G_F))' \subset (G(l)^{alg})'(\mathbb{F}_l).$$

As for the second equality in (6.18) we have

$$\rho_l\big(\overline{G'_F}\big) = \overline{(\rho_l(G_F))'} \subset \prod_{\lambda|l} Sp_{2h}(\mathcal{O}_\lambda), \tag{6.19}$$

where $\overline{(\rho_l(G_F))'}$ denotes the closure of $(\rho_l(G_F))'$ in the natural (λ-adic in each factor) topology of the group $\prod_{\lambda|l} Sp_{2h}(\mathcal{O}_\lambda)$. Using equality (6.17) and Lemma 6.20 stated below, applied to $X = \overline{(\rho_l(G_F))'}$, we finish the proof. □

Lemma 6.20. *Let X be a closed subgroup in $\prod_{\lambda|l} Sp_{2h}(\mathcal{O}_\lambda)$ such that its image via the reduction map*

$$\prod_{\lambda|l} Sp_{2h}(\mathcal{O}_\lambda) \to \prod_{\lambda|l} Sp_{2h}(k_\lambda)$$

is all of $\prod_{\lambda|l} Sp_{2h}(k_\lambda)$. Then $X = \prod_{\lambda|l} Sp_{2h}(\mathcal{O}_\lambda)$.

Proof. The proof is similar to the proof of Lemma 3 in [Se] chapter IV, 3.4. □

7. Applications to classical conjectures.

Choose an imbedding of F into the field of complex numbers $\mathbb{C}$. Let $V = H^1(A(\mathbb{C}), \mathbb{Q})$ be the singular cohomology group with rational coefficients. Consider the Hodge decomposition

$$V \otimes_{\mathbb{Q}} \mathbb{C} = H^{1,0} \oplus H^{0,1},$$

where $H^{p,q} = H^p(A; \Omega^q_{A/\mathbb{C}})$ and $\overline{H^{p,q}} = H^{q,p}$. Observe that $H^{p,q}$ are invariant subspaces with respect to $D = End_{\overline{F}}(A) \otimes \mathbb{Q}$ action on $V \otimes_{\mathbb{Q}} \mathbb{C}$. Hence, in particular $H^{p,q}$ are E-vector spaces. Let

$$\psi : V \times V \to \mathbb{Q}$$

be the $\mathbb{Q}$-bilinear, nondegenerate, alternating form coming from the Riemann form of A. Since A has a principal polarization by assumption, the form ψ is given by the standard matrix

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Define the cocharacter

$$\mu_\infty : \mathbb{G}_m(\mathbb{C}) \to GL(V \otimes_{\mathbb{Q}} \mathbb{C}) = GL_{2g}(\mathbb{C})$$

such that, for any $z \in \mathbb{C}^\times$, the automorphism $\mu_\infty(z)$ is the multiplication by z on $H^{1,0}$ and the identity on $H^{0,1}$.

Definition 7.1. *The Mumford-Tate group of the abelian variety A/F is the smallest algebraic subgroup $MT(A) \subset GL_{2g}$, defined over $\mathbb{Q}$, such that $MT(A)(\mathbb{C})$ contains the image of μ_∞. The Hodge group $H(A)$ is by definition the connected component of the identity in $MT(A) \cap SL_V \cong MT(A) \cap SL_{2g}$.*

We refer the reader to [D] for an excellent exposition on the Mumford-Tate group. In particular, $MT(A)$ is a reductive group *loc. cit.* Since, by definition

$$\mu_\infty(\mathbb{C}^\times) \subset GSp_{(V,\,\psi)}(\mathbb{C}) \cong GSp_{2g}(\mathbb{C}),$$

it follows that the group $MT(A)$ is a reductive subgroup of the group of symplectic similitudes $GSp_{(V,\,\psi)} \cong GSp_{2g}$ and that

(7.2) $$H(A) \subset Sp_{(V,\,\psi)} \cong Sp_{2g}.$$

Remark 7.3. Let V be a finite dimensional vector space over a field K such that it is also an R-module for a K-algebra R. Let G be a K-group subscheme of GL_V. Then by the symbol $C_R(G)$ we will denote the commutant of R in G. The symbol $C_R^\circ(G)$ will denote the connected component of identity in $C_R(G)$. Let $\beta : V \times V \to K$ be a bilinear form and let $G_{(V,\beta)} \subset GL_V$ be the subscheme of GL_V of all isometries with respect to the bilinear form β. It is easy to check that $C_R(G_{(V,\beta)}) \otimes_K L \cong C_{R\otimes_K L}(G_{(V\otimes_K L,\, \beta\otimes_K L)})$. Note that $MT(A) \subset C_D(GSp_{(V,\,\psi)})$ by definitions.

Definition 7.4. *The algebraic group $L(A) = C_D^\circ(Sp_{(V,\,\psi)})$ is called the Lefschetz group of a principally polarized abelian variety A. Note that the group $L(A)$ does not depend on the form ψ cf. [R2].*

By [D], Sublemma 4.7, there is a unique E-bilinear, nondegenerate, alternating pairing

$$\phi : V \times V \to E$$

such that $Tr_{E/\mathbb{Q}}(\phi) = \psi$. Taking into account that the actions of $H(A)$ and $L(A)$ on V commute with the E-structure, we get

(7.5) $$H(A) \subset L(A) \subset R_{E/\mathbb{Q}} Sp_{(V,\,\phi)} \subset Sp_{(V,\,\psi)}.$$

But $R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}) = C_E(Sp_{(V,\,\psi)})$ hence $C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)})) = C_D(Sp_{(V,\,\psi)})$ so

(7.6) $$H(A) \subset L(A) = C_D^\circ(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)})) \subset C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)})).$$

Definition 7.7. *If $L/\mathbb{Q}$ is a field extension of $\mathbb{Q}$ we put*

$$MT(A)_L := MT(A) \otimes_{\mathbb{Q}} L, \quad H(A)_L := H(A) \otimes_{\mathbb{Q}} L, \quad L(A)_L := L(A) \otimes_{\mathbb{Q}} L.$$

Conjecture 7.8 (Mumford-Tate cf. [Se5], C.3.1). *If A/F is an abelian variety over a number field F, then for any prime number l*

$$(G_l^{alg})^{\circ} = MT(A)_{\mathbb{Q}_l}, \tag{7.9}$$

where $(G_l^{alg})^{\circ}$ denotes the connected component of the identity.

Theorem 7.10 (Deligne [D], I, Prop. 6.2). *If A/F is an abelian variety over a number field F and l is a prime number, then*

$$(G_l^{alg})^{\circ} \subset MT(A)_{\mathbb{Q}_l}. \tag{7.11}$$

Theorem 7.12. *The Mumford-Tate conjecture holds true for abelian varieties of class $\mathcal{A}$ defined in the beginning of Section 6.*

Proof. By [LP1], Theorem 4.3, it is enough to verify (7.9) for a single prime l only. We use the equality (6.10) for a big enough prime l. The proof goes similarly to the proof of Theorem 3.6 in [BGK]. In the proof we will make some additional computations, which provide an extra information on the Hodge group $H(A)$. The Hodge group $H(A)$ is semisimple (cf. [G], Prop. B.63) and the center of $MT(A)$ is $\mathbb{G}_m$ (cf. [G], Cor. B.59). Since $MT(A) = \mathbb{G}_m H(A)$, we get

$$(MT(A)_{\mathbb{Q}_l})' = (H(A)_{\mathbb{Q}_l})' = H(A)_{\mathbb{Q}_l}. \tag{7.13}$$

By (7.11), (7.13) and (6.10)

$$\prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(Sp_{(V_\lambda, \psi_\lambda^0)}) \cong \prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(Sp_{2h}) \subset H(A)_{\mathbb{Q}_l}. \tag{7.14}$$

On the other hand by (7.6)

$$H(A)_{\mathbb{Q}_l} \subset L(A)_{\mathbb{Q}_l} \subset C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)})) \otimes_{\mathbb{Q}} \mathbb{Q}_l. \tag{7.15}$$

Since $R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}) = C_E(Sp_{(V,\,\psi)})$, by Remark 7.3, formulae (7.14) and (7.15) we get:

$$\prod_{\lambda | l} R_{E_\lambda/\mathbb{Q}_l}(Sp_{(V_\lambda, \psi_\lambda^0)}) \subset \prod_{\lambda | l} C_{D_\lambda}(R_{E_\lambda/\mathbb{Q}_l}(Sp_{(V_\lambda(A),\,\psi_\lambda^0)})). \tag{7.16}$$

For A of type I, $D_\lambda = E_\lambda$ and $V_\lambda(A) = V_\lambda$ hence, trivially, the inclusion (7.16) is an equality. Assume that A is of type II. Since $V_\lambda(A) = V_\lambda \oplus V_\lambda$ and

$D_\lambda = M_{2,2}(E_\lambda)$, evaluating both sides of the inclusion (7.16) on the $\overline{\mathbb{Q}}_l$-points, we get equality with both sides equal to

$$\prod_{\lambda|l}\prod_{E_\lambda\hookrightarrow\overline{\mathbb{Q}}_l}(Sp_{(V_\lambda,\phi_\lambda|_{V_\lambda})})(\overline{\mathbb{Q}}_l)$$

which is an irreducible algebraic variety over $\overline{\mathbb{Q}}_l$. Then we use Prop. II, 2.6 and Prop. II, 4.10 of [H] in order to conclude that the groups $H(A)_{\overline{\mathbb{Q}}_l}$, $L(A)_{\overline{\mathbb{Q}}_l}$ and $C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}))\otimes_{\mathbb{Q}}\overline{\mathbb{Q}}_l$ are connected. Hence all the groups $H(A)$, $L(A)$ and $C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}))$ are connected, and we have

$$\begin{aligned}(7.17)\qquad &\prod_{\lambda|l}R_{E_\lambda/\mathbb{Q}_l}(Sp_{(V_\lambda,\phi_\lambda|_{V_\lambda})})\cong\prod_{\lambda|l}R_{E_\lambda/\mathbb{Q}_l}(Sp_{2h})=\\ &=H(A)_{\mathbb{Q}_l}=L(A)_{\mathbb{Q}_l}=C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}))\otimes_{\mathbb{Q}}\mathbb{Q}_l.\end{aligned}$$

By (6.10), (7.17) and [Bo], Corollary 1. p. 702 we get

$$(7.18)\qquad MT(A)_{\mathbb{Q}_l}=\mathbb{G}_mH(A)_{\mathbb{Q}_l}=\mathbb{G}_m(G_l^{alg})'\subset G_l^{alg}.$$

The Theorem follows by (7.11) and (7.18). □

Corollary 7.19. *If A is an abelian variety of class $\mathcal{A}$, then*

$$(7.20)\qquad H(A)_{\mathbb{Q}}=L(A)_{\mathbb{Q}}=C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}))=C_D(Sp_{(V,\,\psi)}).$$

Proof. Taking Lie algebras of groups in (7.17) we deduce by a simple dimension argument that

$$(7.21)\qquad \mathcal{L}ie\,H(A)=\mathcal{L}ie\,L(A)=\mathcal{L}ie\,C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)})).$$

In the proof of Theorem 7.12 we have showed that the groups $H(A)$, $L(A)$ and $C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)}))$ are connected. Hence, by Theorem p. 87 of [H1] we conclude that

$$(7.22)\qquad H(A)=L(A)=C_D(R_{E/\mathbb{Q}}(Sp_{(V,\,\phi)})).\qquad\square$$

Corollary 7.23. *If A is an abelian variety of class $\mathcal{A}$, then for all l:*

$$(7.24)\qquad H(A)_{\mathbb{Q}_l}=\prod_{\lambda|l}C_{D_\lambda}(R_{E_\lambda/\mathbb{Q}_l}(Sp_{(V_\lambda(A),\,\phi\otimes_{\mathbb{Q}}E_\lambda)})).$$

In particular, for $l\gg 0$ we get

$$(7.25)\qquad H(A)_{\mathbb{Q}_l}=\prod_{\lambda|l}R_{E_\lambda/\mathbb{Q}_l}(Sp_{(V_\lambda,\,\phi\otimes_{\mathbb{Q}}E_\lambda)}).$$

Proof. Equality (7.24) follows immediately from Corollary 7.19. Equality (7.25) follows then from (7.17). □

We have:

$$H^1(A(\mathbb{C});\,\mathbb{R})\;\cong\;V\otimes_{\mathbb{Q}}\mathbb{R}\;\cong\;\bigoplus_{\sigma:E\hookrightarrow\mathbb{R}}V\otimes_{E,\sigma}\mathbb{R}.$$

Put $V_\sigma(A)=V\otimes_{E,\sigma}\mathbb{R}$ and let ϕ_σ be the form

$$\phi\otimes_{E,\sigma}\mathbb{R}\;:\;V_\sigma(A)\otimes_{\mathbb{R}}V_\sigma(A)\;\rightarrow\;\mathbb{R}.$$

Lemma 7.26. *If A is simple, principally polarized abelian variety of type II, then for each $\sigma : E \hookrightarrow \mathbb{R}$ there is an $\mathbb{R}$-vector space $W_\sigma(A)$ of dimension $\frac{g}{e} = \frac{4\, dim A}{[D\colon \mathbb{Q}]}$ such that:*

(i) $V_\sigma(A) \cong W_\sigma(A) \oplus W_\sigma(A)$,

(ii) *the restriction of $\phi \otimes_{\mathbb{Q}} \mathbb{R}$ to $W_\sigma(A)$ gives a nondegenerate, alternating pairing*

$$\psi_\sigma \,:\, W_\sigma(A) \times W_\sigma(A) \to \mathbb{R}.$$

Proof. Using the assumption that $D \otimes_{\mathbb{Q}} \mathbb{R} \cong M_{2,2}(\mathbb{R})$ the proof is similar to the proof of Theorem 5.4. □

We put

$$W_{\infty,\sigma} = \begin{cases} V_\sigma(A) & \text{if } A \text{ is of type I} \\ \\ W_\sigma(A)\,, & \text{if } A \text{ is of type II} \end{cases}$$

and

$$\psi_\sigma = \begin{cases} \phi_\sigma & \text{if } A \text{ is of type I} \\ \\ \phi_\sigma|_{W_\sigma(A)}\,, & \text{if } A \text{ is of type II.} \end{cases}$$

Observe that

$$dim_{\mathbb{R}}\, W_{\infty,\sigma} = \begin{cases} \frac{2g}{e} = \frac{2\, dim A}{[D\colon \mathbb{Q}]} & \text{if } A \text{ is of type I} \\ \\ \frac{g}{e} = \frac{4\, dim A}{[D\colon \mathbb{Q}]}\,, & \text{if } A \text{ is of type II.} \end{cases}$$

Corollary 7.27. *If A is an abelian variety of class $\mathcal{A}$, then*

$$H(A)_{\mathbb{R}} = L(A)_{\mathbb{R}} = \prod_{\sigma : E \hookrightarrow \mathbb{R}} Sp_{(W_{\infty,\sigma},\, \psi_\sigma)} \tag{7.28}$$

$$H(A)_{\mathbb{C}} = L(A)_{\mathbb{C}} = \prod_{\sigma E \hookrightarrow \mathbb{R}} Sp_{(W_{\infty,\sigma} \otimes_{\mathbb{C}} \mathbb{C},\, \psi_\sigma \otimes_{\mathbb{R}} \mathbb{C})}. \tag{7.29}$$

Proof. It follows from Lemma 7.26 and Corollary 7.19. □

We recall the conjectures of Tate and Hodge in the case of abelian varieties. See [G], [K] and [T1] for more details.

Conjecture 7.30 (Hodge). *If A/F is a simple abelian variety over a number field F, then for every $0 \leq p \leq g$ the natural cycle map induces an isomorphism*

$$A^p(A) \cong H^{2p}(A(\mathbb{C});\, \mathbb{Q}) \cap H^{p,p}, \tag{7.31}$$

where $A^p(A)$ is the $\mathbb{Q}$-vector space of codimension p algebraic cycles on A modulo the homological equivalence.

Conjecture 7.32 (Tate). *If A/F is a simple abelian variety over a number field F and l is a prime number, then for every $0 \leq p \leq g$ the cycle map induces an isomorphism:*

$$A^p(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l \cong H^{2p}_{et}(\overline{A};\, \mathbb{Q}_l(p))^{G_F} \tag{7.33}$$

where $\overline{A} = A \otimes_F \overline{F}$.

Theorem 7.34. *The Hodge conjecture holds true for abelian varieties of class $\mathcal{A}$.*

Proof. By [Mu], Theorem 3.1 the Hodge conjecture follows from the equality (7.20) of Corollary 7.19. □

Theorem 7.35. *The Tate conjecture holds true for abelian varieties of class $\mathcal{A}$.*

Proof. It is known (see Proposition 8.7 of [C1]) that Mumford-Tate conjecture implies the equivalence of Tate and Hodge conjectures. Hence the Tate conjecture follows by Theorems 7.12 and 7.34. □

Conjecture 7.36 (Lang). *Let A be an abelian variety over a number field F. Then for $l \gg 0$ the group $\rho_l(G_F)$ contains the group of all homotheties in $GL_{T_l(A)}(\mathbb{Z}_l)$.*

Theorem 7.37 (Wintenberger [Wi], Cor. 1, p. 5). *Let A be an abelian variety over a number field F. The Lang conjecture holds for such abelian varieties A for which the Mumford-Tate conjecture holds or if $\dim A < 5$.*

Theorem 7.38. *The Lang's conjecture holds true for abelian varieties of class $\mathcal{A}$.*

Proof. It follows by Theorem 7.12 and Theorem 7.37. □

We are going to use Theorem 7.12 and Corollary 7.19 to prove an analogue of the open image Theorem of Serre cf. [Se8]. We start with the following remark which is a plain generalization of remark 7.3.

Remark 7.39. Let $B_1 \subset B_2$ be two commutative rings with identity. Let Λ be a free, finitely generated B_1-module such that it is also an R-module for a B_1-algebra R. Let G be a B_1-group subscheme of GL_Λ. Then $C_R(G)$ will denote the commutant of R in G. The symbol $C^{\circ}_R(G)$ will denote the connected component of identity in $C_R(G)$. Let $\beta : \Lambda \times \Lambda \rightarrow B_1$ be a bilinear form and let $G_{(\Lambda,\beta)} \subset GL_\Lambda$ be the subscheme of GL_Λ of the isometries with respect to the form β. Then we check that $C_R(G_{(\Lambda,\beta)}) \otimes_{B_1} B_2 \cong C_{R\otimes_{B_1} B_2}(G_{(\Lambda\otimes_{B_1} B_2,\, \beta\otimes_{B_1} B_2)})$.

Consider the bilinear form:

$$\psi \; : \; \Lambda \times \Lambda \, \rightarrow \, \mathbb{Z} \tag{7.40}$$

associated with the variety A. Abusing notation sligthly, we will denote by ψ the Riemann form $\psi \otimes_{\mathbb{Z}} \mathbb{Q}$, i.e., we put:

$$\psi \; : \; V \times V \, \rightarrow \, \mathbb{Q}.$$

Consider the group scheme $C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)})$ over $Spec\, \mathbb{Z}$. Since $C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)}) \otimes_{\mathbb{Z}} \mathbb{Q} = C_D(Sp_{(V,\, \psi)})$ (see Remark 7.39), there is an open imbedding in the l-adic topology:

$$C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)})(\mathbb{Z}_l) \subset C_D(Sp_{(V,\, \psi)})(\mathbb{Q}_l). \tag{7.41}$$

Note that the form ψ_l of (4.1) is obtained by tensoring (7.40) with $\mathbb{Z}_l$.

Theorem 7.42. *If A is an abelian variety of class $\mathcal{A}$, then for every prime number l, $\rho_l(G_F)$ is open in the group*

$$C_{\mathcal{R}}(GSp_{(\Lambda,\, \psi)})(\mathbb{Z}_l) = C_{\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_l}(GSp_{(T_l(A),\, \psi_l)})(\mathbb{Z}_l).$$

In addition, for $l \gg 0$ we have:

$$\rho_l(\overline{G_F'}) \;\; = \;\; C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)})(\mathbb{Z}_l). \tag{7.43}$$

Proof. For any ring with identity R the group $GSp_{2g}(R)$ is generated by subgroups $Sp_{2g}(R)$ and

$$\{ \begin{pmatrix} aI_g & 0 \\ 0 & I_g \end{pmatrix} ; \, a \in R^{\times} \}.$$

One checks easily that the group $\mathbb{Z}_l^{\times} Sp_{2g}(\mathbb{Z}_l)$ has index 2 (index 4 resp.) in $GSp_{2g}(\mathbb{Z}_l)$, for $l > 2$ (for $l = 2$ resp.). Here the symbol $\mathbb{Z}_l^{\times}$ stands for the subgroup of homotheties in $GL_{2g}(\mathbb{Z}_l)$. Since by assumption A has a principal polarization, $Sp_{2g}(\mathbb{Z}_l) \cong Sp_{(\Lambda,\, \psi)})(\mathbb{Z}_l)$. By [Bo], Cor. 1. on p. 702, there is an open subgroup $U \subset \mathbb{Z}_l^{\times}$ such that $U \subset \rho_l(G_F)$. Hence $U\, C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)})(\mathbb{Z}_l) = C_{\mathcal{R}}(U\, Sp_{(\Lambda,\, \psi)}(\mathbb{Z}_l))$ is an open subgroup of $C_{\mathcal{R}}(GSp_{(\Lambda,\, \psi)})(\mathbb{Z}_l) = C_{\mathcal{R}}(GSp_{(\Lambda,\, \psi)}(\mathbb{Z}_l))$. By [Bo], Th. 1, p. 701, the group $\rho_l(G_F)$ is open in $G_l^{alg}(\mathbb{Q}_l)$. By Theorem 7.12, Corollary 7.19 and Remark 7.3

$$U\, C_{\mathcal{R}}(Sp_{(\Lambda,\, \psi)})(\mathbb{Z}_l) \;\; \subset \;\; \mathbb{Q}_l^{\times}\, C_D(Sp_{(V,\, \psi)})(\mathbb{Q}_l) \;\; =$$

$$= \;\; \mathbb{G}_m(\mathbb{Q}_l) H(A)(\mathbb{Q}_l) \subset MT(A)(\mathbb{Q}_l) = G_l^{alg}(\mathbb{Q}_l). \tag{7.44}$$

Hence, $U\, C_{\mathcal{R}}(Sp_{(\Lambda,\,\psi)})(\mathbb{Z}_l) \cap \rho_l(G_F)$ is open in $U\, C_{\mathcal{R}}(Sp_{(\Lambda,\,\psi)})(\mathbb{Z}_l)$ and we get that $\rho_l(G_F)$ is open in $C_{\mathcal{R}}(GSp_{(\Lambda,\,\psi)})(\mathbb{Z}_l)$. Using Remark 7.39 and the universality of the fiber product, we observe that

$$C_{\mathcal{R}}(Sp_{(\Lambda,\,\psi)})(\mathbb{Z}_l) = C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(Sp_{(T_l(A),\,\psi_l)})(\mathbb{Z}_l). \tag{7.45}$$

For $l \gg 0$ we get

$$C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(Sp_{(T_l(A),\,\psi_l)}) \;\cong\; C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(C_{\mathcal{O}_E\otimes_{\mathbb{Z}}\mathbb{Z}_l}(Sp_{(T_l(A),\,\psi_l)})) \;\cong$$

$$\cong\; C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(\prod_{\lambda | l} R_{\mathcal{O}_\lambda/\mathbb{Z}_l}(Sp_{(T_\lambda(A),\,\psi_\lambda)})). \tag{7.46}$$

Evaluating the group schemes in (7.46) on $Spec\, \mathbb{Z}_l$ we get

$$C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(Sp_{(T_l(A),\,\psi_l)})(\mathbb{Z}_l) \;\cong\; C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(\prod_{\lambda | l} R_{\mathcal{O}_\lambda/\mathbb{Z}_l}(Sp_{(T_\lambda(A),\,\psi_\lambda)}))(\mathbb{Z}_l) \;\cong$$

$$\cong\; \prod_{\lambda | l} C_{\mathcal{R}_\lambda} Sp_{(T_\lambda(A),\,\psi_\lambda)}(\mathcal{O}_\lambda) \;\cong\; \prod_{\lambda | l} Sp_{(T_\lambda,\,\psi_\lambda)}(\mathcal{O}_\lambda) \cong \prod_{\lambda | l} Sp_{2h}(\mathcal{O}_\lambda). \tag{7.47}$$

Hence by (7.45), (7.46), (7.47), (6.18) and Theorem 7.38, we conclude that for $l \gg 0$ the equality (7.43) holds. □

Theorem 7.48. *If A is an abelian variety of class $\mathcal{A}$, then for every prime number l, the group $\rho_l(G_F)$ is open in the group $\mathcal{G}_l^{alg}(\mathbb{Z}_l)$ in the l-adic topology.*

Proof. By Theorem 7.42 the group $\rho_l(G_F)$ is open in $C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(GSp_{(T_l(A),\,\psi_l)})(\mathbb{Z}_l)$ in the l-adic topology, so $\rho_l(G_F)$ has a finite index in the group $C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(GSp_{(T_l(A),\,\psi_l)})(\mathbb{Z}_l)$. By the definition of $\mathcal{G}_l^{alg}$, we have:

$$\rho_l(G_F) \subset \mathcal{G}_l^{alg}(\mathbb{Z}_l) \subset C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(GSp_{(T_l(A),\,\psi_l)})(\mathbb{Z}_l).$$

Hence, $\rho_l(G_F)$ has a finite index in $\mathcal{G}_l^{alg}(\mathbb{Z}_l)$, and the claim follows since $C_{\mathcal{R}\otimes_{\mathbb{Z}}\mathbb{Z}_l}(GSp_{(T_l(A),\,\psi_l)})(\mathbb{Z}_l)$ is a profinite group. □

Acknowledgements. The first author would like to thank G. Faltings for conversations concerning l-adic representations associated with abelian varieties. The first and the second authors would like to thank Mathematics Department of Ohio State University and Max Planck Institut in Bonn for financial support during visits in 2003 and 2004. The second author thanks the CRM in Barcelona for the hospitality during the visit in June and July 2004. The research has been partially sponsored by a KBN grant 1 P03A 027 27 and by Marie Curie Research Training Network "Arithmetic Algebraic Geometry" MRTN-CT-2003-504917.

References

[Ab] S. Abdulali, *Hodge structures on abelian varieties of type III*, Annals of Math. **155** (2002), 915-928.

[A] E. Artin, *Theory of Algebraic Numbers*, notes by Gerhard Würges, Göttingen (1959).

[BGK] G.Banaszak, W.Gajda, P.Krasoń, *On Galois representations for abelian varieties with complex and real multiplications*, Journal of Number Theory 100, no. 1 (2003), 117-132.

[Bo] F.A. Bogomolov, *Sur l'algébricité des représentations l-adiques*, vol. 290, C.R.Acad.Sci. Paris Sér. A-B, 1980.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, 21, Springer-Verlag, 1990.

[B] N. Bourbaki, *Groupes et algèbres de Lie*, Hermann, 1975.

[C1] W. Chi, *l-adic and λ-adic representations associated to abelian varieties defined over a number field*, American Jour. of Math. **114, No. 3** (1992), 315-353.

[C2] W. Chi, *On the Tate modules of absolutely simple abelian varieties of Type II*, Bulletin of the Institute of Mathematics Acadamia Sinica **18, No. 2** (1990), 85-95.

[D] P. Deligne, *Hodge cycles on abelian varieties*, Lecture Notes in Mathematics **900** (1982), 9-100.

[SGA3] dirigé par M. Demazure, A. Grothendieck, *Schémas en Groupes III*, LNM 151, 152, 153, Springer-Verlag, 1970.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zalhkörpern*, Inv. Math. **73** (1983), 349-366.

[G] B. Gordon, *A survey of the Hodge Conjecture for abelian varieties*, Appendix B in "A survey of the Hodge conjecture", by J. Lewis (1999), AMS, 297-356.

[H] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer Verlag, New York, Heidelberg, Berlin (1977).

[H1] J.E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, 1975.

[H2] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, 1972.

[I] T. Ichikawa, *Algebraic groups associated with abelian varieties*, Math. Ann **289** (1991), 133-142.

[K] S.L. Kleiman, *Algebraic cycles and the Weil conjectures in Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, Masson and CIE, Paris, North-Holland Amsterdam **3** (1968), 359-386.

[LP1] M. Larsen, R. Pink, *Abelian varieties, l-adic representations and l independence* **302** (1995), Math. Annalen, 561-579.

[LP2] M. Larsen, R. Pink, *A connectedness criterion for l-adic representations* **97** (1997), Israel J. of Math, 1-10.

[La] S. Lang, *Complex Multiplication*, Springer Verlag, 1983.

[Mi] J.S. Milne, *Abelian varieties Arithmetic Geometry G. Cornell, J.H. Silverman (eds.)* (1986), Springer-Verlag, 103-150.

[M] D. Mumford, *Abelian varieties*, Oxford University Press, 1988.

[Mu] V.K. Murty, *Exceptional Hodge classes on certain abelian varieties*, Math. Ann. **268** (1984), 197-206.

[No] M. V. Nori, *On subgroups of* $GL_n(\mathbb{F}_p)$, Invent. Math. **88** (1987), 257-275.

[O] T. Ono, *Arithmetic of algebraic tori*, Annals of Mathematics **74. No. 1** (1961), 101-139.

[P] R. Pink, *l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. reine angew. Math. **495** (1998), 187-237.

[Po] H. Pohlmann, *Algebraic cycles on abelian varieties of complex multiplication type*, Annals of Math. **88** (1968), 161-180.

[R] I. Reiner, *Maximal orders*, Academic Press, London, New York, San Francisco, 1975.

[R1] K. A. Ribet, *Galois action on division points of abelian varieties with real multiplications*, American Jour. of Math. **98, No. 3** (1976), 751-804.

[R2] K. A. Ribet, *Hodge classes on certain types of abelian varieties*, American Jour. of Math. **105, No. 2** (1983), 523-538.

[Sch] S.S. Schatz, *Group schemes, Formal groups, and p-divisible Groups*, in Arithmetic geometry by G.Cornell and J.H. Silverman (eds.) (1986), 29-78.

[Se] J.P. Serre, *Abelian l-adic representations and elliptic curves*, McGill University Lecture Notes, W.A. Benjamin, New York, Amsterdam (1968).

[Se1] J.P. Serre, *Résumés des cours au Collège de France*, Annuaire du Collège de France (1985-1986), 95-100.

[Se2] J.P. Serre, *Lettre à Daniel Bertrand du 8/6/1984*, Oeuvres. Collected papers. IV. (1985 - 1998), Springer-Verlag, Berlin, 21 - 26.

[Se3] J.P. Serre, *Lettre à Marie-France Vignéras du 10/2/1986*, Oeuvres. Collected papers. IV. (1985-1998), Springer-Verlag, Berlin, 38-55.

[Se4] J.P. Serre, *Lettres à Ken Ribet du 1/1/1981 et du 29/1/1981*, Oeuvres. Collected papers. IV. (1985-1998), Springer-Verlag, Berlin, 1-20.

[Se5] J.P. Serre, *Représentations l-adiques, in "Algebraic Number Theory" (ed. S.Iyanaga)* (1977), Japan Society for the promotion of Science, 177-193.

[Se6] J.P. Serre, *Deux Lettres de Serre*, Soc. Math. France 2e série no. 2 (1980), 95-102.

[Se7] J.P. Serre, *Lie algebras and Lie groups*, The Benjamin/Cummings Publishing Company (1981).

[Se8] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[ST] J.P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Math. **68** (1968), 492-517.

[Ta1] S.G. Tankeev, *On algebraic cycles on surfaces and abelian varieties*, Mathematics of the USSR, Izvestiya (Translation of Izv. Acad. Nauk SSSR. Ser. Mat. 45, 1981) **18** (1982), 349-380.

[Ta2] S.G. Tankeev, *Cycles on simple abelian varieties of prime dimension over number fields*, Mathematics of the USSR, Izvestiya (Translation of Izv. Acad. Nauk SSSR, Ser. Mat. v. 55, 1987) **31** (1988), 527-540.

[Ta3] S.G. Tankeev, *On the Mumford-Tate conjecture for abelian varieties*, Algebraic Geometry 4, J. Math. Sci **81 no. 3** (1996), 2719-2737.

[Ta4] S.G. Tankeev, *Abelian varieties and the general Hodge conjecture*, Mathematics of the USSR, Izvestiya (Translation of Izv. Acad. Nauk SSSR. Ser. Mat. 57, 1993) **43** (1994), 179-191.

[Ta5] S.G. Tankeev, *Cycles on simple abelian varieties of prime dimension.*, Izv. Akad. Nauk SSSR Ser. Mat. **46 no. 1** (1982), 155–170.

[T1] J. Tate, *Algebraic cycles and poles of zeta functions in Arithmetical Algebraic Geometry*, O.F.G Schilling (ed.), New York: Harper and Row (1965), 93-110.

[T2] J. Tate, *p-divisible groups, proceedings of the Conference on local Fields*, Springer-Verlag (1968).

[Va1] A. Vasiu, *Surjectivity Criteria for p-adic Representations, Part I*, Manuscripta Math. **112** (2003), 325-355.

[Va2] A. Vasiu, *Surjectivity Criteria for p-adic Representations, Part II*, Manuscripta Math. **114** (2004), 399-422.

[V1] V.E. Voskresensky, *Algebraiceskije tory*, Izdatelstvo "Nauka", 1977.

[V2] V.E. Voskresensky, *Algebraic groups and their birational invariants*, Translation of Mathematical Monographs vol. **179**, AMS, 1998.

[W1] A. Weil, *The field of definition of a variety*, American Journal of Math. **56** (1956), 509-524.

[W2] A. Weil, *Adeles and algebraic groups*, Progress in Mathematics vol. **23**, Birkhäuser, 1982.

[Wi] J. P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1-16.

[Za] Y.G. Zarhin, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction*, Invent. Math. **79** (1985), 309-321.

G. Banaszak
Department of Mathematics
Adam Mickiewicz University
Poznań
Poland
banaszak@amu.edu.pl

W. Gajda
Department of Mathematics
Adam Mickiewicz University
Poznań
Poland
gajda@amu.edu.pl

P. Krasoń
Department of Mathematics
Szczecin University
Szczecin
Poland
krason@sus.univ.szczecin.pl

Admissible p-adic Measures Attached to Triple Products of Elliptic Cusp Forms

To dear John Coates for his sixtieth birthday

Siegfried Böcherer*, A. A. Panchishkin†

Received: August 26, 2005
Revised: February 16, 2006

Abstract. We use the Siegel-Eisenstein distributions of degree three, and their higher twists with Dirichlet characters, in order to construct admissible p-adic measures attached to the triple products of elliptic cusp forms. We use an integral representation of Garrett's type for triple products of three cusp eigenforms. For a prime p and for three primitive cusp eigenforms f_1, f_2, f_3 of equal weights $k_1 = k_2 = k_3 = k$, we study the critical values of Garrett's triple product $L(f_1 \otimes f_2 \otimes f_3, s, \chi)$ twisted with Dirichlet characters χ. The result is stated in framework of a general program by John Coates, see [Co], [Co-PeRi].

2000 Mathematics Subject Classification: 11F60, 11S80
Keywords and Phrases: Siegel-Eisenstein series, triple products, admissible measures

0 Introduction

The purpose of this paper is to give a construction of p-adic admissible measures (in the sense of Amice-Vélu) attached to Garrett's triple L-function attached to three primitive cusp eigenforms of equal weight k, where p is a prime. For this purpose we use the theory of p-adic integration with values in spaces of *nearly-holomorphic modular forms* (in the sense of Shimura, see [ShiAr]) over a normed $\mathcal{O}$-algebra A where $\mathcal{O}$ is the ring of integers in a finite extension K of $\mathbb{Q}_p$. Often we simply assume that $A = \mathbb{C}_p$.

*Supported by a French-German cooperation program by J.-P. Demailly (Institut Fourier, Grenoble)

†Supported by DFG - Forschergruppe "Arithmetik Heidelberg-Mannheim"

0.1 Generalities on triple products

Consider three primitive cusp eigenforms

$$f_j(z) = \sum_{n=1}^{\infty} a_{n,j} e(nz) \in \mathcal{S}_{k_j}(N_j, \psi_j),\ (j = 1, 2, 3) \tag{0.1}$$

of weights k_1, k_2, k_3, of conductors N_1, N_2, N_3, and of nebentypus characters $\psi_j \bmod N_j$ $(j = 1, 2, 3)$, and let χ denote a Dirichlet character.
The triple product twisted with Dirichlet characters χ is defined as the following complex L-function (an Euler product of degree eight):

$$L^S(f_1 \otimes f_2 \otimes f_3, s, \chi) = \prod_{p \notin S} L((f_1 \otimes f_2 \otimes f_3)_p, \chi(p)p^{-s}),\ \text{where} \tag{0.2}$$

$$L((f_1 \otimes f_2 \otimes f_3)_p, X)^{-1} = \tag{0.3}$$

$$\det\left(1_8 - X \begin{pmatrix} \alpha_{p,1}^{(1)} & 0 \\ 0 & \alpha_{p,1}^{(2)} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{p,2}^{(1)} & 0 \\ 0 & \alpha_{p,2}^{(2)} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{p,3}^{(1)} & 0 \\ 0 & \alpha_{p,3}^{(2)} \end{pmatrix}\right)$$
$$= \prod_{\eta} (1 - \alpha_{p,1}^{(\eta(1))} \alpha_{p,2}^{(\eta(2))} \alpha_{p,3}^{(\eta(3))} X), \quad \eta : \{1, 2, 3\} \to \{1, 2\},\ \text{and}$$

$$1 - a_{p,j}X - \psi_j(p)p^{k_j-1}X^2 = (1 - \alpha_{p,j}^{(1)}(p)X)(1 - \alpha_{p,j}^{(2)}(p)X), \quad j = 1, 2, 3,$$

are the Hecke p–polynomials of forms f_j and the product is extended over all primes $p \notin S$, and $S = \mathrm{Supp}(N_1N_2N_3)$ denotes the set of all prime divisors of the product $N_1N_2N_3$. We always assume that

$$k_1 \geq k_2 \geq k_3, \tag{0.4}$$

including the case of equal weights $k_1 = k_2 = k_3 = k$.
We use the corresponding normalized motivic L function (see [De79], [Co], [Co-PeRi]), which in the case of "balanced" weights (i.e. $k_1 \leq k_2 + k_3 - 2$) has the form:

$$\Lambda^S(f_1 \otimes f_2 \otimes f_3, s, \chi) = \tag{0.5}$$
$$\Gamma_{\mathbb{C}}(s)\Gamma_{\mathbb{C}}(s - k_3 + 1)\Gamma_{\mathbb{C}}(s - k_2 + 1)\Gamma_{\mathbb{C}}(s - k_1 + 1)L(f_1 \otimes f_2 \otimes f_3, s, \chi),$$

where $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$. The motivic Gamma-factor

$$\Gamma_{\mathbb{C}}(s)\Gamma_{\mathbb{C}}(s - k_3 + 1)\Gamma_{\mathbb{C}}(s - k_2 + 1)\Gamma_{\mathbb{C}}(s - k_1 + 1)$$

determines the critical values $s = k_1, \cdots, k_2 + k_3 - 2$ and a (conjectural) functional equation of the form: $s \mapsto k_1 + k_2 + k_3 - 2 - s$.
Throughout the paper we fix an embedding

$$i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p,\ \text{and define} \tag{0.6}$$

$$\lambda(p) = \alpha_{p,1}^{(1)}\alpha_{p,2}^{(1)}\alpha_{p,3}^{(1)},\ \text{where we assume that}\ |i_p(\alpha_{p,j}^{(1)})| \leq |i_p(\alpha_{p,j}^{(2)})|, j = 1, 2, 3. \tag{0.7}$$

0.2 Statement of main results

For a fixed positive integer $N \in \mathbb{N}$ consider the profinite group

$$Y = Y_{N,p} = \varprojlim_{v} Y_v, \quad \text{where} \quad Y_v = (\mathbb{Z}/Np^v\mathbb{Z})^\times.$$

There is a natural projection $y_p : Y \to \mathbb{Z}_p^\times$. Let us fix a normed $\mathcal{O}$-algebra A where $\mathcal{O}$ is the ring of integers in a finite extension K of $\mathbb{Q}_p$.

Definition 0.1 (a) *For $h \in \mathbb{N}, h \geq 1$ let $\mathcal{P}^h(Y, A)$ denote the A-module of locally polynomial functions of degree $< h$ of the variable $y_p : Y \to \mathbb{Z}_p^\times \hookrightarrow A^\times$; in particular,*

$$\mathcal{P}^1(Y, A) = \mathcal{C}^{loc-const}(Y, A)$$

(the A-submodule of locally constant functions). We adopt the notation $\Phi(\mathcal{U}) := \Phi(\chi_{\mathcal{U}})$ for the characteristic function $\chi_{\mathcal{U}}$ of an open subset $\mathcal{U} \subset Y$. Let also denote $\mathcal{C}^{loc-an}(Y, A)$ the A-module of locally analytic functions and $\mathcal{C}(Y, A)$ the A-module of continuous functions so that

$$\mathcal{P}^1(Y, A) \subset \mathcal{P}^h(Y, A) \subset \mathcal{C}^{loc-an}(Y, A) \subset \mathcal{C}(Y, A).$$

(b) *For a given positive integer h we define an h-admissible measure on Y with values in an A-module M as a homomorphism of A-modules:*

$$\tilde{\Phi} : \mathcal{P}^h(Y, A) \to M,$$

such that for all $a \in Y$ and for $v \to \infty$

$$\left| \int_{a+(Np^v)} (y_p - a_p)^j d\tilde{\Phi} \right|_{p,M} = o(p^{-v(j-h)}) \quad \text{for all} \quad j = 0, 1, \cdots, h-1,$$

where $a_p = y_p(a)$.

We adopt the notation $(a)_v = a + (Np^v)$ for both an element of Y_v and the corresponding open compact subset of Y.

U_p–Operator and Method of Canonical projection.

In Section 2.2, we construct an h-admissible measure $\widetilde{\Phi}^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}(A)$ out of a sequence of distributions

$$\Phi_r : \mathcal{P}^1(Y, A) \to \mathcal{M}(A)$$

with values in an A-module $M = \mathcal{M}(A)$ of nearly-holomorphic triple modular forms over A (for all $r \in \mathbb{N}$ with $r \leq h-1$), where $\lambda \in A^\times$ is a fixed non-zero eigenvalue of triple Atkin's operator $U_T = U_{T,p}$, acting on $\mathcal{M}(A)$, and

$h = [2\mathrm{ord}_p\lambda(p)] + 1$. In our case $\mathcal{M}(A) \subset A[\![q_1, q_2, q_3]\!][R_1, R_2, R_3]$, and such modular forms are formal series

$$g = \sum_{n_1,n_2,n_3=0}^{\infty} a(n_1, n_2, n_3; R_1, R_2, R_3) q_1^{n_1} q_2^{n_2} q_3^{n_3} \in A[\![q_1, q_2, q_3]\!][R_1, R_2, R_3]$$

such that for $A = \mathbb{C}$, for all $z_j = x_j + iy_j \in \mathbb{H}$ and for $R_j = (4\pi y_j)^{-1}$ the series converges to a $\mathcal{C}^\infty$-modular form on $\mathbb{H}^3$ of a given weight (k, k, k) and character (ψ_1, ψ_2, ψ_3), $j = 1, 2, 3$. The usual action of $U = U_p$ on elliptic modular forms of one variable extends to triple Atkin's operator $U_T = U_{T,p} = (U_p)^{\otimes 3}$ acting on triple modular forms by

$$U_T(g) = \sum_{n_1,n_2,n_3=0}^{\infty} a(pn_1, pn_2, pn_3; pR_1, pR_2, pR_3) q_1^{n_1} q_2^{n_2} q_3^{n_3}. \tag{0.8}$$

We consider the canonical projection operator $\pi_\lambda : \mathcal{M}(A) \to \mathcal{M}(A)^\lambda$ onto the maximal A-submodule $\mathcal{M}(A)^\lambda$ over which the operator $U_T - \lambda I$ is nilpotent, and such that $\mathrm{Ker}\,\pi_\lambda = \bigcap_{n\geq 1} \mathrm{Im}\,(U_T - \lambda I)^n$. We define an A-linear map

$$\widetilde{\Phi}^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}(A)$$

on local monomials y_p^j by

$$\int_{(a)_v} y_p^j \, d\widetilde{\Phi}^\lambda = \pi_\lambda(\Phi_j((a)_v))$$

where $\Phi_j : \mathcal{P}^1(Y, A) \to \mathcal{M}(A)$ is a sequence of $\mathcal{M}(A)$-valued distributions on Y (for $j = 0, 1, \ldots, h-1$). Recall that for a primitive cusp eigenform $f_j = \sum_{n=1}^\infty a_n(f) q^n$ of conductor $C = C_{f_j}$, the function $f_{j,0} = \sum_{n=1}^\infty a_n(f_{j,0}) q^n \in \overline{\mathbb{Q}}[\![q]\!]$ is defined as an eigenfunction of $U = U_p$ with the eigenvalue $\alpha_{p,j}^{(1)} \in \overline{\mathbb{Q}}$ $(U(f_0) = \alpha f_0)$ which satisfies the identity

$$f_{j,0} = f_j - \alpha_{p,j}^{(2)} f_j | V_p = f_j - \alpha_{p,j}^{(2)} p^{-k/2} f_j | \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \tag{0.9}$$
$$\sum_{n=1}^\infty a_n(f_{j,0}) n^{-s} = \sum_{\substack{n=1 \\ p\nmid n}}^\infty a_n(f_j) n^{-s} (1 - \alpha_{p,j}^{(1)} p^{-s})^{-1}.$$

For any fixed $n_0 = n \cdot p^m$ with $p \nmid n$ we have $a_{n_0}(f_{j,0}) = a_n(f_j) \cdot (\alpha_{p,j}^{(1)})^m \in \overline{\mathbb{Q}}$ and $a_n(f_j)$ are eigenvalues of Hecke operators T_n. Therefore, $U_T(f_{1,0} \otimes f_{2,0} \otimes f_{3,0}) = \lambda(f_{1,0} \otimes f_{2,0} \otimes f_{3,0})$. Moreover,

$$f_j^0 = f_{j,0}^\rho \Big|_k \begin{pmatrix} 0 & -1 \\ Np & 0 \end{pmatrix}, \text{ where } f_{j,0}^\rho = \sum_{n=1}^\infty \overline{a(n, f_0)} q^n. \tag{0.10}$$

Consider the triple product defined by (0.2) as an Euler product of degree eight: $\mathcal{D}(f_1 \otimes f_2 \otimes f_3, s, \chi) = L^{(N)}(f_1 \otimes f_2 \otimes f_3, s, \chi)$, attached to three cusp eigenforms $f_j(z) = \sum_{n=1}^{\infty} a_{n,j} e(nz) \in \mathcal{S}_{k_j}(N_j, \psi_j)$, $(j = 1, 2, 3)$ of weight k, of conductors N_1, N_2, N_3, and of nebentypus characters $\psi_j \bmod N_j$ $(j = 1, 2, 3)$, where $\chi \bmod Np^v$ is an arbitrary Dirichlet character, and the notation $L^{(N)}$ means that the local factors at primes dividing $N = \mathrm{LCM}(N_1, N_2, N_2)$ are removed from an Euler product. Before giving the precise statements of our results on p-adic triple L-functions, we describe in more detail critical values of the L function $\mathcal{D}(f_1 \otimes f_2 \otimes f_3, s, \chi)$.

Let us introduce the following normalized L-function

$$\begin{aligned}&\mathcal{D}^\star(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, s + 2k - 2, \psi_1\psi_2\chi) = \\ &\Gamma_{\mathbb{C}}(s + 2k - 2)\Gamma_{\mathbb{C}}(s + k - 1)^3 L^{(N)}(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, s + 2k - 2, \psi_1\psi_2\chi),\end{aligned} \tag{0.11}$$

where $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$, and $\Gamma_{\mathbb{C}}(s + 2k - 2)\Gamma_{\mathbb{C}}(s + k - 1)^3$ is the motivic Gamma-factor (compare with (0.5), and see [Co], [Co-PeRi], [Pa94]). For an arbitrary Dirichlet character $\chi \bmod Np^v$ consider the following Dirichlet characters:

$$\begin{aligned}&\chi_1 \bmod Np^v = \chi,\ \chi_2 \bmod Np^v = \psi_2\bar{\psi}_3\chi, \\ &\chi_3 \bmod Np^v = \psi_1\bar{\psi}_3\chi, \boldsymbol{\psi} = \chi^2\psi_1\psi_2\overline{\psi}_3;\end{aligned} \tag{0.12}$$

later on we impose the condition that the conductors of the corresponding primitive characters $\chi_{0,1}, \chi_{0,2}, \chi_{0,3}$ are Np-complete (i.e., have the same prime divisors as those of Np).

Theorem A (Algebraic properties of the triple product) *Assume that $k \geq 2$. Then for all pairs (χ, r) such that the corresonding Dirichlet characters χ_j are Np-complete, and $0 \leq r \leq k - 2$, we have that*

$$\frac{\mathcal{D}^\star(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, 2k - 2 - r, \psi_1\psi_2\chi)}{\langle f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, f_1^\rho \otimes f_2^\rho \otimes f_3^\rho\rangle_T} \in \overline{\mathbb{Q}}$$

where

$$\begin{aligned}\langle f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, f_1^\rho \otimes f_2^\rho \otimes f_3^\rho\rangle_T &:= \langle f_1^\rho, f_1^\rho\rangle_N \langle f_2^\rho, f_2^\rho\rangle_N \langle f_3^\rho, f_3^\rho\rangle_N \\ &= \langle f_1, f_1\rangle_N \langle f_2, f_2\rangle_N \langle f_3, f_3\rangle_N.\end{aligned}$$

For the p-adic construction, let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ denote the completion of an algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers. Fix a positive integer N, a Dirichlet character $\psi \bmod N$ and consider the commutative profinite group $Y = Y_{N,p} = \varprojlim_m (\mathbb{Z}/Np^m\mathbb{Z})^*$ and its group $X_{N,p} = \mathrm{Hom}_{cont}(Y, \mathbb{C}_p^\times)$ of (continuous) p-adic characters (this is a $\mathbb{C}_p$-analytic Lie group). The group $X_{N,p}$ is isomorphic to a finite union of discs $U = \{z \in \mathbb{C}_p \mid |z|_p < 1\}$.

A p-adic L-function $L_{(p)} : X_{N,p} \to \mathbb{C}_p$ is a certain meromorphic function on $X_{N,p}$. Such a function often come from a p-adic measure $\mu_{(p)}$ on Y (*bounded* or *admissible* in the sense of Amice-Vélu, see [Am-V]). In this case we write for all $x \in X_{N,p}$

$$L_{(p)}(x) = \int_{Y_{N,p}} x(y) \mathrm{d}\mu_{(p)}(y)$$

In order to establish p-adic properties, let us use the product (0.7) $\lambda = \lambda(p) = \alpha_{p,1}^{(1)} \alpha_{p,2}^{(1)} \alpha_{p,3}^{(1)}$, where we assume that $|i_p(\alpha_{p,j}^{(1)})| \le |i_p(\alpha_{p,j}^{(2)})|, j = 1, 2, 3$.

Theorem B (on admissible measures attached to the triple product). *Under the assumptions as above there exist a $\mathbb{C}_p$-valued measure $\tilde{\mu}^{\lambda}_{f_1 \otimes f_2 \otimes f_3}$ on $Y_{N,p}$, and a $\mathbb{C}_p$-analytic function*

$$\mathcal{D}_{(p)}(x, f_1 \otimes f_2 \otimes f_3) : X_p \to \mathbb{C}_p,$$

given for all $x \in X_{N,p}$ by the integral

$$\mathcal{D}_{(p)}(x, f_1 \otimes f_2 \otimes f_3) = \int_{Y_{N,p}} x(y) \mathrm{d}\tilde{\mu}^{\lambda}_{f_1 \otimes f_2 \otimes f_3}(y),$$

and having the following properties:
(i) *for all pairs (r, χ) such that $\chi \bmod C_\chi$ is a primitive Dirichlet character modulo C_χ, $\chi \in X_{N,p}^{\mathrm{tors}}$, assuming that all three corresonding Dirichlet characters χ_j given by (0.12) have Np-complete conductor* $(j = 1, 2, 3)$, *and $r \in \mathbb{Z}$ is an integer with $0 \le r \le k-2$, the following equality holds:*

$$\begin{aligned} &\mathcal{D}_{(p)}(\chi x_p^r, f_1 \otimes f_2 \otimes f_3) = \qquad (0.13)\\ &i_p\Big(\frac{(\psi_1\psi_2)(2) C_\chi^{4(2k-2-r)}}{G(\chi_1)G(\chi_2)G(\chi_3)G(\psi_1\psi_2\chi_1)\lambda(p)^{2v}} \\ &\qquad \frac{\mathcal{D}^\star(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, 2k-2-r, \psi_1\psi_2\chi)}{\langle f_1^0 \otimes f_2^0 \otimes f_3^0, f_{1,0} \otimes f_{2,0} \otimes f_{3,0}\rangle_{T,Np}}\Big) \end{aligned}$$

where $v = \mathrm{ord}_p(C_\chi)$, $\chi_1 \bmod Np^v = \chi$, $\chi_2 \bmod Np^v = \psi_2\bar{\psi}_3\chi, \chi_3 \bmod Np^v = \psi_1\bar{\psi}_3\chi$, $G(\chi)$ denotes the Gauß sum of a primitive Dirichlet character χ_0 attached to χ (modulo the conductor of χ_0).
(ii) *if $\mathrm{ord}_p\lambda(p) = 0$ then the holomorphic function in (i) is a bounded $\mathbb{C}_p$-analytic function;*
(iii) *in the general case (but assuming that $\lambda(p) \neq 0$) the holomorphic function in (i) belongs to the type $o(\log(x_p^h))$ with $h = [2\mathrm{ord}_p\lambda(p)] + 1$ and it can be represented as the Mellin transform of the h-admissible $\mathbb{C}_p$-valued measure $\tilde{\mu}^{\lambda}_{f_1 \otimes f_2 \otimes f_3}$ (in the sense of Amice-Vélu) on Y*
(iv) *if $h \le k-2$ then the function $\mathcal{D}_{(p)}$ is uniquely determined by the above conditions (i).*

Remark 0.2 *It was checked by B.Gorsse and G.Robert that*

$$\langle f_1^{0,\rho} \otimes f_2^{0,\rho} \otimes f_3^{0,\rho}, f_{1,0}^\rho \otimes f_{2,0}^\rho \otimes f_{3,0}^\rho\rangle_{T,Np} = \beta \cdot \langle f_1, f_1\rangle_N \langle f_2, f_2\rangle_N \langle f_3, f_3\rangle_N$$

for some $\beta \in \overline{\mathbb{Q}}^*$ (see [Go-Ro]).

0.3 Scheme of the Proof

We construct $\overline{\mathbb{Q}}$-valued distributions denoted by $\mu_{f_1\otimes f_2\otimes f_3,r}$ on the profinite group $Y_{N,p}$, and attached to the special values at $s = 2k-2-r$ with $0 \le r \le k-2$ of the triple product $L(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, s, \psi_1\psi_2\chi)$ twisted with a Dirichlet character $\psi_1\psi_2\chi \bmod Np^v$. We use an integral representation of this special value in terms of a $\mathcal{C}^\infty$-Siegel-Eisenstein series $F_{\chi,r}$ of degree 3 and of weight k (to be specified later), where $0 \le r \le k-2$. Such a series $F_{\chi,r}$ depends on the character χ, but its precise nebentypus character is $\boldsymbol{\psi} = \chi^2\psi_1\psi_2\overline{\psi}_3$, and it is defined by $F_{\chi,r} = G^\star(\mathcal{Z}, -r; k, (Np^v)^2, \boldsymbol{\psi})$, where $\mathcal{Z}$ denotes a variable in the Siegel upper half space $\mathbb{H}_3$, and the normalized series $G^\star(\mathcal{Z}, s; k, (Np^v)^2, \boldsymbol{\psi})$ is given by (A.12). This series depends on $s = -r$, and for the critical values at integral points $s \in \mathbb{Z}$ such that $2-k \le s \le 0$, it represents a (*nearly-*) *holomorphic* Siegel modular form in the sense of Shimura [ShiAr].

Our construction consists of the following steps:

1) We consider the profinite ring $A_{N,p} = \varprojlim_v (\mathbb{Z}/Np^v\mathbb{Z})$. Starting from any sequence F_r of nearly-holomorphic Siegel modular forms we construct first a sequence Ψ_{F_r} of modular distributions on the additive profinite group

$$S = S_{N,p} := \left\{ \boldsymbol{\varepsilon} = \begin{pmatrix} 0 & \varepsilon_{12} & \varepsilon_{13} \\ \varepsilon_{12} & 0 & \varepsilon_{23} \\ \varepsilon_{13} & \varepsilon_{23} & 0 \end{pmatrix} \middle| \varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23} \in A_{N,p} \right\};$$

such distributions take values in $\mathcal{C}^\infty$-(nearly-holomorphic) modular forms on the Siegel half plane $\mathbb{H}_3$. This construction, given in Section 1, generalizes the *higher twist* of F_r, already utilized in the work [Boe-Schm], in a simpler situation.

2) Next we consider the (real analytic) Siegel-Eisenstein series $F_{\chi,r}$ as a formal (nearly-holomorphic) Fourier series, whose coefficients admit explicit polynomial expressions (see Section 1 and Appendix A), and we use the fact that they may be written in terms of p-adic integrals of χ over Y (see [PaSE] and [PaIAS]).

A crucial point of our construction is the *higher twist* in Section 1. We define the higher twist of the series $F_{\chi,r}$ by the characters (0.12) as the following formal nearly-holomorphic Fourier expansion:

$$F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3} = \sum_{\mathcal{T}} \bar\chi_1(t_{12})\bar\chi_2(t_{13})\bar\chi_3(t_{23})Q(R,\mathcal{T};k-2r,r)a_{\chi,r}(\mathcal{T})q^{\mathcal{T}}. \tag{0.14}$$

The series (0.14) can be naturally interpreted as an integral of the Dirichlet character χ on the group Y with respect to a *modular distribution* Ψ_r:

$$F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3} = \int_Y \chi(y)\mathrm{d}\Psi_r(y) =: \Psi_r(\chi). \tag{0.15}$$

These modular distributions take values in the ring of formal Fourier expansion whose coefficients are polynomials in $R = (4\pi\,\mathrm{Im}\,(\mathcal{Z}))^{-1}$ over the field $\overline{\mathbb{Q}}$ (which is imbedded into $\mathbb{C}_p$ via (0.6). The distributions Ψ_r are uniformly bounded (coefficient-by-coefficient).

3) If we consider the diagonal embedding

$$\mathrm{diag} : \mathbb{H} \times \mathbb{H} \times \mathbb{H} \to \mathbb{H}_3,$$

then the restriction produces a sequence $\Phi_r = 2^r \,\mathrm{diag}^* \,\Psi_r$ of distributions on Y with values in the tensor product $\mathcal{M}_{k,r}(\overline{\mathbb{Q}}) \otimes \mathcal{M}_{k,r}(\overline{\mathbb{Q}}) \otimes \mathcal{M}_{k,r}(\overline{\mathbb{Q}})$ of three spaces of elliptic nearly-holomorphic modular forms on the Poincaré upper half plane $\mathbb{H}$ (the normalizing factor 2^r is neeeded in order to prove certain congruences between Φ_r in Section 3).

The important property of these distributions, established in Section 1, is that the nebentypus character of the triple modular form $\Phi_r(\chi)$ is fixed and is equal to (ψ_1, ψ_2, ψ_3), see Proposition 1.5. Using this property, and applying the canonical projector π_λ of Section 2 to $\Phi_r(\chi)$, we prove in Section 3 that the sequence of modular distributions Φ_r on Y produces a p-adic admissible measure $\tilde{\Phi}^\lambda$ (in the sense of Amice-Vélu, [Am-V]) with values in a finite dimensional subspace

$$\mathcal{M}^\lambda(\mathbb{C}_p) \subset \mathcal{M}(\mathbb{C}_p),\ \mathcal{M}(\mathbb{C}_p) = \mathcal{M}_{k,r}(\mathbb{C}_p) \otimes \mathcal{M}_{k,r}(\mathbb{C}_p) \otimes \mathcal{M}_{k,r}(\mathbb{C}_p)$$

of the $\mathbb{C}_p$-vector space $\mathcal{M}(\mathbb{C}_p) = \bigcup_{v \geq 0} \mathcal{M}_{k,r}(Np^v, \psi_1, \psi_2, \psi_3; \mathbb{C}_p)$ of formal nearly-holomorphic triple modular forms of levels Np^v and the fixed nebentypus characters (ψ_1, ψ_2, ψ_3). We use congruences between triple modular forms $\Phi_r(\chi) \in \mathcal{M}(\overline{\mathbb{Q}})$ (they have cyclotomic formal Fourier coefficients), and a general admissibility criterion (see Theorem 2.4). Proof of the Main Congruence is contained in Section 3.

4) Application of a $\overline{\mathbb{Q}}$-valued linear form of type

$$\mathcal{L}\ : h \longmapsto \frac{\left\langle \tilde{f}_1 \otimes \tilde{f}_2 \otimes \tilde{f}_3, h \right\rangle}{\left\langle \tilde{f}_1, \tilde{f}_1 \right\rangle \left\langle \tilde{f}_2, \tilde{f}_2 \right\rangle \left\langle \tilde{f}_3, \tilde{f}_3 \right\rangle}$$

for $h \in \mathcal{M}_{k,r}(\overline{\mathbb{Q}}) \otimes \mathcal{M}_{k,r}(\overline{\mathbb{Q}}) \otimes \mathcal{M}_{k,r}(\overline{\mathbb{Q}})$, produces a sequence of $\overline{\mathbb{Q}}$-valued distributions given by $\mu_r^\lambda(\chi) = \mathcal{L}(\pi_\lambda(\Phi_r)(\chi))$, $\lambda \in \overline{\mathbb{Q}}^\times$. More precisely, we consider three auxilliary modular forms

$$\tilde{f}_j(z) = \sum_{n=1}^{\infty} \tilde{a}_{n,j} e(nz) \in S_k(\Gamma_0(N_j p^{\nu_j}), \psi_j) \quad (1 \leq j \leq 3, \nu_j \geq 1), \qquad (0.16)$$

with the same eigenvalues as those of (0.1), for all Hecke operators T_q, with q prime to Np. In our construction we use as $\tilde{f}_j$ certain "easy transforms" of primitive cusp forms in (0.1). In particular, we choose as $\tilde{f}_j$ eigenfunctions $\tilde{f}_j = f_j^0$ of the adjoint Atkin's operator U_p^*, in this case we denote by $f_{j,0}$ the corresponding eigenfunctions of U_p. The $\overline{\mathbb{Q}}$-linear form $\mathcal{L}$ produces a $\mathbb{C}_p$-valued

admissible measure $\tilde{\mu}^\lambda = \ell(\tilde{\Phi}^\lambda)$ starting from the modular p-adic admissible measure $\tilde{\Phi}^\lambda$ of stage 3), where $\ell : \mathcal{M}(\mathbb{C}_p) \to \mathbb{C}_p$ denotes a $\mathbb{C}_p$-linear form, interpolating $\mathcal{L}$. See Section 4 for the construction of $\tilde{\mu}^\lambda$.
5) We show in Section 5 that for any suitable Dirichlet character χ mod Np^v the integral

$$\mu_r^\lambda(\chi) = \mathcal{L}(\pi_\lambda(\Phi_r(\chi)))$$

coincides (up to a normalisation) with the special L-value

$\mathcal{D}^*(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, 2k-2-r, \psi_1\psi_2\chi)$ (under the above assumptions on χ and r).

We use a general integral representation of Section B. The basic idea how a Dirichlet character χ is incorporated in the integral representation [Ga87, BoeSP] is somewhat similar to the one used in [Boe-Schm], but (surprisingly) more complicated to carry out. Note however that the existence of a $\mathbb{C}_p$-valued admissible measure $\tilde{\mu}^\lambda = \ell(\tilde{\Phi}^\lambda)$ established at stage 4), does not depend on this technical computation, and details will appear elsewhere.

Remark 0.3 *Similar techniques can be applied in the case of three arbitrary "balanced" weights (0.4) $k_1 \geq k_2 \geq k_3$, i.e. when $k_1 \leq k_2 + k_3 - 2$, using various differential operators acting on modular forms (the Maaß-Shimura differential operators (see [ShiAr], [Or]), and Ibukiyama's differential operators (see [Ibu], [BSY]). More precisely, one applies these operators to a twisted Eisenstein series. In this case the critical values of the L function $\mathcal{D}(f_1 \otimes f_2 \otimes f_3, s, \chi)$ correspond to $s = k_1, \cdots, k_2 + k_3 - 2$. The equality of weights in the present paper is made to avoid (for lack of space) the calculus of differential operators.*

0.4 Conclusion: some advantages of our p-adic method

The whole construction works in various situations and it can be split into several independent steps:

1) Construction of modular distributions Φ_r (on a profinite or even adelic space Y of type $Y = \mathbb{A}_K^*/K^*$ for a number field K) with values in an infinite dimensional modular tower $\mathcal{M}(\mathcal{A})$ over complex numbers (or in an $\mathcal{A}$-module of infinite rank over some p-adic algebra $\mathcal{A}$).

2) Application of a canonical projector of type π_λ onto a finite dimensional subspace $\mathcal{M}^\lambda(\mathcal{A})$ of $\mathcal{M}(\mathcal{A})$ (or over a locally free $\mathcal{A}$-module of finite rank over some $\mathcal{A}$) in the form: $\pi_\lambda(g) = (U^\lambda)^{-v}\pi_{\lambda,1}(U^v(g)) \in \mathcal{M}^\lambda(Np, \mathcal{A})$ as in (2.3) of Section 2 (this method works only for $\lambda \in \mathcal{A}^\times$, and gives the λ-characteristic projector of $g \in \mathcal{M}(Np^v, \mathcal{A})$ (independently of a sufficiently large v)).

3) One proves the admissibility criterium of Theorem 2.4 saying that the sequence $\pi_\lambda(\Phi_r)$ of distributions with values in $\mathcal{M}^\lambda(\mathcal{A})$ determines an h-admissible measure $\tilde{\Phi}^\lambda$ with values in this finite dimensional space for a suitable h (determined by the slope $\mathrm{ord}_p(\lambda)$).

4) Application of a linear form ℓ of type $g \mapsto \langle f^0, \pi_\lambda(g)\rangle / \langle f, f\rangle$ to the modular distributions Φ_r produces a sequence of $\mathcal{A}$-valued distributions $\mu_r^\lambda = \ell(\pi_\lambda(\Phi_r))$, and an $\mathcal{A}$-valued admissible measure. The growth condition can be verified starting from congruences between modular forms $\Phi_j(\chi)$, generalizing our Main Congruence of Section 3.

5) One shows that certain integrals $\mu_j^\lambda(\chi)$ of the constructed distributions μ_j^λ coincide with normalized L-values; however, computing these integrals is not needed for the construction of p-adic admissible measures $\tilde{\mu}^\lambda$ (which is already done at stage 4)).

6) Under some assumptions, one can show a result on uniqueness for the constructed h-admissibles measures: they are determined by the integrals $\mu_j^\lambda(\chi)$ over almost all Dirichlet characters and sufficiently many $j = 0, 1, \cdots, h-1$ (this stage is not necessary, but it is nice to have uniqueness of the construction), see [JoH05].

7) If we are lucky, we can prove a functional equation for the constructed measure $\tilde{\mu}^\lambda$ (using the uniqueness in 6)), and using a functional equation for the L-values (over complex numbers), computed at stage 5), for almost all Dirichlet characters (again, this stage is not necessary, but it is nice to have a functional equation).

This strategy is applicable in various cases (described above), cf. [PaJTNB], [Puy], [Go02]. An interesting discussion in the Bourbaki talk [Colm03] of P.Colmez indicates the use of this method for constructing Euler systems.

Acknowledgement

Both authors are very grateful to the Institut Fourier (UJF, Grenoble-1) and to the Mathematical Institutes in Heidelberg (Forschergruppe "Arithmetik Heidelberg-Mannheim"), and Oberwolfach for the permanent excellent working environment.
A part of these results was exposed by the second author in a talk “Une nouvelle méthode pour construire des fonctions L p-adiques associées aux formes modulaires” at the Séminaire de théorie des nombres de Jussieu (Chevaleret).
It is a great pleasure for us to thank P.Colmez, C.-G.Schmidt and R.Schulze-Pillot for valuable discussions.
Our special thanks go to John Coates, Helmut Klingen and Yury I. Manin, for providing us with fruitful motivations and advice.

Contents

1 Modular distributions attached to the higher twist of Eisenstein series

1.1 Higher twists of the Siegel-Eisenstein series

In this Section we study a $\mathcal{C}^\infty$-Siegel-Eisenstein series $F_{\chi,r}$ of degree 3 and of weight k, where $0 \le r \le k-2$. As in the Introduction, consider the Dirichlet characters (0.12) $\chi_1 \bmod Np^v = \chi$, $\chi_2 \bmod Np^v = \psi_2\bar{\psi}_3\chi$, $\chi_3 \bmod Np^v = \psi_1\bar{\psi}_3\chi$.
The series $F_{\chi,r} = G^\star(\mathcal{Z}, -r; k, (Np^v)^2, \boldsymbol{\psi})$, depends on the character χ, but its precise nebentypus character is $\boldsymbol{\psi} = \chi^2\psi_1\psi_2\overline{\psi}_3$. Here $\mathcal{Z}$ denotes a variable in the Siegel upper half space $\mathbb{H}_3$, and the normalized series $G^\star(\mathcal{Z}, s; k, (Np^v)^2, \boldsymbol{\psi})$ is given by (A.12). This series depends on $s = -r$, and for the critical values at integral points $s \in \mathbb{Z}$ such that $2 - k \le s \le 0$, it represents a (*nearly-*) *holomorphic* function in the sense of Shimura [ShiAr] viewed as formal (nearly-holomorphic) Fourier series, whose coefficients admit explicit polynomial expressions in terms of simple p-adic integrals for $p \nmid \det(\mathcal{T})$:

$$F_{\chi,r} = \sum_{\mathcal{T}\in B_3} \det(\mathcal{T})^{k-2r-\kappa} Q(R, \mathcal{T}; k-2r, r) a_{\chi,r}(\mathcal{T}) q^{\mathcal{T}},$$

where $B_3 = \{\mathcal{T} = (\mathcal{T}_{ij}) \in \mathrm{M}_3(\mathbb{R}) \mid \mathcal{T} = {}^t\mathcal{T}, \mathcal{T} \ge 0, \mathcal{T}_{ij}, 2\mathcal{T}_{ii} \in \mathbb{Z}\}$, and $q^{\mathcal{T}} = \exp(2\pi i \mathrm{tr}(\mathcal{T}\mathcal{Z}))$, $R = (4\pi \mathrm{Im}(\mathcal{Z}))^{-1}$. More precisely, for any $\mathcal{T}$ with $p \nmid \det(\mathcal{T})$ there exists a bounded measure $\mathcal{F}_{\mathcal{T}}$ on Y with values in $\overline{\mathbb{Q}}$ such that

$$a_{\chi,r}(\mathcal{T}) = \int_Y y_p^r \chi(y) d\mathcal{F}_{\mathcal{T}} = \prod_{\ell \mid \det(2\mathcal{T})} M_\ell(\mathcal{T}, \boldsymbol{\psi}(\ell)\ell^{-k+2r}), \tag{1.1}$$

where $\boldsymbol{\psi} = \chi^2\psi_1\psi_2\overline{\psi}_3$ (see (A.17), Theorem A.2 in Appendix A, also in [PaSE], [PaIAS]). Here we use arithmetical nearly-holomorphic Siegel modular forms (see [ShiAr] and Appendix A.2 for more details) viewed as formal power series $g = \sum\limits_{\mathcal{T}\in B_m} a(\mathcal{T}, R_{i,j}) q^{\mathcal{T}} \in \overline{\mathbb{Q}}[\![q^{B_m}]\!][R_{i,j}]$ such that for all $\mathcal{Z} \in \mathbb{H}_m$ the series converges to a $\mathcal{C}^\infty$-Siegel modular form of a given weight k and character ψ. As in the introduction, (0.14), we define the higher twist of the series $F_{\chi,r}$

by the characters (0.12) as the following formal nearly-holomorphic Fourier expansion:

$$F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3} = \sum_{\mathcal{T}} \bar\chi_1(t_{12})\bar\chi_2(t_{13})\bar\chi_3(t_{23})Q(R,\mathcal{T};k-2r,r)a_{\chi,r}(\mathcal{T})q^{\mathcal{T}} = \Psi_r(\chi).$$

We construct in this section a sequence of distributions Φ_r on Y using the restriction to the diagonal

$$\Phi_r(\chi) := 2^r \operatorname{diag}^* \Psi_r(\chi) = 2^r F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3} \circ \operatorname{diag} \tag{1.2}$$

$$\begin{gathered} = 2^r \sum_{t_1,t_2,t_3\ge 0} \sum_{\substack{\mathcal{T}: t_{11}=t_1,\\ t_{22}=t_2, t_{23}=t_3}} \bar\chi_1(t_{12})\bar\chi_2(t_{13})\bar\chi_3(t_{23}) \det(\mathcal{T})^{k-2r-\kappa} \times \\ \times Q(\operatorname{diag}(R_1,R_2,R_3),\mathcal{T};k-2r,r)a_{\chi,r}(\mathcal{T})q_1^{t_1}q_2^{t_2}q_3^{t_3}, \\ \text{where } \bar\chi_1(t_{12})\bar\chi_2(t_{13})\bar\chi_3(t_{23}) = \bar\chi(t_{12}t_{13}t_{23})\bar\psi_2\psi_3(t_{13})\bar\psi_1\psi_3(t_{23}), \end{gathered}$$

taking values in the tensor product of three spaces of nearly-holomorphic elliptic modular forms on the Poincaré upper half plane $\mathbb{H}$ (recall that the normalizing factor 2^r is neeeded in order to prove congruences between Φ_r in Section 3). We show in Proposition 1.5 that the (diagonal) nebentypus character of $F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3}$ is (ψ_1,ψ_2,ψ_3), thus it *does not depend* on χ.

1.2 The higher twist as a distribution

Let us fix a Dirichlet character $\chi \bmod Np^v$ as above with $v \ge 1$, and an arbitrary $\mathcal{C}^\infty$-modular function

$$F \in \mathcal{M}_k^{(3)}(\Gamma_0(Np^v), \boldsymbol{\psi})^\infty,$$

with a Dirichlet character $\boldsymbol{\psi} \bmod Np^v$ which depends on $\chi \bmod Np^v$, for example, the series $F_{\chi,r}$ with the nebentypus character $\boldsymbol{\psi} = \chi^2\psi_1\psi_2\overline{\psi}_3$. Then the higher twist of F with χ_1,χ_2,χ_3 was initially defined by the formula

$$\tilde F = \sum_{\varepsilon_{12},\varepsilon_{13},\varepsilon_{23} \bmod Np^v} \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23})F|_k t_{\boldsymbol{\varepsilon},Np^v} \tag{1.3}$$

where we use the translation $t_{\boldsymbol{\varepsilon},Np^v} = \begin{pmatrix} 1_3 & \frac{1}{Np^v}\boldsymbol{\varepsilon} \\ 0_3 & 1_3 \end{pmatrix}$ on $\mathbb{H}_3$ with $\boldsymbol{\varepsilon} = \begin{pmatrix} 0 & \varepsilon_{12} & \varepsilon_{13} \\ \varepsilon_{12} & 0 & \varepsilon_{23} \\ \varepsilon_{13} & \varepsilon_{23} & 0 \end{pmatrix}$. The idea of the construction. We wish to interpret the series (1.3) in terms of a distribution on a profinite group, using the following model example: consider the profinite ring $A_{N,p} = \varprojlim_v(\mathbb{Z}/Np^v\mathbb{Z})$, and a compact open subset $\alpha + (Np^v) \subset A_{N,p}$ with α an integer mod Np^v, and N is prime to p. For any formal series $f = \sum_{n\geq 1} a_n q^n \in \mathbb{C}[\![q]\!]$ and for any open subset $\alpha + (Np^v) \subset A_{N,p}$ consider the following partial series:

$$\mu_f(\alpha + (Np^v)) = \sum_{\substack{n\geq 1 \\ n\equiv\alpha \bmod Np^v}} a_n q^n \in \mathbb{C}[\![q]\!].$$

If $q = \exp(2\pi i z)$ with $z \in \mathbb{H}$, it follows from the orthogonality relations that

$$\mu_f(\alpha + (Np^v)) = (Np^v)^{-1} \sum_{\beta \bmod Np^v} \exp(-2\pi i\alpha\beta/Np^v) f\left(z + \frac{\beta}{Np^v}\right),$$

and that for any Dirichlet character χ mod Np^v one has

$$\int_{A_{N,p}} \chi(\alpha) d\mu_f(\alpha) = \sum_{n\geq 1} \chi(n) a_n q^n = f(\chi) \in \mathbb{C}[\![q]\!].$$

(the series f twisted by the character χ).
In the same fashion, consider the additive profinite group

$$S = S_{N,p} := \left\{ \boldsymbol{\varepsilon} = \begin{pmatrix} 0 & \varepsilon_{12} & \varepsilon_{13} \\ \varepsilon_{12} & 0 & \varepsilon_{23} \\ \varepsilon_{13} & \varepsilon_{23} & 0 \end{pmatrix} \middle| \varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23} \in A_{N,p} \right\};$$

equipped with the scalar product $\langle \cdot, \cdot \rangle : S_{N,p} \times S_{N,p} \longrightarrow A_{N,p}$:

$$\left\langle \boldsymbol{\varepsilon}^{(1)}, \boldsymbol{\varepsilon}^{(2)} \right\rangle = \operatorname{tr}(\boldsymbol{\varepsilon}^{(1)}\boldsymbol{\varepsilon}^{(2)}) = 2\varepsilon_{12}^{(1)}\varepsilon_{12}^{(2)} + 2\varepsilon_{13}^{(1)}\varepsilon_{13}^{(2)} + 2\varepsilon_{23}^{(1)}\varepsilon_{23}^{(2)}, \text{ where}$$

$$\boldsymbol{\varepsilon}^{(1)} = \begin{pmatrix} 0 & \varepsilon_{12}^{(1)} & \varepsilon_{13}^{(1)} \\ \varepsilon_{12}^{(1)} & 0 & \varepsilon_{23}^{(1)} \\ \varepsilon_{13}^{(1)} & \varepsilon_{23}^{(1)} & 0 \end{pmatrix}, \boldsymbol{\varepsilon}^{(2)} = \begin{pmatrix} 0 & \varepsilon_{12}^{(2)} & \varepsilon_{13}^{(2)} \\ \varepsilon_{12}^{(2)} & 0 & \varepsilon_{23}^{(2)} \\ \varepsilon_{13}^{(2)} & \varepsilon_{23}^{(2)} & 0 \end{pmatrix}.$$

Proposition 1.1 *Suppose that the function F is invariant with respect to any integer translation of type $t_{\boldsymbol{\varepsilon},1}$: $F|t_{\varepsilon,1} = F$. Then*
1) *The action $F|t_{\boldsymbol{\varepsilon},Np^v}$ depends only on the class of $\boldsymbol{\varepsilon} \in S/Np^vS$, and the additive character $e_{\boldsymbol{\varepsilon}^{(0)}} : \boldsymbol{\varepsilon} \mapsto \exp(\langle \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}^{(0)} \rangle / Np^v)$ on S is trivial iff $\boldsymbol{\varepsilon}^{(0)} \in Np^vS$.*
2) *The formula*

$$\Psi_F(\boldsymbol{\varepsilon}^{(0)} + (Np^v)) = (Np^v)^{-3} \sum_{\boldsymbol{\varepsilon}\in S \bmod Np^vS} \exp(-2\pi i \left\langle \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}^{(0)} \right\rangle / Np^v) F|t_{\boldsymbol{\varepsilon},Np^v} \tag{1.4}$$

$$= (Np^v)^{-3} \sum_{\boldsymbol{\varepsilon}\in S \bmod Np^vS} e(-\left\langle \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}^{(0)} \right\rangle / Np^v) F|t_{\boldsymbol{\varepsilon},Np^v}$$

defines a distribution with values in $\mathcal{C}^\infty$-functions on $\mathbb{H}_3$, where $e(\alpha/Np^v) := \exp(2\pi i\alpha/Np^v)$ is well-defined for all $\alpha \in A_N$.

Proof: 1) Follows directly from the invariance: $F|t_{\boldsymbol{\varepsilon},1} = F$.
2) It suffices to check the finite-additivity condition:

$$\Psi_F(\boldsymbol{\varepsilon}^{(0)} + (Np^v)) = \sum_{\boldsymbol{\varepsilon}^{(1)} \in S \bmod p} \Psi_F(\boldsymbol{\varepsilon}^{(0)} + Np^v\boldsymbol{\varepsilon}^{(1)} + (Np^{v+1})), \tag{1.5}$$

i.e.,

$$(Np^v)^{-3} \sum_{\boldsymbol{\varepsilon} \in S/Np^vS} e(-\left\langle \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}^{(0)} \right\rangle / Np^v) F|t_{\boldsymbol{\varepsilon},Np^v} \tag{1.6}$$

$$= (Np^{v+1})^{-3} \times$$
$$\sum_{\boldsymbol{\varepsilon}^{(1)} \in S/pS} \sum_{\boldsymbol{\varepsilon}^{(2)} \in S/Np^{v+1}S} e(-\left\langle \boldsymbol{\varepsilon}^{(2)}, (\boldsymbol{\varepsilon}^{(0)} + Np^v\boldsymbol{\varepsilon}^{(1)}) \right\rangle / Np^{v+1}) F|t_{\boldsymbol{\varepsilon}^{(2)},Np^{v+1}}. \tag{1.7}$$

For all $\boldsymbol{\varepsilon}^{(2)}$ the sum on the right on $\boldsymbol{\varepsilon}^{(1)} \in S/pS$ in (1.6) becomes

$$(Np^{v+1})^{-3} \sum_{\boldsymbol{\varepsilon}^{(1)} \in S/pS} e(-\left\langle \boldsymbol{\varepsilon}^{(2)}, (\boldsymbol{\varepsilon}^{(0)} + Np^v\boldsymbol{\varepsilon}^{(1)}) \right\rangle / Np^{v+1}) F|t_{\boldsymbol{\varepsilon}^{(2)},Np^{v+1}} \tag{1.8}$$

$$= (Np^{v+1})^{-3} e(-\frac{\left\langle \boldsymbol{\varepsilon}^{(2)}, \boldsymbol{\varepsilon}^{(0)} \right\rangle}{Np^{v+1}}) F|t_{\boldsymbol{\varepsilon}^{(2)},Np^{v+1}} \sum_{\boldsymbol{\varepsilon}^{(1)} \in S/pS} e(-\frac{\left\langle \boldsymbol{\varepsilon}^{(2)}, Np^v\boldsymbol{\varepsilon}^{(1)} \right\rangle}{Np^{v+1}})$$

$$= (Np^{v+1})^{-3} e(-\left\langle \boldsymbol{\varepsilon}^{(2)}, \boldsymbol{\varepsilon}^{(0)} \right\rangle / Np^{v+1}) F|t_{\boldsymbol{\varepsilon}^{(2)},Np^{v+1}} \sum_{\boldsymbol{\varepsilon}^{(1)} \in S/pS} e\left(-\left\langle \boldsymbol{\varepsilon}^{(2)}, \boldsymbol{\varepsilon}^{(1)} \right\rangle\right).$$

It remains to notice that

$$\sum_{\boldsymbol{\varepsilon}^{(1)} \in S/pS} e(-\left\langle \boldsymbol{\varepsilon}^{(2)}, \boldsymbol{\varepsilon}^{(1)} \right\rangle / p) = \begin{cases} p^3, & \text{if } \boldsymbol{\varepsilon}^{(2)} = p\boldsymbol{\varepsilon}^{(3)}, \boldsymbol{\varepsilon}^{(3)} \in S \\ 0, & \text{otherwise,} \end{cases} \tag{1.9}$$

because $\boldsymbol{\varepsilon}^{(1)} \mapsto e(-\langle \boldsymbol{\varepsilon}^{(2)}, \boldsymbol{\varepsilon}^{(1)} \rangle / p)$ is a non trivial character of S/pS iff $\boldsymbol{\varepsilon}^{(2)} \in pS$. The right hand side of (1.6) becomes

$$(Np^{v+1})^{-3} \sum_{\boldsymbol{\varepsilon}^{(1)} \in S/pS} \sum_{\boldsymbol{\varepsilon}^{(2)} \in S/Np^{v+1}S} e(-\left\langle \boldsymbol{\varepsilon}^{(2)}, (\boldsymbol{\varepsilon}^{(0)} + Np^v\boldsymbol{\varepsilon}^{(1)}) \right\rangle / Np^{v+1}) F|t_{\boldsymbol{\varepsilon}^{(2)},Np^{v+1}} \tag{1.10}$$

$$= (Np^{v+1})^{-3} p^3 \sum_{\boldsymbol{\varepsilon}^{(3)} \in S/Np^vS} e(-\left\langle \boldsymbol{\varepsilon}^{(3)}, \boldsymbol{\varepsilon}^{(0)} \right\rangle / Np^v) F|t_{\boldsymbol{\varepsilon}^{(3)},Np^v}.$$

Remark 1.2 *The Fourier expansions of the nearly-holomorphic Siegel modular form*

$$F_{\boldsymbol{\varepsilon},v} :=$$
$$\Psi_F(\boldsymbol{\varepsilon} + (Np^v)) = (Np^v)^{-3} \sum_{\boldsymbol{\varepsilon}' \in S \bmod Np^vS} \exp(-2\pi i \langle \boldsymbol{\varepsilon}', \boldsymbol{\varepsilon} \rangle / Np^v) F|t_{\boldsymbol{\varepsilon}',Np^v}.$$

is given as the following partial Fourier series

$$F_{\boldsymbol{\varepsilon},v}(\mathcal{Z}) = \sum_{\substack{\mathcal{T},t_{12}\equiv\varepsilon_{12} \bmod Np^v\\ t_{13}\equiv\varepsilon_{13},t_{23}\equiv\varepsilon_{23} \bmod Np^v}} a(\mathcal{T},R)q^{\mathcal{T}}, \tag{1.11}$$

where F is a nearly-holomorphic Siegel modular form, which is a periodic function on $\mathbb{H}_3$: $F = \sum\limits_{\mathcal{T}} a(\mathcal{T},R)q^{\mathcal{T}}$, and $\mathcal{T} = \begin{pmatrix} t_{11} & t_{12} & t_{13}\\ t_{12} & t_{22} & t_{23}\\ t_{13} & t_{23} & t_{33}\end{pmatrix}$ runs over half integral symmetric non negative matrices.

Indeed,
$F|t_{\boldsymbol{\varepsilon}',Np^v} = \sum\limits_{\mathcal{T}} a(\mathcal{T},R)q^{\mathcal{T}}|t_{\boldsymbol{\varepsilon}',Np^v} = \sum\limits_{\mathcal{T}} \exp(2\pi i \mathrm{tr}(\boldsymbol{\varepsilon}'\mathcal{T})/Np^v)a(\mathcal{T},R)q^{\mathcal{T}}$,
hence

$$F_{\boldsymbol{\varepsilon},v} = (Np^v)^{-3} \sum_{\boldsymbol{\varepsilon}'\in S \bmod Np^vS} \exp(-2\pi i\langle\boldsymbol{\varepsilon}',\boldsymbol{\varepsilon}\rangle/Np^v) \sum_{\mathcal{T}} \exp(2\pi i \mathrm{tr}(\boldsymbol{\varepsilon}'\mathcal{T})/Np^v)a(\mathcal{T},R)q^{\mathcal{T}}.$$

It suffices to notice that

$$\mathrm{tr}(\boldsymbol{\varepsilon}'\mathcal{T}) = \mathrm{tr}\left(\begin{pmatrix} 0 & \varepsilon'_{12} & \varepsilon'_{13}\\ \varepsilon'_{12} & 0 & \varepsilon'_{23}\\ \varepsilon'_{13} & \varepsilon'_{23} & 0\end{pmatrix}\begin{pmatrix} t_{11} & t_{12} & t_{13}\\ t_{12} & t_{22} & t_{23}\\ t_{13} & t_{23} & t_{33}\end{pmatrix}\right) = 2(\varepsilon'_{12}t_{12}+\varepsilon'_{13}t_{13}+\varepsilon'_{23}t_{23}).$$

∎

Let us consider now three Dirichlet characters χ_1, χ_2, χ_3 mod Np^v, and let us compute the corresponding integrals against the constructed modular distribution (1.4) of the locally constant function $\boldsymbol{\varepsilon} \mapsto \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23})$ on the profinite additive group

$$S = S_N := \left\{ \boldsymbol{\varepsilon} = \left(\begin{matrix} 0 & \varepsilon_{12} & \varepsilon_{13}\\ \varepsilon_{12} & 0 & \varepsilon_{23}\\ \varepsilon_{13} & \varepsilon_{23} & 0\end{matrix}\right) \middle| \varepsilon_{12},\varepsilon_{13},\varepsilon_{23} \in A_N \right\}.$$

Proposition 1.3 *Let F be a function invariant with respect to any translation of type $t_{\boldsymbol{\varepsilon},1}$: $F|t_{\boldsymbol{\varepsilon},1} = F$. Let us write $F_{\bar\chi_1,\bar\chi_2,\bar\chi_3} = \int_S \bar\chi_1(\varepsilon_{12})\bar\chi_2(\varepsilon_{13})\bar\chi_3(\varepsilon_{23})d\Psi_F(\boldsymbol{\varepsilon})$. Then*

$$\begin{aligned}&F_{\bar\chi_1,\bar\chi_2,\bar\chi_3} = \\ &(Np^v)^{-3} \sum_{\boldsymbol{\varepsilon}\in S/Np^vS} G_{Np^v}(\bar\chi_1,-\varepsilon_{12})G_{Np^v}(\bar\chi_2,-\varepsilon_{13})G_{Np^v}(\bar\chi_3,-\varepsilon_{23})F|t_{\boldsymbol{\varepsilon},Np^v}.\end{aligned} \tag{1.12}$$

Here $G_{Np^v}(\chi,\boldsymbol{\varepsilon}) := \sum\limits_{\alpha'} e(\boldsymbol{\varepsilon}\alpha'/Np^v)\chi(\alpha')$ denotes the Gauß sum (of a non necessarily primitive Dirichlet character χ).

Remarks 1.4 *1) The advantage of the expression* (1.12) *in compare with* (1.3) *is that it does not depend on a choice of* v.
2)It follows from (1.11, that the Fourier expansion of the series (1.12) is given by

$$F_{\bar\chi_1,\bar\chi_2,\bar\chi_3} = \sum_{\mathcal{T}} \bar\chi_1(t_{12})\bar\chi_2(t_{13})\bar\chi_3(t_{23})a(\mathcal{T},R)q^{\mathcal{T}}. \tag{1.13}$$

Proof is similar to that of Proposition 1.1, and it follows from the definitions. ∎

1.3 The level of the higher twist

Let us consider the symplectic inclusion:

$$i\ : \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Sp}_3(\mathbb{Z}) \tag{1.14}$$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \mapsto \begin{pmatrix} a_1 & & & b_1 & & \\ & a_2 & & & b_2 & \\ & & a_3 & & & b_3 \\ c_1 & & & d_1 & & \\ & c_2 & & & d_2 & \\ & & c_3 & & & d_3 \end{pmatrix}$$

We study the behaviour of the modular form $F_{\bar\chi_1,\bar\chi_2,\bar\chi_3}$ with respect to the subgroup

$$i(\Gamma_0(N^2p^{2v})^3) \subset \Gamma_0^{(3)}(N^2p^{2v}),$$

where $(\chi_1 \otimes \chi_2 \otimes \chi_3)(\boldsymbol{\varepsilon}) = \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23})$.
We will have to study two different types of twist; we can treat them simultaneously if we consider a function

$$\phi : \mathbb{Z}/N\mathbb{Z} \longmapsto \mathbb{C}$$

which is "φ-spherical" i.e.

$$\phi(gXh) = \varphi(g)\varphi(h)\phi(X)$$

for all $g, h \in (\mathbb{Z}/N\mathbb{Z})^\times, X \in \mathbb{Z}/N\mathbb{Z}$, where φ is a Dirichlet character mod N.
Let us use Proposition 1.12 and the spherical function

$$\phi : (\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23}) \mapsto G_{Np^v}(\bar\chi_1, -\varepsilon_{12})G_{Np^v}(\bar\chi_2, -\varepsilon_{13})G_{Np^v}(\bar\chi_3, -\varepsilon_{23}),$$

with respect to three variables $(\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23})$, and the Dirichlet characters

$$(\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23}) \mapsto \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23}).$$

PROPOSITION 1.5 *Consider a (nearly-holomorphic) Siegel modular form F for the group $\Gamma_0^{(3)}(Np^v)$ and the Dirichlet character $\boldsymbol{\psi} = \chi^2\psi_1\psi_2\overline{\psi}_3$).*
Then for all $M = i\left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}\right) \in \Gamma_0^{(3)}(N^2p^{2v})$ one has:
1) $\tilde{F}|M = \underbrace{\boldsymbol{\psi}\bar{\chi}_1\bar{\chi}_2(d_1)}_{\psi_1}\underbrace{\boldsymbol{\psi}\bar{\chi}_1\bar{\chi}_3(d_2)}_{\psi_2}\underbrace{\boldsymbol{\psi}\bar{\chi}_2\bar{\chi}_3(d_3)}_{\psi_3}\tilde{F}$, where $\tilde{F}$ is defined by (1.3),
2) $F_{\bar{\chi}_1,\bar{\chi}_2,\bar{\chi}_3}|M = \underbrace{\boldsymbol{\psi}\bar{\chi}_1\bar{\chi}_2(d_1)}_{\psi_1}\underbrace{\boldsymbol{\psi}\bar{\chi}_1\bar{\chi}_3(d_2)}_{\psi_2}\underbrace{\boldsymbol{\psi}\bar{\chi}_2\bar{\chi}_3(d_3)}_{\psi_3}F_{\bar{\chi}_1,\bar{\chi}_2,\bar{\chi}_3}$, where $F_{\bar{\chi}_1,\bar{\chi}_2,\bar{\chi}_3}$ is defined by (1.12).

Proof. We study modular forms on $\mathbb{H}_3$. Let us consider a more general situation and write N instead of Np^v. We use the (somewhat unconventional) congruence subgroup (with $N \mid M$):

$$\Gamma_1^{(3)}(M,N) := \left\{\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_0^{(3)}(M) \,\middle|\, D \equiv \operatorname{diag}(D_1, D_2, D_3) \bmod N\right\}.$$

Here the D_i denote integers along the diagonal of D. It is easy to see that this defines a subgroup of $\mathrm{Sp}(3,\mathbb{Z})$ and that a similar congruence also holds for A. The appropriate space of modular forms, denoted by $\mathcal{M}_k^{(3)}(M,N;\chi;\psi_1,\psi_2,\psi_3)$, with Dirichlet characters ψ_j mod N and a Dirichlet character χ mod M is then the set of holomorphic functions on $\mathbb{H}_3$ satisfying

$$f \mid_k \gamma = \chi(\det D)\left(\prod_{j=1}^{3}\psi_j(D_j)\right) f$$

for all $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_1^{(3)}(M,N)$. For any $\alpha \in \mathbb{R}$ and any $1 \le i < j \le 3$ we define a symmetric matrix of size 3 by

$$S_{ij}^{(3)}(\alpha) := \begin{pmatrix} & & & \\ & & \alpha & \\ & \alpha & & \\ & & & \end{pmatrix}$$

(the number α sits in the (i,j)th and (j,i)positions). Then, for a function $F \in \mathcal{M}_k^{(3)}(M,N;\chi;\psi_1,\psi_2,\psi_3)$ we define a new function F_{ij}^{ϕ} on $\mathbb{H}_3$ by

$$F_{ij}^{\phi}(\mathcal{Z}) = \sum_{\alpha \bmod N} \phi(\alpha)\cdot F(\mathcal{Z} + S_{ij}^{(3)}(\frac{\alpha}{N}))$$

PROPOSITION 1.6 *Assume that $N^2 \mid M$, χ is a character* mod $\frac{M}{N}$*, and $F \in \mathcal{M}_k^{(3)}(M,N;\chi;\psi_1,\psi_2,\psi_3)$. Then*

$$F_{ij}^{\phi} \in \mathcal{M}_k^{(3)}(M,N;\chi;\psi_1',\psi_2',\psi_3')$$

with

$$\psi_r' = \begin{cases} \psi_r & \text{if } \ r \notin \{i,j\} \\ \psi_r \cdot \overline{\varphi} & \text{if } \ r \in \{i,j\} \end{cases}$$

Remarks 1.7 *1) We mention here two basic types of φ-spherical functions $\phi : \mathbb{Z}/N\mathbb{Z}$:*
Type I: *"Dirichlet character" $\phi(X) := \varphi(X)$*
Type II: *"Gauß sum" $\phi(X) = G(\overline{\varphi}, -X)$ where $G(\varphi, X)$ denotes a Gauß sum (a version of such spherical functions of matrix argument was studied in [Boe-Schm]):*

$$G(\varphi, X) := \sum_{\alpha \bmod N} \varphi(\alpha) \exp(2\pi i \frac{1}{N} \alpha X)$$

2) Our basic example *is as follows: let $\varphi_1, \varphi_2, \varphi_3$ be three Dirichlet characters mod N and let ϕ_i be φ_i-spherical functions on $\mathbb{Z}/N\mathbb{Z}$. Furthermore let $F \in \mathcal{M}_k^{(3)}(\Gamma_0(M), \chi)$ with $N^2 \mid M$ and χ a Dirichlet character* mod $\frac{M}{N}$. *Then*

$$h(z_1, z_2, z_3) := \sum_{\alpha,\beta,\gamma \bmod N} \phi_1(\alpha)\phi_2(\beta)\phi_3(\gamma) F(\begin{pmatrix} z_1 & \frac{\alpha}{N} & \frac{\beta}{N} \\ \frac{\alpha}{N} & z_2 & \frac{\gamma}{N} \\ \frac{\beta}{N} & \frac{\gamma}{N} & z_3 \end{pmatrix})$$

is an element of

$$\mathcal{M}_k(\Gamma_0(M), \chi\bar{\varphi}_1\bar{\varphi}_2) \otimes \mathcal{M}_k(\Gamma_0(M), \chi\bar{\varphi}_1\bar{\varphi}_3) \otimes \mathcal{M}_k(\Gamma_0(M), \chi\bar{\varphi}_2\bar{\varphi}_3)$$

(note that the definition of h depends on N)
3) Other important cases are treated in [Boe-Schm] it can also (by iteration) be applied to cases of block matrices of different size which e.g. occur in the work [Boe-Ha] on the L-function for GSp(2) × GL(2).

Proof. We first try to find $X \in \mathrm{Sym}_3(\frac{1}{N}\mathbb{Z})$ such that

$$\begin{pmatrix} 1_3 & S(\frac{\alpha}{N}) \\ 0_3 & 1_3 \end{pmatrix} \begin{pmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{pmatrix} \begin{pmatrix} 1_3 & -X \\ 0_3 & 1_3 \end{pmatrix}$$
$$= \begin{pmatrix} \mathcal{A} + S(\frac{\alpha}{N})\mathcal{C} & -\mathcal{A}X + \mathcal{B} - S(\frac{\alpha}{N})\mathcal{C}X + S(\frac{\alpha}{N})\mathcal{D} \\ \mathcal{C} & -\mathcal{C}X + \mathcal{D} \end{pmatrix}$$

is in $\Gamma_0^{(3)}(M)$ (for the moment we only assume here that $\begin{pmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{pmatrix}$ is integral. The conditions $N^2 \mid M$ and the congruences mod M and N will then be forced to hold). The first (evident) condition is that $\mathcal{C} \equiv 0 \bmod M$. It is easy to see that the two numbers on the diagonal

$$-\mathcal{C}X + \mathcal{D} \qquad \text{and} \qquad \mathcal{A} + S(\frac{\alpha}{N})\mathcal{C}$$

are integers, if $\mathcal{C}$ is congruent to 0 modulo N.

The remaining condition is that

$$-\mathcal{A}X+\mathcal{B}-S(\frac{\alpha}{N})\mathcal{C}X+S(\frac{\alpha}{N})\mathcal{D}$$

is integral, which is satisfied if $\mathcal{C}\equiv 0 \bmod N^2$ and $-\mathcal{A}\cdot X+S(\frac{\alpha}{N})\mathcal{D}$ is integral. Therefore we should choose any X satisfying

$$(NX)\equiv\overline{\mathcal{A}}S(\alpha)\mathcal{D} \quad \bmod N$$

where $\overline{\mathcal{A}}$ is a (multiplicative) inverse of the matrix $\mathcal{A}$ mod N. Now we use the fact that $\mathcal{A}\equiv\operatorname{diag}(A_1,A_2,A_3)$ mod N and $\mathcal{D}\equiv\operatorname{diag}(D_1,D_2,D_3)$ mod N are matrices which are diagonal modulo N, we may therefore choose the integral symmetric matrix NX to be modulo N equal to

$$NX:=S^{(3)}_{ij}\left(\overline{A_i}\cdot\alpha\cdot D_j\right)\Rightarrow X=X(\alpha)=S^{(3)}_{ij}\left(\frac{\overline{A_i}\cdot\alpha\cdot D_j}{N}\right).$$

By the above,

$$\begin{aligned}
F^{\phi}_{ij}\mid_k\begin{pmatrix}\mathcal{A}&\mathcal{B}\\ \mathcal{C}&\mathcal{D}\end{pmatrix} &= \sum_{\alpha \bmod N}\phi(\alpha)F\mid_k\begin{pmatrix}1&S(\frac{\alpha}{N})\\ 0&1\end{pmatrix}\begin{pmatrix}\mathcal{A}&\mathcal{B}\\ \mathcal{C}&\mathcal{D}\end{pmatrix}\\
&= \sum_{\alpha \bmod N}\phi(\alpha)F\mid_k\begin{pmatrix}\tilde{\mathcal{A}}&\tilde{\mathcal{B}}\\ \tilde{\mathcal{C}}&\tilde{\mathcal{D}}\end{pmatrix}\begin{pmatrix}1&X(\alpha)\\ 0&1\end{pmatrix}
\end{aligned}$$

where $\begin{pmatrix}\tilde{\mathcal{A}}&\tilde{\mathcal{B}}\\ \tilde{\mathcal{C}}&\tilde{\mathcal{D}}\end{pmatrix}\in\Gamma^{(3)}_1(M,N)$ with

$$\tilde{\mathcal{A}}\equiv\mathcal{A}\bmod\frac{M}{N}\quad\text{and}\quad\tilde{\mathcal{D}}\equiv\mathcal{D}\quad\bmod\frac{M}{N}$$

(in particular, these congruences hold mod N). Therefore

$$F^{\phi}_{ij}\mid_k\begin{pmatrix}\mathcal{A}&\mathcal{B}\\ \mathcal{C}&\mathcal{D}\end{pmatrix}=\chi(\det(\mathcal{D}))\psi_1(D_1)\dots\psi_n(D_n)\sum_{\alpha \bmod N}\phi(\alpha)F\mid_k\begin{pmatrix}1_3&X(\alpha)\\ 0_3&1_3\end{pmatrix}.$$

Instead of summing over α we may as well sum over $\beta:=D_i\cdot\alpha\cdot D_j$ mod N. Then we obtain

$$\begin{aligned}
&\chi(\det(\mathcal{D}))\psi_1(D_1)\dots\psi_n(D_n)\overline{\varphi}(D_i)\overline{\varphi}(D_j)\sum_{\beta \bmod N}\phi(\beta)F\mid_k\begin{pmatrix}1_3&S^{(3)}_{ij}(\frac{\beta}{N})\\ 0_3&1_3\end{pmatrix}\\
&=\chi(\det(\mathcal{D})\psi_1(D_1)\dots\psi_n(D_n)\overline{\varphi}(D_i)\overline{\varphi}(D_j)F^{\phi}_{ij}.\quad\blacksquare
\end{aligned}$$

Notice that the properties of Propositions 1.6 hold for the *iterated twists*, and Propositions 1.5 follows from Propositions 1.6 by three iterated twists with N equal to Np^v. ∎

2 Computation of the canonical projection

2.1 A general construction: the canonical λ-characteristic projection

We explain now a general method which associates a p-adic measure $\mu_{\lambda,\Phi}$ on a profinite group Y, to a sequence of distributions Φ_r on Y with values in a suitable (infinite dimensional) vector space $\mathcal{M}$ of modular forms, and to a nonzero eigenvalue λ of the Atkin operator $U = U_p$ acting on $\mathcal{M}$. We consider holomorphic (or nearly-holomorphic) modular forms in a space of the type

$$\mathcal{M} = \mathcal{M}_k(\psi, \overline{\mathbb{Q}}) = \bigcup_{v\geq 0} \mathcal{M}_k(Np^v, \psi, \overline{\mathbb{Q}}) \subset \mathcal{M}(\mathbb{C}_p) = \bigcup_{v\geq 0} \mathcal{M}_k(Np^v, \psi, \mathbb{C}_p),$$

with finite dimensional vector spaces $\mathcal{M}_k(Np^v, \psi, \overline{\mathbb{Q}})$ at each fixed level, endowed with a natural $\overline{\mathbb{Q}}$-rational structure (for example, given by the Fourier coefficients). The parameters here are triples $k = (k_1, k_2, k_3)$, $\psi = (\psi_1, \psi_2, \psi_3)$ of weights and characters. The important property of our construction is that does not use *passage to a p-adic limit.* We put

$$\mathcal{M}_k(Np^v, \psi, A) = \mathcal{M}_k(Np^v, \psi, \overline{\mathbb{Q}}) \otimes_{\overline{\mathbb{Q}}} A.$$

for any $\overline{\mathbb{Q}}$-algebra A.

Definition 2.1 *Let $A = \mathbb{C}_p$, $A = \overline{\mathbb{Q}}$, or $A = \mathbb{C}$, and $\mathcal{M} = \mathcal{M}(A)$.*
(a) *For a $\lambda \in A$ let us define $\mathcal{M}^{(\lambda)} = \mathrm{Ker}\,(U - \lambda I)$ the subspace of eigenvectors with eigenvalue λ).*
(b) *Let us define the λ-characteristic subspace of U on $\mathcal{M}$ by*

$$\mathcal{M}^{\lambda} = \bigcup_{n\geq 1} \mathrm{Ker}\,(U - \lambda I)^n$$

(c) *Let us define for any $v \geq 0$*

$$\mathcal{M}^{\lambda}(Np^v) = \mathcal{M}^{\lambda} \cap \mathcal{M}(Np^v), \quad \mathcal{M}^{(\lambda)}(Np^v) = \mathcal{M}^{(\lambda)} \cap \mathcal{M}(Np^v).$$

Proposition 2.2 *Let $\psi \bmod N$ be a fixed Dirichlet character, then $U^v(\mathcal{M}(Np^{v+1}, \psi)) \subset \mathcal{M}(Np, \psi)$.*

Proof follows from a known formula of J.-P. Serre: for $g \in \mathcal{M}_k(Np^{v+1}, \psi)$,

$$g|_k U^v = p^{3v(k/2-1)} g|_k W_{Np^{v+1}} \mathrm{Tr}_{Np}^{Np^{v+1}} W_{Np}, \tag{2.1}$$

where $W_N : \mathcal{M}(N, \psi) \to \mathcal{M}(N, \bar{\psi})$ is the involution (over $\mathbb{C}$) of level N (see [Se73] for the elliptic modular case, which extends to the triple modular case).

Proposition 2.3 *Let $A = \mathbb{C}_p$ or $A = \overline{\mathbb{Q}}$, $\mathcal{M} = \mathcal{M}(A)$, $\lambda \in A^*$, and let U^λ be the restriction of U on $\mathcal{M}^\lambda$, then*
(a) $(U^\lambda)^v : \mathcal{M}^\lambda(Np^{v+1}) \xrightarrow{\sim} \mathcal{M}^\lambda(Np)$ *is an A-linear invertible operator, where* $U^\lambda = U|_{\mathcal{M}^\lambda(Np^{v+1})}$.
(b) *The vector subspace $\mathcal{M}^\lambda(Np^{v+1}) = \mathcal{M}^\lambda(Np)$ does not depend on v.*
(c) *Let $\pi_{\lambda,v+1} : \mathcal{M}(Np^{v+1}) \to \mathcal{M}^\lambda(Np^{v+1})$ be the projector on the λ-characteristic subspace of U with the kernel* $\operatorname{Ker}(\pi_{\lambda,v}) = \bigcap\limits_{n\geq 1} \operatorname{Im}(U - \lambda I)^n = \bigoplus\limits_{\beta\neq\lambda} \mathcal{M}^\beta(N_0p^v))$, *then the following diagram is commutative*

$$\begin{tikzcd}
\mathcal{M}(Np^{v+1}) \arrow[r, "\pi_{\lambda,v+1}"'] \arrow[d, "U^v"'] & \mathcal{M}^\lambda(Np^{v+1}) \arrow[d, "\wr\, U^v"] \\
\mathcal{M}(Np) \arrow[r, "\pi_{\lambda,1}"'] & \mathcal{M}^\lambda(Np)
\end{tikzcd} \tag{2.2}$$

Let us use the notation

$$\pi_\lambda(g) = (U^\lambda)^{-v}\pi_{\lambda,1}(U^v(g)) \in \mathcal{M}^\lambda(\Gamma_0(Np), \psi, \mathbb{C}) \tag{2.3}$$

for the canonical λ-characteristic projection of $g \in \mathcal{M}(\Gamma_0(Np^{v+1}), \psi, \mathbb{C})$.
Proof of (a). The linear operator $(U^\lambda)^v$ acts on the A-linear vector space $\mathcal{M}^\lambda(Np^{v+1})$ of finite dimension, and its determinant is in A^*, hence the A-linear operator $(U^\lambda)^v$ is *invertible*.
Proof of (b). We have the obvious inclusion of vector spaces: $\mathcal{M}^\lambda(Np) \subset \mathcal{M}^\lambda(Np^{v+1})$. On the other hand the A-vector spaces $\mathcal{M}^\lambda(Np^{v+1})$ and $\mathcal{M}^\lambda(Np)$ are isomorphic by (a), hence they coincide:

$$\mathcal{M}^\lambda(Np) \subset \mathcal{M}^\lambda(Np^{v+1}) = U^v(\mathcal{M}^\lambda(Np^{v+1})) \subset \mathcal{M}^\lambda(Np).$$

Proof of (c). Following the theory of reduction of endomorphisms in finite dimensional vector spaces over a field K, the canonical projector $\pi_{\lambda,v}$ onto the λ-characteristic subspace $\bigcup_{n\geq 1} \operatorname{Ker}(U - \lambda I)^n$ with the kernel $\bigcap_{n\geq 1} \operatorname{Im}(U - \lambda I)^n$ can be expressed, on one hand, as a polynomial of U over K, hence $\pi_{\lambda,v}$ commutes with U. On the other hand, the restriction of $\pi_{\lambda,v+1}$ on $\mathcal{M}(Np)$ coincides with $\pi_{\lambda,1} : \mathcal{M}(Np) \to \mathcal{M}^\lambda(Np)$, because its image is

$$\bigcup_{n\geq 1} \operatorname{Ker}(U - \lambda I)^n \cap \mathcal{M}(Np) = \bigcup_{n\geq 1} \operatorname{Ker}(U|_{\mathcal{M}(Np)} - \lambda I)^n,$$

and its kernel is

$$\bigcap_{n\geq 1} \operatorname{Im}(U - \lambda I)^n \cap \mathcal{M}(Np) = \bigcap_{n\geq 1} \operatorname{Im}(U|_{\mathcal{M}(Np)} - \lambda I)^n. \quad \blacksquare$$

2.2 A general result on admissible measures with values in modular forms (a criterion for admissibility)

Consider the profinite group $Y = \varprojlim_{v} Y_v$ where $Y_v = (\mathbb{Z}/Np^v\mathbb{Z})^\times$. There is a natural projection $y_p : Y \to \mathbb{Z}_p^\times$. Let A be a normed ring over $\mathbb{Z}_p$, and M be a normed A-module with the norm $|\cdot|_{p,M}$.

Let us recall Definition 0.1, c): for a given positive integer h an h-*admissible measure* on Y with values in M is an A-module homomorphism

$$\tilde{\Phi} : \mathcal{P}^h(Y, A) \to M$$

such that for fixed $a \in Y$ and for $v \to \infty$

$$\left| \int_{a+(Np^v)} (y_p - a_p)^{h'} d\tilde{\Phi} \right|_{p,M} = o(p^{-v(h'-h)}) \text{ for all } \quad h' = 0, 1, \ldots, h-1,$$

where $a_p = y_p(a)$, $\mathcal{P}^h(Y, A)$ denotes the A-module of *locally polynomial functions* of degree $< h$ of the variable $y_p : Y \to \mathbb{Z}_p^\times \hookrightarrow A^\times$. We adopt the notation $(a)_v = a+(Np^v)$ for both an element of Y_v and the corresponding open compact subset of Y.

We wish now to construct an h-admissible measure $\tilde{\Phi}^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}(A)$ out of a sequence of distributions

$$\Phi_r^\lambda : \mathcal{P}^1(Y, A) \to \mathcal{M}(A)$$

with values in an A-module $M = \mathcal{M}(A)$ of modular forms over A as in Section 2.1).

For this purpose we recall first Proposition 2.3, (c). Suppose that $\lambda \in A^\times$ is an invertible element of the algebra A. Recall that the λ-*characteristic projection operator*

$$\pi_{\lambda,v} : \mathcal{M}(Np^v; A) \to \mathcal{M}(Np^v; A)^\lambda \subset \mathcal{M}(Np^v; A) \ (v \geq 1)$$

is determined by the kernel $\bigcap\limits_{n \geq 1} \mathrm{Im}(U - \lambda I)^n$; this projector is given as a polynomial of U over A whose degree is bounded by the *rank* of $\mathcal{M}(Np^v; A)$.

Using Proposition 2.3(c), the sequence of projectors $\pi_{\lambda,v}$ can be glued to the *canonical projection operator*

$$\pi_\lambda : \mathcal{M}(A) \to \mathcal{M}(A)^\lambda \subset \mathcal{M}(A) \tag{2.4}$$

given for all $g \in \mathcal{M}(A)$ by

$$\pi_\lambda(g) = g^\lambda = U^{-v} \left[\pi_{\lambda,1} U^v(g)\right]$$

(g^λ is well defined if v is sufficiently large so that $g \in \mathcal{M}(Np^{v+1})$).

Next we construct an admissible measure

$$\tilde{\Phi}^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}(Np; A)$$

such that

$$\int_{(a)_v} y_p^r \, d\tilde{\Phi}^\lambda = \Phi_r^\lambda((a)_v) = \pi_\lambda(\Phi_r((a)_v))$$

where $\Phi_r : \mathcal{P}^1(Y, A) \to \mathcal{M}(A)$ are $\mathcal{M}(A)$-valued distributions on Y for $r = 0, 1, \ldots, h-1$, and $\Phi_r^\lambda((a)_v)$ are their λ-characteristic projections given by

$$\Phi_r^\lambda((a)_v) = U^{-v'} \left[\pi_{\lambda,1} U^{v'} \Phi_r((a)_v)\right]$$

for any sufficiently large v'. Note first of all that the definition

$$\int_{(a)_v} y_p^r \, d\tilde{\Phi}^\lambda = \Phi_r^\lambda((a)_v) = U^{-\kappa v} \left[\pi_{\lambda,1} U^{\kappa v} \Phi_r((a)_v)\right].$$

of the linear form $\tilde{\Phi}^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}(A)$ is independent on the choice of the level: for any sufficiently large v', we have by Proposition 2.3 the following comutative diagram

$$\begin{tikzcd}
\mathcal{M}(Np^{v'+1}; A) \arrow[r, "\pi_{\lambda,v'+1}"] \arrow[d, "U^{v'}"'] & \mathcal{M}(Np^{v'+1}; A)^\lambda \arrow[d, "U^{v'}", "\wr"'] \\
\mathcal{M}(Np; A) \arrow[r, "\pi_{\lambda,1}"] & \mathcal{M}(Np; A)^\lambda
\end{tikzcd}$$

in which the right vertical arrow is an A-isomorphism by Proposition 2.3 (b), and the A-linear endomorphism U commutes with the characteristic projectors $\pi_{\lambda,v'+1}$, $\pi_{\lambda,1}$. Hence the following sequence stabilizes: for some v_0' and for all $v' \geq v_0'$ we have that

$$U^{-v'} \left[\pi_{\lambda,1} U^{v'} \Phi_r((a)_v)\right] = U^{-v_0'} \left[\pi_{\lambda,1} U^{v_0'} \Phi_r((a)_v)\right].$$

Theorem 2.4 *Let $\lambda \in A$ be an element whose absolute value is a positive constant with $0 < |\lambda|_p < 1$. Suppose that there exists a positive integer $\varkappa$ such that for any $(a)_v \subset Y$ the following two conditions are satisfied:*

$$\Phi_r\big((a)_v\big) \in \mathcal{M}(N'p^{\varkappa v}), \text{ with } N' \text{ independent of } v, \qquad (level)$$

$$\left| U^{\varkappa v}\Big(\sum_{r'=0}^{r} \binom{r}{r'} (-y_p^0)^{r-r'} \Phi_{r'}\big((a)_v\big)\Big)\right|_p \leq Cp^{-vr} \qquad (growth)$$

for all $r = 0, 1, \ldots, h-1$ with $h = [\varkappa \mathrm{ord}_p(\lambda)] + 1$.
Then there exists an h-admissible measure $\tilde{\Phi}^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}$ such that for all $((a)_v) \subset Y$ and for all $r = 0, 1, \ldots, h-1$ one has

$$\int_{(a)_v} y_p^r \, d\tilde{\Phi}^\lambda = \Phi_r^\lambda((a)_v)$$

where

$$\Phi_r^\lambda((a)_v) = \pi_\lambda(\Phi_r((a)_v)) := U^{-\varkappa v}\left[\pi_{\lambda,1}U^{\varkappa v}\Phi_r((a)_v)\right]$$

is the canonical projection of π_λ *of the modular form* $\Phi_r((a)_v)$ *(note that* $U^{\varkappa v}\Phi_r((a)_v) \in \mathcal{M}(Np^{\varkappa v}; A)^\lambda = \mathcal{M}(Np; A)^\lambda$ *because of the inclusion* $U^{\varkappa v-1}(\mathcal{M}(Np^{\varkappa v}; A)) \subset \mathcal{M}(Np; A)$ for all $v \geq 1$*, see Proposition 2.3 (a))*

Proof. We need to check the h-growth condition of Definition 0.1, c) for the linear form

$$\tilde\Phi^\lambda : \mathcal{P}^h(Y, A) \to \mathcal{M}(A)^\lambda$$

(given by the condition of Theorem 2.4). This growth condition says that for all $a \in Y$ and for $v \to \infty$

$$\left|\int_{(a)_v}(y_p - y_p^0)^r\, d\tilde\Phi^\lambda\right|_{p,\mathcal{M}} = o(p^{-v(r-h)})$$

for all $r = 0, 1, \ldots, h-1$, where $h = [\varkappa\mathrm{ord}_p(\lambda)] + 1$ and $y_p^0 = y_p(a)$.
Let us develop the definition of $\tilde\Phi^\lambda$ using the binomial formula:

$$\int_{(a)_v}(y_p - y_p^0)^r\, d\tilde\Phi^\lambda = \sum_{r'=0}^{r}\binom{r}{r'}(-y_p^0)^{r-r'}\Phi_{r'}^\lambda((a)_v) = \lambda^{-v\varkappa}\cdot$$

$$\lambda^{v\varkappa}\cdot U^{-v\varkappa}\left[\pi_{\lambda,1}U^{\varkappa v}\Big(\sum_{r'=0}^{r}\binom{r}{r'}(-y_p^0)^{r-r'}\Phi_{r'}\big((a)_v\big)\Big)\right]. \qquad (2.5)$$

First we notice that all the operators

$$\lambda^{v\varkappa}\cdot U^{-v\varkappa} = \left(\lambda^{-1}U\right)^{-v\varkappa} = \left(I + \lambda^{-1}Z\right)^{-v\varkappa} = \sum_{j=0}^{n-1}\binom{-v\varkappa}{j}\left(\lambda^{-1}Z\right)^j$$

are uniformly bounded for $v \to \infty$ by a positive constant C_1 (where $U = \lambda I + Z$ and $Z^n = 0$ where n is the rank of $\mathcal{M}(Np; A)$). Note that the binomial coefficients $\binom{-v\varkappa}{j}$ are all $\mathbb{Z}_p$-integral.
On the other hand by the condition (*growth*) of the theorem (for the distributions Φ_r) we have the following inequality:

$$\left|U^{\varkappa v}\Big(\sum_{r'=0}^{r}\binom{r}{r'}(-y_p^0)^{r-r'}\Phi_{r'}((a)_v)\Big)\right|_{p,\mathcal{M}} \leq Cp^{-vr}$$

for all $r = 0, 1, \ldots, \varkappa h - 1$. If we apply to this estimate the previous bounded operators we get

$$\left|\int_{(a)_v}(y_p - y_p^0)^r\, d\tilde\Phi^\lambda\right|_{p,\mathcal{M}} \leq C\cdot C_1|\lambda^{-v\varkappa}|_p\cdot p^{-vr} = o(p^{-v(r-h)})$$

because of the estimate

$$|\lambda^{-v\varkappa}|_p = \left(p^{\mathrm{ord}_p(\lambda)}\right)^{v\varkappa} = o(p^{vh}),\text{ and } \varkappa\mathrm{ord}_p(\lambda) < h = [\varkappa\mathrm{ord}_p(\lambda)] + 1. \quad \blacksquare \tag{2.6}$$

We apply Theorem 2.4 in Section 5.1 in order to obtain a p-adic measure in the form $\mu_{\lambda,\Phi} = \ell(\pi_\lambda(\Phi))$. Here λ is a non-zero eigenvalue of Atkin's operator $U = U_p$ acting on $\mathcal{M}$, $\ell : \mathcal{M}^\lambda(Np; A) \to A$ is an A-linear form, applied to the projection $\pi_\lambda \ : \mathcal{M} \to \mathcal{M}^\lambda \subset \mathcal{M}^\lambda(Np; A)$ of a modular distribution Φ, where $A = \mathbb{C}_p$.

3 Main Congruence for the higher twists of the Siegel-Eisenstein series

The purpose of this section is to show that the admissibility criterion of Theorem 2.4 with $h^* = 2$ is satisfied by a sequence of modular distributions (1.2), constructed in Section 1.

3.1 Construction of a sequence of modular distributions

As in the Introduction, consider the series $F_{\chi,r} = G^\star(\mathcal{Z}, -r; k, (Np^v)^2, \boldsymbol{\psi})$, given by (A.12), viewed as formal (nearly-holomorphic) Fourier series, whose coefficients admit explicit polynomial expressions. The only property that we use in this section is the fact that they can be written in terms of simple p-adic integrals:

$$F_{\chi,r} = \sum_{\mathcal{T}} \det(\mathcal{T})^{k-2r-\kappa} Q(R, \mathcal{T}; k-2r, r) a_{\chi,r}(\mathcal{T}) q^{\mathcal{T}},$$

[PaSE], [PaIAS] and (1.1)). Here we use a universal polynomial, described in [CourPa], Theorem 3.14 as follows:

$$\begin{aligned} Q(R,\mathcal{T}) &= Q(R,\mathcal{T}; k-2r, r) \qquad\qquad\qquad\qquad\qquad\qquad (3.1)\\ &= \sum_{t=0}^{r} \binom{r}{t} \det(\mathcal{T})^{r-t} \sum_{|L| \le mt-t} R_L(\kappa - k + r) Q_L(R,\mathcal{T}),\\ Q_L(R,\mathcal{T}) &= \mathrm{tr}\left({}^t\rho_{m-l_1}(R)\rho^\star_{l_1}(\mathcal{T})\right) \cdot \ldots \cdot \mathrm{tr}\left({}^t\rho_{m-l_t}(R)\rho^\star_{l_t}(\mathcal{T})\right)), \end{aligned}$$

where we use the natural representation $\rho_r : \mathrm{GL}_m(\mathbb{C}) \longrightarrow \mathrm{GL}(\wedge^r\mathbb{C}^m)$ $(0 \le r \le m)$ of the group $\mathrm{GL}_m(\mathbb{C})$ on the vector space $\Lambda^r\mathbb{C}^m$. Thus $\rho_r(z)$ is a matrix of size $\binom{m}{r} \times \binom{m}{r}$ composed of the subdeterminants of z of degree r. Put $\rho^\star_r(z) = \det(z)\rho_{m-r}({}^tz)^{-1}$. Then the representations ρ_r and $\rho^\star_r$ turn out to be polynomial representations so that for each $z \in \mathrm{M}_m(\mathbb{C})$ the linear operators $\rho_r(z)$, $\rho^\star_r(z)$ are well defined. In (3.1), L runs over all the multi-indices $0 \le l_1 \le \cdots \le l_t \le m$, such that $|L| = l_1 + \cdots + l_t \le mt - t$. The coefficients $R_L(\beta) \in \mathbb{Z}[1/2][\beta]$ in (3.1) are polynomials in β of degree $(mt - |L|)$ and with coefficients in the ring $\mathbb{Z}[1/2]$.

3.2 Utilizing the admissibility criterion

Recall an important property of the sequence of distributions Φ_r defined by (1.2), Section 1: the nebentypus character of $\Phi_r(\chi)$ is (ψ_1, ψ_2, ψ_3), so that it *does not depend* on χ. Now let us prove that the sequence of distributions Φ_r on Y produces a certain *admissible measure* $\tilde{\Phi}$ with values in a finite dimensional $\mathbb{C}_p$-vector subspace

$$\mathcal{M}^\lambda \subset \mathcal{M},\ \mathcal{M} = \mathcal{M}_{k,r}(\mathbb{C}_p) \otimes \mathcal{M}_{k,r}(\mathbb{C}_p) \otimes \mathcal{M}_{k,r}(\mathbb{C}_p),$$

(of nearly-holomorphic triple modular forms over $\mathbb{C}_p$) using a general admissibility criterion (see Theorem 2.4).

3.3 Sufficient conditions for admissibility of measures with values in nearly-holomorphic modular forms

In order to construct the admissible measures of Theorem B we use the admissible measures $\tilde{\mu}^\lambda(f_1 \otimes f_2 \otimes f_3, y)$ constructed in Section 5 out of the modular distributions Φ_r in the form

$$\tilde{\mu}^\lambda(f_1 \otimes f_2 \otimes f_3)(\chi y_p^r) = \ell(\pi_\lambda(\Phi_r)(\chi)).$$

The growth condition for $\tilde{\mu}^\lambda$ follows then from a growth condition for Φ_r:

$$\sup_{a\in Y}\left|\int_{a+(Np^v)}(y_p-a_p)^r d\widetilde{\Phi}^\lambda\right|_p = o\left(|Np^v|_p^{r-2\mathrm{ord}_p\lambda}\right), \tag{3.2}$$

where

$$\tilde{\Phi}^\lambda(\chi y_p^r) = \pi_\lambda(\Phi_r(\chi)).$$

Let us use a general result giving a sufficient condition for the admissibility of measures with values in nearly-holomorphic Siegel modular forms (given in Theorem 2.4) with $\varkappa = 2$, $h = [2\mathrm{ord}_p\lambda] + 1$. Then we need to check that the nearly-holomorphic triple modular forms $\Phi_r(\chi)$ are of level $N^2\chi^{2v}$, nebentypus (ψ_1, ψ_2, ψ_3), and satisfy the congruences

$$\left|U_T^{2v}\Big(\sum_{r'=0}^{r}\binom{r}{r'}(-a_p^0)^{r-r'}\Phi_{r'}\big((a)_v\big)\Big)\right|_p \le Cp^{-vr} \tag{3.3}$$

and for all $r = 0, 1, \cdots, k-2$.

3.4 Special Fourier coefficients of the higher twist of the Siegel-Eisenstein distributions

Let us use the Fourier expansions (1.13) for $\Psi_r(\chi)$. These formulas directly imply the Fourier expansion of $\Phi_r(\chi)|U_p^{2v}$ as follows

$$\Phi_r(\chi)|U_p^{2v} = \sum_{t_1,t_2t_3\ge 0} a(p^{2v}t_1, p^{2v}t_2, p^{2v}t_3; p^{2v}R_1, p^{2v}R_2, p^{2v}R_3, r)q_1^{t_1}q_2^{t_2}q_3^{t_3} \tag{3.4}$$

with

$$a(p^{2v}t_1,p^{2v}t_2,p^{2v}t_3;p^{2v}R_1,p^{2v}R_2,p^{2v}R_3,r)$$

$$=\sum_{\mathcal{T}:\mathrm{diag}(\mathcal{T})=(p^{2v}t_1,p^{2v}t_2,p^{2v}t_3)}\bar\chi(t_{12}t_{13}t_{23})\bar\psi_2\psi_3(t_{13})\bar\psi_1\psi_3(t_{23})\times$$

$$\times\det(\mathcal{T})^{k-2r-\kappa}Q(p^{2v}\,\mathrm{diag}(R_1,R_2,R_3),\mathcal{T};k-2r,r)2^r a_{\chi,r}(\mathcal{T})$$

$$=\sum_{\mathcal{T}:\mathrm{diag}(\mathcal{T})=(p^{2v}t_1,p^{2v}t_2,p^{2v}t_3)}v_{\chi,r}(\mathcal{T},\mathrm{diag}(R_1,R_2,R_3)),$$

where

$$v_{\chi,r}(\mathcal{T},\mathrm{diag}(R_1,R_2,R_3))=\bar\chi(t_{12}t_{13}t_{23})\bar\psi_2\psi_3(t_{13})\bar\psi_1\psi_3(t_{23})\times \tag{3.5}$$

$$\times\det(\mathcal{T})^{k-2r-\kappa}Q(p^{2v}\,\mathrm{diag}(R_1,R_2,R_3),\mathcal{T};k-2r,r)2^r a_{\chi,r}(\mathcal{T})$$

$$=\chi^{(p)}(2)\bar\chi^{(p)}(\mathcal{T})\chi^\circ(t_{12}t_{13}t_{23})\bar\psi_2\psi_3(t_{13})\bar\psi_1\psi_3(t_{23})\times$$

$$\times\det(\mathcal{T})^{k-2r-\kappa}Q(p^{2v}\,\mathrm{diag}(R_1,R_2,R_3),\mathcal{T};k-2r,r)2^r a_{\chi,r}(\mathcal{T}).$$

Let us notice that, for any $\mathcal{T}$ with $\mathrm{diag}(\mathcal{T})=(p^{2v}t_1,p^{2v}t_2,p^{2v}t_3)$ one has

$$\begin{aligned}
&\det(\mathcal{T})\equiv 2t_{12}t_{13}t_{23}\bmod p^{2v},\\
&\qquad\chi^{(p)}(2t_{12}t_{13}t_{23})=\chi^{(p)}(\det(\mathcal{T}))=\chi(\det(\mathcal{T})\overline{\chi^\circ(\det(\mathcal{T})},\\
&2^r a_{\chi,r}(\mathcal{T})=\int_Y y_p^r\chi(y)\mathrm{d}\mathcal{F}_{\mathcal{T}},\\
&\qquad\text{with }\chi=\chi^{(p)}\chi^\circ,\chi^{(p)}\bmod p^v,\chi^\circ\bmod N,\text{ and }p\nmid N,
\end{aligned}$$

for a bounded measure $\mathcal{F}_{\mathcal{T}}$ on Y with values in $\overline{\mathbb{Q}}$. It follows that

$$v_{\chi,r}(\mathcal{T},\mathrm{diag}(R_1,R_2,R_3))$$

$$=\chi^{(p)}(2)\bar\chi(\det(\mathcal{T}))\det(\mathcal{T})^{-r}\overline{\chi^\circ(\det(\mathcal{T})}\bar\psi_2\psi_3(t_{13})\bar\psi_1\psi_3(t_{23})\cdot \tag{3.6}$$

$$\cdot\det(\mathcal{T})^{k-r-\kappa}Q(p^{2v}\,\mathrm{diag}(R_1,R_2,R_3),\mathcal{T};k-2r,r)2^r a_{\chi,r}(\mathcal{T}) \tag{3.7}$$

$$=\det(\mathcal{T})^{k-r-\kappa}Q(p^{2v}\,\mathrm{diag}(R_1,R_2,R_3),\mathcal{T};k-2r,r)\overline{\chi^\circ}(2)\int_Y\chi y_p^r\mathrm{d}\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3},$$

where $\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3}$ denotes the bounded measure defined by the equality:

$$\begin{aligned}\int_Y \chi y_p^r \mathrm{d}\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (3.8)\\ = \chi^{(p)}(2)\chi^\circ(2)2^r\bar{\chi}(\det(\mathcal{T}))\det(\mathcal{T})^{-r}\overline{\chi^\circ(\det(\mathcal{T})}\bar{\psi}_2\psi_3(t_{13})\bar{\psi}_1\psi_3(t_{23})a_{\chi,r}(\mathcal{T}).\end{aligned}$$

3.5 Main Congruence for the Fourier expansions

Let us use the orthogonality relations for Dirichlet characters in order to prove the admissibility of the distributions given by the sequence $\pi_\lambda(\Phi_r(\chi))$ using the Fourier expansions (3.4). According to the admissibility criterion of Theorem 2.4 we need to check the following *Main Congruence*:

$$\begin{aligned}\Big|\sum_{r'=0}^{r}\binom{r}{r'}(-a_p^0)^{r-r'}\frac{1}{\varphi(Np^v)}\sum_{\chi \mod Np^v}\chi^{-1}(a)v_{\chi,r'}(\mathcal{T},p^{2v}\operatorname{diag}(R_1,R_2,R_3))\Big|_p\\ \le Cp^{-vr}, \qquad (3.9)\end{aligned}$$

where we use the notation (3.6) for $v_{\chi,r'}(\mathcal{T},\operatorname{diag}(R_1,R_2,R_3))$, implying that the coefficients

$$i_p(v_{\chi,r'}(\mathcal{T},\operatorname{diag}(R_1,R_2,R_3)))$$

in (3.5) are given as sums of the following expressions:

$$\begin{aligned}B_r(\chi,\mathcal{T}) = \overline{\chi^\circ}(2)\det(\mathcal{T})^{k-r-\kappa}\int_Y \chi y_p^r \mathrm{d}\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3}\cdot \qquad (3.10)\\ \cdot\sum_{t=0}^{r}\binom{r}{t}\det(\mathcal{T})^{r-t}\sum_{|L|\le mt-t}R_L(\kappa-k+r)Q_L(p^{2v}\operatorname{diag}(R_1,R_2,R_3),\mathcal{T}),\end{aligned}$$

where $\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3}$ denotes the bounded measure defined by (3.8). Using the expressions (3.10), the main congruence (3.9) is reduced to proving the congruence for the numbers $B_r(\chi,\mathcal{T})$: there exists a non-zero integer C_k such that

$$\begin{aligned}C_k\cdot\sum_{r'=0}^{r}\binom{r}{r'}(-a_p^0)^{r-r'}\frac{1}{\varphi(Np^v)}\sum_{\chi \mod Np^v}\chi^{-1}(a)B_{r'}(\chi,\mathcal{T}) \equiv 0 \mod p^{vr}\\ (3.11)\\ \iff C_k\cdot A \equiv 0 \mod Np^{vr},\end{aligned}$$

where we use the notation

$$A = A_r(\mathcal{T}; \chi^\circ, \psi_1, \psi_2, \psi_3) = \sum_{r'=0}^{r} \binom{r}{r'} (-a_p^0)^{r-r'} \frac{1}{\varphi(Np^v)} \sum_{\chi \bmod Np^v} \chi^{-1}(a) \cdot \tag{3.12}$$

$$\cdot \overline{\chi^\circ}(2) \det(\mathcal{T})^{k-r'-\kappa} \int_Y \chi y_p^{r'} \, d\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3} \sum_{t=0}^{r'} \binom{r'}{t} \det(\mathcal{T})^{r'-t}$$

$$\sum_{|L| \le mt-t} R_L(\kappa - k + r') Q_L(p^{2v} \operatorname{diag}(R_1, R_2, R_3), \mathcal{T}).$$

Note that $R_L(\kappa - k + r')$ is a polynomial of degree $mt - |L| = 3t - |L|$ in $\kappa - k + r'$ (see (3.1)), hence in r', and $\binom{r'}{t}$ is a polynomial of degree t in r'. One can therefore write

$$\binom{r'}{t} R_L(\kappa - k + r) = \sum_{n=0}^{4t-|L|} \mu_n \frac{(r'+n+1)!}{(r'+1)!}.$$

Here the coefficients μ_n are fixed rational numbers (independent of r').
Using the orthogonality relations for Dirichlet characters mod Np^v, we see that the sum over r' in (3.12), denoted by $C = C_r(t, L, \mathcal{T}; \chi^\circ, \psi_1, \psi_2, \psi_3)$, takes the form

$$C_r(t, L, \mathcal{T}; \chi^\circ, \psi_1, \psi_2, \psi_3) = \overline{\chi^\circ}(2) \det(\mathcal{T})^{k-t-\kappa}$$

$$\int_{y \equiv a \bmod p^v} \sum_{n=0}^{4t-|L|} \mu_n \underbrace{\sum_{r'=0}^{r} \binom{r}{r'} (-a)^{r-r'} \frac{(r'+n+1)!}{(r'+1)!} y^{r'}}_{y^{-n} \frac{\partial^n}{\partial y^n} \left(y^{n+1}(y-a)^r\right)} d\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3}(y)$$

Note that we write $\chi = \chi^\circ \chi^{(p)}$, fix χ°, and sum over all characters $\chi^{(p)}$ mod p^v. We have therefore $(y-a)^r \equiv 0 \bmod (p^v)^r$ in the integration domain $y \equiv a$ mod p^v, implying the congruence

$$c_k C_r(t, L, \mathcal{T}; \chi^\circ, \psi_1, \psi_2, \psi_3) \equiv 0 \pmod{(p^v)^{r-n}} \equiv 0 \pmod{(p^v)^{r-4t+|L|}}, \tag{3.13}$$

where $c_k \in \mathbb{Q}^*$ is a nonzero constant coming from the denominators of the fixed rational numbers μ_n, and of the bounded distributions $\mathcal{F}_{\mathcal{T};\chi^\circ,\psi_1,\psi_2,\psi_3}$.

3.6 Proof of the Main Congruence

Now the expression (3.12) transforms to

$$A_r(\mathcal{T}) = \sum_{t=0}^{r} \sum_{|L| \le 2t} \det(\mathcal{T})^t \cdot C(t, L, \mathcal{T}) \det(\mathcal{T})^{k-2r-\kappa} Q_L(p^{2v} \operatorname{diag}(R_1, R_2, R_3), \mathcal{T}), \tag{3.14}$$

where $Q_L(p^{2v}\operatorname{diag}(R_1,R_2,R_3),\mathcal{T})$ is a homogeneuos polynomial of degree $3t-|L|$ in the variables R_{ij} implying the congruence

$$Q_L(p^{2v}\operatorname{diag}(R_1,R_2,R_3),\mathcal{T}) \equiv 0 \pmod{(p^{2v})^{(3t-|L|)}}. \tag{3.15}$$

On the other hand we know from the description (3.1) of the polynomial

$$Q(R,\mathcal{T}) = Q(R,\mathcal{T};k-2r,r) = \sum_{t=0}^{r}\binom{r}{t}\det(\mathcal{T})^{r-t}\sum_{|L|\le 2t} R_L(\kappa-k+r)Q_L(R,\mathcal{T}),$$

$$Q_L(R,\mathcal{T}) = \operatorname{tr}\left({}^t\rho_{3-l_1}(R)\rho^\star_{l_1}(\mathcal{T})\right)\cdot\ldots\cdot\operatorname{tr}\left({}^t\rho_{3-l_t}(R)\rho^\star_{l_t}(\mathcal{T})\right),$$

that $2t-|L|\ge 0$ so we obtain the desired congruence as follows

$$\begin{cases} c_kC_r(t,L,\mathcal{T})\equiv 0 \pmod{(p^v)^{r-4t+|L|}} \\ Q_L(p^{2v}\operatorname{diag}(R_1,R_2,R_3),\mathcal{T})\equiv 0 \pmod{(p^{2v})^{(3t-|L|)}} \end{cases} \tag{3.16}$$
$$\Rightarrow c_kA_r(\mathcal{T})\equiv 0 \pmod{p^{vr}},$$

since $v(r-4t+|L|)+2v(3t-|L|) = vr+2vt-v|L| \ge vr$, proving (3.9). ∎

3.7 Construction of admissible measures with values in nearly-holomorphic modular forms

We wish now to construct an h-admissible measure $\tilde\Phi^\lambda : \mathcal{P}^h(Y,A)\to\mathcal{M}_T(A)$ on Y out of the following sequence of the higher twists of Siegel-Eisenstein distributions given by the equality (1.2):

$$\Phi_r := 2^r\operatorname{diag}^*\Psi_r = 2^rF^{\bar\chi_1,\bar\chi_2,\bar\chi_3}_{\chi,r},\ \Phi_r:\mathcal{P}^1(Y,A)\to\mathcal{M}_T(A)$$

(they take values in the A-module

$$M=\mathcal{M}_T(\psi_1,\psi_2,\psi_3;A)\subset\mathcal{M}_{k,r}(\psi_1;A)\otimes\mathcal{M}_{k,r}(\psi_2;A)\otimes\mathcal{M}_{k,r}(\psi_3;A)$$

of triple modular forms over $A=\mathbb{C}_p$ or $A=\overline{\mathbb{Q}}$).

Theorem 3.1 *Let $\lambda\in A$ be an element whose absolute value is a positive constant with $0<|\lambda|_p<1$, and define $h=[2\mathrm{ord}_p(\lambda)]+1$. Then the sequence (1.2) satisfies for any $(a)_v\subset Y$ the following two conditions:*

$$\Phi_r\big((a)_v\big)\in\mathcal{M}(N'p^{2v}),\ \textit{with } N' \textit{ independent of } v, \qquad (\textit{level})$$

$$\left|U_T^{2v}\Big(\sum_{r'=0}^{r}\binom{r}{r'}(-y_p^0)^{r-r'}\Phi_{r'}\big((a)_v\big)\Big)\right|_p \le Cp^{-vr} \qquad (\textit{growth})$$

for all $r=0,1,\ldots,h-1$.
Moreover, there exists an h-admissible measure $\tilde\Phi^\lambda:\mathcal{P}^h(Y,A)\to\mathcal{M}_T$ such that for all $((a)_v)\subset Y$ and for all $r=0,1,\ldots,h-1$ one has

$$\int_{(a)_v} y_p^r\,d\tilde\Phi^\lambda = \Phi_r^\lambda((a)_v)$$

where

$$\Phi_r^\lambda((a)_v) = \pi_{\lambda,T}(\Phi_r((a)_v)) := U_T^{-2v}\left[\pi_{\lambda,1}U_T^{2v}\Phi_r((a)_v)\right]$$

is the canonical projection of π_λ *of the triple modular form* $\Phi_r((a)_v)$ *(note that* $U_T^{2v}\Phi_r((a)_v) \in \mathcal{M}_T(Np^{2v};A)^\lambda = \mathcal{M}_T(Np;A)^\lambda$ *because of the inclusion* $U_T^{2v-1}(\mathcal{M}_T(Np^{2v};A)) \subset \mathcal{M}_T(Np;A)$ for all $v \geq 1$*, see Proposition 2.3 (a)).*

Proof. We use Theorem 2.4 with $\varkappa = 2$, and we to check the h-growth condition for the A-linear map

$$\tilde{\Phi}^\lambda : \mathcal{P}^h(Y,A) \to \mathcal{M}_T(A)$$

defined in Theorem 3.1. We have to check that for any $((a)_v) \in Y$ the following two conditions are satisfied: for all $r = 0, 1, \ldots, h-1$,

$$\Phi_r((a)_v) \in \mathcal{M}(N^2p^{2v}), \qquad (level)$$

$$\left| U_T^{2v}\Big(\sum_{r'=0}^{r}\binom{r}{r'}(-y_p^0)^{r-r'}\Phi_{r'}((a)_v)\Big)\right|_p \leq Cp^{-vr}. \qquad (growth)$$

The (*level*) condition is implied by the definition (1.2)

$$\Phi_r(\chi) = 2^r \operatorname{diag}^* F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3},$$

and Proposition 1.5.

The (*growth*) is deduced from the Main Congruence (3.9) (proved in Section 3.6) for the Fourier coefficients of the functions (1.2). ∎

4 A trilinear form on the characteristic subspace of the U-operator

4.1 The adjoint operator U^*

Let $f = \sum_{n=1}^\infty a_nq^n$ denote a primitive cusp eigenform of conductor dividing Np, with coefficients $i_p(a_n)$ in a finite extension K of $\mathbb{Q}_p$ and of Dirichlet character ψ modulo N. Let $\alpha \in K$ be a root of the Hecke polynomial $x^2 - a_p(f)x + \psi(p)p^{k-1}$ as above, and let α' denote the other root.

Recall that the function $f_0 = \sum_{n=1}^\infty a_n(f_0)q^n \in \overline{\mathbb{Q}}[[q]]$ is defined by (0.9) as an eigenfunction of $U = U_p$ with the eigenvalue $\alpha \in \overline{\mathbb{Q}}$. In the following proposition, let U^* denote the operator adjoint to

$$U = U_p : \mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C}) \to \mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$$

in the complex vector space $\mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$ with respect to the Petersson inner product.

Proposition 4.1 (a) *The following operator identity holds:* $U^* = W_{Np}^{-1}UW_{Np}$ *(in the complex vector space* $\mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$*).*

(b) *There are the following identities in* $\mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$*:*

$$f^0|U^* = \overline{\alpha} f^0 \text{ and } T_l(f^0) = a_l(f)f^0$$

for all "good primes" $l \nmid Np$.
(c) *The linear form* $g \mapsto \langle f^0, g\rangle_{Np}$ *on* $\mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$ *vanishes on the complex vector subspace* $\mathrm{Ker}\pi_{\alpha,1} = \mathrm{Im}(U-\alpha I)^{n_1}$ *where* $n_1 = \dim \mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$*, and we use the same notation as above*

$$\pi_{\alpha,1} : \mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C}) \to \mathcal{M}^{\alpha}_{r,k}(\Gamma_1(Np),\mathbb{C})$$

for the complex characteristic projection onto the α*-primary subspace of the operator* U *(acting on the finite-dimensional complex vector space* $\mathcal{M}_{r,k}(\Gamma_1(Np),\mathbb{C})$*) hence*

$$\langle f^0, g\rangle_{Np} = \langle f^0, \pi_{\alpha,1}(g)\rangle_{Np}$$

(d) *If* $g \in \mathcal{M}(Np^{v+1};\overline{\mathbb{Q}})$ *and* $\alpha \neq 0$*, then we have the equality*

$$\langle f^0, \pi_\alpha(g)\rangle_{Np} = \alpha^{-v}\langle f^0, U^v g\rangle_{Np}$$

where

$$\pi_\alpha(g) = g^\alpha = U^{-v}\big[\pi_{\alpha,1}U^v g\big] \in \mathcal{M}^\alpha(Np)$$

is the α*-part of* g.
(e) *The linear form*

$$\mathcal{L}_{f,\alpha} : \mathcal{M}(Np^v;\mathbb{C}) \to \mathbb{C}, \quad g \mapsto \frac{\langle f^0, \alpha^{-v}U^v(g)\rangle_{Np}}{\langle f^0, f_0\rangle_{Np}}$$

is defined over $\overline{\mathbb{Q}}$*:*

$$\mathcal{L}_{f,\alpha} : \mathcal{M}(Np^v;\overline{\mathbb{Q}}) \to \overline{\mathbb{Q}}$$

and there exists a unique $\mathbb{C}_p$*-linear form* $\ell_{f,\alpha}$ *on* $\mathcal{M}(Np^v;\mathbb{C}_p) = \mathcal{M}(Np^v;\overline{\mathbb{Q}})\otimes_{i_p}\mathbb{C}_p$ *such that* $\ell_{f,\alpha}(g) = i_p(\mathcal{L}_{f,\alpha}(g))$ *for all* $g \in i_p(\mathcal{M}(Np^v;\overline{\mathbb{Q}}))$.

Proof (a) See [Miy], Theorem 4.5.5 (see also [Ran90]).
(b) Let us use directly the statement a):

$$f^0|U^* = f_0^\rho|W_{Np}W_{Np}^{-1}UW_{Np} = \bar{\alpha}f^\rho|W_{Np} = \bar{\alpha}f^0.$$

(c) If $g \in \mathrm{Ker}\pi_{\alpha,1} = \mathrm{Im}(U-\alpha I)^{n_1}$ then $g = (U-\alpha I)^{n_1}g_1$ and

$$\langle f^0, (U-\alpha I)^{n_1}g_1\rangle_{Np} = \langle (U^* - \bar{\alpha}I)f^0, (U-\alpha I)^{n_1-1}g_1\rangle_{Np} = 0$$

hence $\langle f^0, g\rangle_{Np} = 0$; moreover

$$\langle f^0, g\rangle_{Np} = \langle f^0, \pi_{\alpha,1}(g) + (g - \pi_{\alpha,1}(g))\rangle_{Np} = \langle f^0, \pi_{\alpha,1}(g)\rangle_{Np}.$$

(d) Let us use the definitions and write the following product:

$$\begin{aligned}\alpha^v\langle f^0,\pi_\alpha g\rangle_{Np} &= \langle U^{*v}(f^0),U^{-v}\big[\pi_{\alpha,1}U^v g\big]\rangle_{Np}\\ &= \langle f^0,\pi_{\alpha,1}(U^v g)\rangle_{Np} = \langle f^0,U^v g\rangle_{Np}\end{aligned}$$

by (c) as $U^v g\in\mathcal{M}(Np)$.
(e) Note that $\mathcal{L}_{f,\alpha}(f_0)=1$, $f_0\in\mathcal{M}(Np;\overline{\mathbb{Q}})$. Consider the complex vector space

$$\mathrm{Ker}\mathcal{L}_{f,\alpha}=\langle f^0\rangle^\perp=\{g\in\mathcal{M}(Np^v;\mathbb{C})\mid\langle f^0,g\rangle_{Np^v}=0\}.$$

It admits a $\overline{\mathbb{Q}}$-rational basis (as it is stable under all “good” Hecke operators T_l $(l\nmid Np)$:

$$\langle f^0,g\rangle_{Np^v}=0\Rightarrow\langle f^0,T_l g\rangle_{Np^v}=\langle T_l^* f^0,g\rangle_{Np^v}=0$$

and diagonalizing the action of T_l (over $\overline{\mathbb{Q}}$) we get such a basis establishing e). We obtain then the $\mathbb{C}_p$-linear form $\ell_{f,\alpha}$ on $\mathcal{M}(Np^v;\mathbb{C}_p)=\mathcal{M}(Np^v;\overline{\mathbb{Q}})\otimes_{i_p}\mathbb{C}_p$ such that $\ell_{f,\alpha}(g)=i_p(\mathcal{L}_{f,\alpha}(g))$ by extending scalars from $\overline{\mathbb{Q}}$ to $\mathbb{C}_p$ via the imbedding i_p.
Note that we use here only the α-part $\mathcal{M}(Np^v;A)^\alpha$ because the constructed linear form $\ell_{f,\alpha}$ passes through the π_α (for $A=\mathbb{C}_p$, $A=\overline{\mathbb{Q}}$, or $A=\mathbb{C}$). Moreover, f_0 can be included to a basis $\{f_0,g_i\}_{i=2,\cdots,n}$ of $\mathcal{M}(Np^v;A)^\alpha$, where g_i are eigenfunctions of all Hecke operators T_l for primes $l\nmid Np$; they are algebraically orthogonal to f_0 (in the sense of the algebraic Petersson product studied by Hida [Hi90]) so that projection to the f_0 part of this basis gives such an A-linear form.

4.2 The triple U-operator

In the following proposition, we consider the triple U-operator

$$U_T=U_{1,p}\otimes U_{2,p}\otimes U_{3,p}:\mathcal{M}_T(\Gamma_1(Np),\mathbb{C})\to\mathcal{M}_T(\Gamma_1(Np),\mathbb{C}),\ \text{where}\qquad(4.1)$$

$$\mathcal{M}_T(\Gamma_1(Np),\mathbb{C})=\mathcal{M}_{k_1}(\Gamma_1(Np),\mathbb{C})\otimes\mathcal{M}_{k_2}(\Gamma_1(Np),\mathbb{C})\otimes\mathcal{M}_{k_3}(\Gamma_1(Np),\mathbb{C}),$$

acting on the complex vector space $\mathcal{M}_T(\Gamma_1(Np),\mathbb{C})$ endowed with the triple Petersson inner product $\langle\cdot,\cdot\rangle$ defined by

$$\langle g_1\otimes g_2\otimes g_3,h_1\otimes h_2\otimes h_3\rangle_T=\langle g_1,h_1\rangle_{Np}\langle g_2,h_2\rangle_{Np}\langle g_3,h_3\rangle_{Np}.$$

Let

$$U_T^*=U_{1,p}^*\otimes U_{2,p}^*\otimes U_{3,p}^*$$

denote the adjoint operator on $\mathcal{M}_T(\Gamma_1(Np),\mathbb{C})$ for the triple Petersson inner product. Recall the notation (0.9) and (0.10):

$$\begin{aligned}f_{j,0}&=f_j-\alpha_{p,j}^{(2)}f_j|V_p=f_j-\alpha_{p,j}^{(2)}p^{-k/2}f_j|\begin{pmatrix}p\,0\\0\,1\end{pmatrix}\\ f_{j,0}^\rho&=\sum_{n=1}^\infty\overline{a(n,f_0)}q^n,\ \ f_j^0=f_{j,0}^\rho|_k\ W_{Np}=f_{j,0}^\rho\Big|_k\begin{pmatrix}0&-1\\Np&0\end{pmatrix}.\end{aligned}$$

Proposition 4.2 (a) *The following operator identity holds:*

$$U_T^* = W_{Np}^{-1}U_{p,1}W_{Np} \otimes W_{Np}^{-1}U_{p,2}W_{Np} \otimes W_{Np}^{-1}U_{p,3}W_{Np}$$

(in the complex vector space $\mathcal{M}_T(\Gamma_1(Np), \mathbb{C})$).
(b) *There are the following identities in $\mathcal{M}_T(\Gamma_1(Np), \mathbb{C})$:*

$$U_T^*(f_1^0 \otimes f_2^0 \otimes f_3^0) = \overline{\lambda}(f_1^0 \otimes f_2^0 \otimes f_3^0).$$

(c)*The linear form on $\mathcal{M}_T(\Gamma_1(Np), \mathbb{C})$ defined by*

$$g_1 \otimes g_2 \otimes g_3 \otimes \mapsto \left\langle f_1^0 \otimes f_2^0 \otimes f_3^0, g_1 \otimes g_2 \otimes g_3 \right\rangle_T = \langle f_1^0, g_1\rangle_{Np}\langle f_2^0, g_2\rangle_{Np}\langle f_3^0, g_3\rangle_{Np}$$

vanishes on the complex vector subspace $\mathrm{Ker}\,\pi_{\lambda,T,1} = \mathrm{Im}(U_T - \lambda I)^{n_T}$ where we write $n_T = \dim \mathcal{M}_T(\Gamma_1(Np), \mathbb{C})$, and we use the notation

$$\pi_{\lambda,T,1} : \mathcal{M}_T(\Gamma_1(Np), \mathbb{C}) \to \mathcal{M}_T^\lambda(\Gamma_1(Np), \mathbb{C})$$

for the complex characteristic projection onto the λ-primary subspace of the operator U_T acting on the finite-dimensional complex vector space $\mathcal{M}_T(\Gamma_1(Np), \mathbb{C})$. Moreover, the following equality holds

$$\left\langle f_1^0 \otimes f_2^0 \otimes f_3^0, g_1 \otimes g_2 \otimes g_3 \right\rangle_T = \left\langle f_1^0 \otimes f_2^0 \otimes f_3^0, \pi_{\lambda,T,1}(g_1 \otimes g_2 \otimes g_3) \right\rangle_T.$$

(d) *If $g \in \mathcal{M}_T(Np^{v+1}; \overline{\mathbb{Q}})$ and $\lambda \neq 0$, then we have the equality*

$$\langle f_1^0 \otimes f_2^0 \otimes f_3^0, \pi_{\lambda,T}(g)\rangle_{T,Np} = \lambda^{-v}\langle f_1^0 \otimes f_2^0 \otimes f_3^0, U_T^v g\rangle_{T,Np}$$

where

$$\pi_{\lambda,T}(g) = g^\lambda = U_T^{-v}\left[\pi_{\lambda,T,1}U_T^v g\right] \in \mathcal{M}_T^\lambda(Np)$$

is the λ-part of g.
(e) *The linear form*

$$\mathcal{L}_{T,\lambda} : \mathcal{M}_T(Np^v; \mathbb{C}) \to \mathbb{C}, \quad g \mapsto \frac{\langle f_1^0 \otimes f_2^0 \otimes f_3^0, \lambda^{-v}U_T^v g\rangle_{T,Np}}{\langle f_1^0 \otimes f_2^0 \otimes f_3^0, f_{1,0} \otimes f_{2,0} \otimes f_{3,0}\rangle_{T,Np}}$$

is defined over $\overline{\mathbb{Q}}$:

$$\mathcal{L}_{T,\lambda} : \mathcal{M}_T(Np^v; \overline{\mathbb{Q}}) \to \overline{\mathbb{Q}}$$

and there exists a unique $\mathbb{C}_p$-linear form $\ell_{T,\lambda}$ on $\mathcal{M}_T(Np^v; \mathbb{C}_p) = \mathcal{M}_T(Np^v; \overline{\mathbb{Q}}) \otimes_{i_p} \mathbb{C}_p$ such that $\ell_{T,\lambda}(g) = i_p(\mathcal{L}_{f,\alpha}(g))$ for all $g \in i_p(\mathcal{M}_T(Np^v; \overline{\mathbb{Q}}))$.

Remark 4.3 *We may view the trilinear form*

$$(g_1, g_2, g_3) \mapsto \ell_{T,\lambda}(g_1 \otimes g_2 \otimes g_3)$$

as a p-adic version of the triple Petersson product following Hida [Hi90].

Proof of Proposition 4.2, a), b) follows directly from that of Proposition 4.1. In order to prove c) we need to show that the linear form on $\mathcal{M}_T(\Gamma_1(Np),\mathbb{C})$ defined by

$$\begin{aligned} g_1\otimes g_2\otimes g_3\otimes \mapsto \left\langle f_1^0\otimes f_2^0\otimes f_3^0, g_1\otimes g_2\otimes g_3\right\rangle_{T,Np} \\ = \langle f_1^0, g_1\rangle_{Np}\langle f_2^0, g_2\rangle_{Np}\langle f_3^0, g_3\rangle_{Np}\end{aligned}$$

vanishes on the complex vector subspace

$$\operatorname{Ker}\pi_{\lambda,T,1} = \operatorname{Im}(U_T-\lambda I)^{n_T} = (\operatorname{Ker}(U_T^*-\overline{\lambda}I)^{n_T})^{\perp}.$$

It suffices to notice that

$$f_1^0\otimes f_2^0\otimes f_3^0 \in \operatorname{Ker}(U_T^*-\overline{\lambda}I)\subset \operatorname{Ker}(U_T^*-\overline{\lambda}I)^{n_T},$$

because of the equality

$$U_T^*(f_1^0\otimes f_2^0\otimes f_3^0) = U_{1,p}^*(f_1^0)\otimes U_{2,p}^*(f_2^0)\otimes U_{3,p}^*(f_3^0) = \overline{\lambda}(f_1^0\otimes f_2^0\otimes f_3^0).$$

More precisely, if $g\in\operatorname{Ker}\pi_{\lambda,T,1} = \operatorname{Im}(U_T-\lambda I)^{n_T}$ then $g=(U_T-\lambda I)^{n_T}g_1$ and

$$\begin{aligned}&\langle f_1^0\otimes f_2^0\otimes f_3^0, (U_T-\lambda I)^n g_1\rangle_{T,Np}\\ &= \langle (U_T^*-\overline{\lambda}I)(f_1^0\otimes f_2^0\otimes f_3^0, (U_T-\lambda I)^{n-1}g_1)\rangle_{T,Np} = 0\end{aligned}$$

hence $\langle f_1^0\otimes f_2^0\otimes f_3^0, g\rangle_{T,Np}=0$. Moreover, the following equality holds

$$\left\langle f_1^0\otimes f_2^0\otimes f_3^0, g_1\otimes g_2\otimes g_3\right\rangle_T = \left\langle f_1^0\otimes f_2^0\otimes f_3^0, \pi_{\lambda,T,1}(g_1\otimes g_2\otimes g_3)\right\rangle_T,$$

by the definition of the projection $\pi_{\lambda,T,1}$:

$$g_1\otimes g_2\otimes g_3 - \pi_{\lambda,T,1}(g_1\otimes g_2\otimes g_3)\in\operatorname{Ker}\pi_{\lambda,T,1}.$$

d) Let us use the definitions and write the following product:

$$\begin{aligned}&\lambda^v\langle f_1^0\otimes f_2^0\otimes f_3^0, \pi_{\lambda,T}g\rangle_{T,Np} = \langle {U_T^*}^v(f_1^0\otimes f_2^0\otimes f_3^0), U_T^{-v}\left[\pi_{\lambda,T,1}U_T^v g\right]\rangle_{T,Np} =\\ &\langle f_1^0\otimes f_2^0\otimes f_3^0, \pi_{\lambda,T,1}(U_T^v g)\rangle_{T,Np} = \langle f_1^0\otimes f_2^0\otimes f_3^0, U_T^v g\rangle_{T,Np}\end{aligned}$$

by c) as $U_T^v g\in\mathcal{M}_T(Np)$.
e) Note that $\mathcal{L}_{T,\lambda}(f_1^0\otimes f_2^0\otimes f_3^0)=1$, $f_1^0\otimes f_2^0\otimes f_3^0\in\mathcal{M}_T(Np;\overline{\mathbb{Q}})$. Consider the complex vector space

$$\operatorname{Ker}\mathcal{L}_{T,\lambda} = \langle f_1^0\otimes f_2^0\otimes f_3^0\rangle^{\perp} = \{g\in\mathcal{M}_T(Np^v;\mathbb{C}) \mid \langle f^0, g\rangle_{T,Np^v}=0\}.$$

It admits a $\overline{\mathbb{Q}}$-rational basis (as in Proposition 4.1) establishing e).
We obtain then the $\mathbb{C}_p$-linear form $\ell_{T,\lambda}$ on $\mathcal{M}_T(Np^v;\mathbb{C}_p)=\mathcal{M}_T(Np^v;\overline{\mathbb{Q}})\otimes_{i_p}\mathbb{C}_p$ such that $\ell_{T,\lambda}(g)=i_p(\mathcal{L}_{T,\lambda}(g))$ by extending scalars from $\overline{\mathbb{Q}}$ to $\mathbb{C}_p$ via the imbedding i_p. ∎

5 Computation of p-adic integrals and L-values

5.1 Construction of p-adic measures

Let $\mathcal{M} = \mathcal{M}_T(A) = \bigcup_{v\geq 0}\mathcal{M}_{k,r}(Np^v,\psi_1;A)\otimes_A \mathcal{M}_{k,r}(Np^v,\psi_2;A)\otimes_A \mathcal{M}_{k,r}(Np^v,\psi_3;A)$ be the A-module of nearly-holomorphic triple modular forms with formal Fourier coefficients in A, where $A=\mathbb{C}_p$. Let us define an A-valued measure

$$\tilde{\mu}^\lambda(y; f_1\otimes f_2\otimes f_3) : \mathcal{C}^{loc-an}(Y,A)\to A$$

by applying the trilinear form $\ell_{T,\lambda} : \mathcal{M}(Np^v;A)\to A$ of Proposition 4.2

$$\tilde{\mu}^\lambda(y; f_1\otimes f_2\otimes f_3) = \ell_{T,\lambda}(\tilde{\Phi}^\lambda) \tag{5.1}$$

to the h-admissible measure $\tilde{\Phi}^\lambda$ of Theorem 2.4 on Y with values in $\mathcal{M}(A)^\lambda\subset\mathcal{M}(Np;A)$. That h-admissible measure was defined as an A-linear map $\tilde{\Phi}^\lambda : \mathcal{P}^h(Y,A)\to\mathcal{M}(A)^\lambda$ satisfying for any $(a)_\nu\subset Y$ and for all $r=0,1,\ldots,h-1$ the following equality:

$$\int_{(a)_\nu} y_p^r\, d\tilde{\Phi}^\lambda = \pi_\lambda(\Phi_r((a)_\nu))\in\mathcal{M}(Np),$$

where $h=[2\mathrm{ord}_p\lambda(p)]+1$, hence

$$\int_{(a)_\nu} y_p^r\,\mathrm{d}\tilde{\mu}^\lambda(y; f_1\otimes f_2\otimes f_3) = \ell_{T,\lambda}\left(\int_{(a)_\nu} y_p^r\,\mathrm{d}\tilde{\Phi}^\lambda(y)\right). \tag{5.2}$$

5.2 Evaluation of the integral

$$\int_Y \chi(y)\, y_p^r\,\mathrm{d}\tilde{\mu}^\lambda(y; f_1\otimes f_2\otimes f_3) \tag{5.3}$$

for $r\in\mathbb{N}$, $0\leq r\leq k-2$. The result is given in terms of Garrett's triple L function $\mathcal{D}^\star(f_1^\rho\otimes f_2^\rho\otimes f_3^\rho, 2k-2-r,\psi_1\psi_2\chi)$. Let us use the action of the involution $W_{N_j}=\begin{pmatrix}0 & -1\\ N_j & 0\end{pmatrix}$ of the exact level N_j of f_j:

$$f_j\big|_k W_{N_j} = \begin{pmatrix}0 & -1\\ N_j & 0\end{pmatrix} = \gamma_j\cdot f_j^\rho,\qquad f_j^\rho\big|_k W_{N_j} = \begin{pmatrix}0 & -1\\ N_j & 0\end{pmatrix} = \bar{\gamma}_j\cdot f_j,$$

$$\text{where } f_j^\rho(z) = \sum_{n=1}^\infty \bar{a}_{n,j}e(nz)\in\mathcal{S}_k(N_j,\bar{\psi}_j), \tag{5.4}$$

$$(j=1,2,3) \text{ and } \gamma_j \text{ is the corresponding root number.} \tag{5.5}$$

Recall the notation (0.9) and (0.10):

$$f_{j,0} = f_j - \alpha_{p,j}^{(2)} f_j|V_p = f_j - \alpha_{p,j}^{(2)} p^{-k/2} f_j| \begin{pmatrix} p\,0 \\ 0\,1 \end{pmatrix}$$
$$f_{j,0}^{\rho} = \sum_{n=1}^{\infty} \overline{a(n, f_0)} q^n, \; f_j^0 = f_{j,0}^{\rho}|_k \; W_{Np} = f_{j,0}^{\rho}\Big|_k \begin{pmatrix} 0 & -1 \\ Np & 0 \end{pmatrix}.$$

Proposition 5.1 *Under the notations and assumptions as in Theorem B.2, the value of the integral (5.3) is given for $0 \le r \le k-2$ by the image under i_p of the following algebraic number*

$$T \cdot \lambda^{-2v} \mathfrak{L}_{Np}(-r) \frac{\mathcal{D}^{\star}(f_1^{\rho} \otimes f_2^{\rho} \otimes f_3^{\rho}, 2k-2-r, \psi_1\psi_2\chi)}{\langle f_1^0 \otimes f_2^0 \otimes f_3^0, f_{1,0} \otimes f_{2,0} \otimes f_{3,0} \otimes \rangle_{T,N^2p^{2v}}},$$

where

$$T = 2^{-r} \frac{((Np)^3/N_1N_2N_3)^{k/2} \bar{\gamma}_1\bar{\gamma}_2\bar{\gamma}_3 (\chi_1\chi_2\chi_3)(2) p^{3\cdot v(k-2)}}{N_{1,1}N_{1,2}N_{1,3} G(\chi_{1,0}) G(\chi_{2,0}) G(\chi_{3,0})} \times$$
$$\times (Np^{2v})^{k-2r} \frac{N^2p^{2v} \varphi(N^2p^{2v}) \varphi(Np^v)}{[\Gamma_0(N^2p^{2v}) : \Gamma(N^2p^{2v})]^3}.$$

γ_j is the corresponding root number, given by (5.4), and the factor $\mathfrak{L}_{Np}(-r)$, given by (5.13).

Remark. In particular, Propostion 5.1 implies Theorem A, using a computation by B.Gorsse and G.Robert (see [Go-Ro]) that for some $\beta \in \overline{\mathbb{Q}}^*$

$$\langle f_1^{0,\rho} \otimes f_2^{0,\rho} \otimes f_3^{0,\rho}, f_{1,0}^{\rho} \otimes f_{2,0}^{\rho} \otimes f_{3,0}^{\rho} \rangle_{T,Np} = \beta \cdot \langle f_1, f_1 \rangle_N \langle f_2, f_2 \rangle_N \langle f_3, f_3 \rangle_N.$$

5.3 Evaluation of the trilinear form

In order to compute the p-adic integral, the next step of the proof uses computations similar to those in [Hi85], §4 and §7. More precisely let us write the integral in the form

$$\int_Y \chi(y)\, y_p^r \, \mathrm{d}\tilde{\mu}_{\lambda}(y; f_1 \otimes f_2 \otimes f_3) = \sum_{a \in Y_v} \chi(a) \int_{(a)_v} y_p^r \, \mathrm{d}\ell_{T,\lambda}(\tilde{\Phi}^{\lambda})(y)) =$$
$$= \ell_{T,\lambda} \left(\sum_{a \in Y_v} \chi(a) \int_{(a)_v} y_p^r \, \mathrm{d}\tilde{\Phi}^{\lambda}(y) \right) = \ell_{T,\lambda} \left(\sum_{a \in Y_v} \chi(a) \Phi_r^{\lambda}((a)_v) \right), \tag{5.6}$$

where $(a)_v = (a + (Np^v)) \subset Y$, and by definition (5.1)

$$\tilde{\mu}^{\lambda}(y; f_1 \otimes f_2 \otimes f_3) = \ell_{T,\lambda}(\tilde{\Phi}^{\lambda})(y), \tag{5.7}$$

$$\int_{(a)_v} y_p^r \, \mathrm{d}\big(\tilde{\Phi}^{\lambda}\big) = \Phi_r^{\lambda}((a)_v) \in \mathcal{M}_T^{\lambda}(Np) \tag{5.8}$$

for $r = 0, 1, \dots, h-1$. Moreover $\Phi_r\big((a)_v\big)$ is a triple modular form given by (1.2) of level N^2p^{2v} as a value of a higher twist of a Siegel-Eisenstein distributions, hence

$$\Phi_r^\lambda(\chi) = U_T^{-2v}\left[\pi_{\lambda,T,1}U_T^{2v}\left(2^r F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3}\circ \mathrm{diag}\right)\right]. \tag{5.9}$$

Taking into account the equalities (5.9), the integral (5.6) transforms to the following

$$\int_Y \chi(y)\, y_p^r \,\mathrm{d}\tilde\mu^\lambda(y; f_1\otimes f_2\otimes f_3) = \ell_{T,\lambda}\left(\sum_{a\in Y_v}\chi(a)\Phi_r^\lambda((a)_v)\right) \tag{5.10}$$
$$= \ell_{T,\lambda}\Big(U_T^{-2v}\Big[\pi_{\lambda,T,1}U_T^{2v}\big(2^r F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3}\circ \mathrm{diag}\big)\Big]\Big)$$

Notice that then it follows that the sum in the right hand side of the equality (5.10) can be expressed through the functions (1.2):

$$\int_Y \chi(y)\, y_p^r \,\mathrm{d}\tilde\mu^\lambda(y; f_1\otimes f_2\otimes f_3)(y)$$
$$\ell_{T,\lambda}\Big(U_T^{-2v}\Big[\pi_{\lambda,T,1}U_T^{2v}\big(2^r F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3}\circ \mathrm{diag}\big)\Big]\Big) \tag{5.11}$$

where we use the functions (1.2). The function

$$g = \Phi_r(\chi) = 2^r F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3}\circ \mathrm{diag}$$

is computed in (B.5), Appendix B as follows:

$$\mathcal{E}(z_1,z_2,z_3; -r, k, Np^v, \boldsymbol{\psi}, \chi_1,\chi_2,\chi_3)$$
$$= N_{1,1}N_{1,2}N_{1,3}(\bar\chi_1\bar\chi_2\bar\chi_3)(2)G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3})2^{-r}\Phi_r(\chi),$$

thus it is a *nearly-holomorphic* triple modular form in in the $\mathbb{Q}^{\mathrm{ab}}$-module

$$M(\mathbb{Q}^{\mathrm{ab}}) = \mathcal{M}_T(N^2p^{2v}, \psi_1\otimes\psi_2\otimes\psi_3; \mathbb{Q}^{\mathrm{ab}})$$
$$\subset \mathcal{M}_{k,r}(N^2p^{2v},\psi_1;\mathbb{Q}^{\mathrm{ab}})\otimes\mathcal{M}_{k,r}(N^2p^{2v},\psi_2;\mathbb{Q}^{\mathrm{ab}})\otimes\mathcal{M}_{k,r}(N^2p^{2v},\psi_3;\mathbb{Q}^{\mathrm{ab}}).$$

Then by the general formula of Proposition 4.2 e) we have:

$$\mathcal{L}_{T,\lambda}: \mathcal{M}_T(N^2p^{2v};\mathbb{C}) \to \mathbb{C}, \quad g \mapsto \frac{\langle f_1^0\otimes f_2^0\otimes f_3^0, \lambda^{-2v}U_T^{2v}g\rangle_{T,N^2p}}{\langle f_1^0\otimes f_2^0\otimes f_3^0, f_{1,0}\otimes f_{2,0}\otimes f_{3,0}\rangle_{T,N^2p}}, \tag{5.12}$$

$$\ell_{T,\lambda}\left(U_T^{-2v}\left[\pi_{\lambda,T,1}U_T^{2v}(g)\right]\right) = i_p\left(\frac{\langle f_1^0\otimes f_2^0\otimes f_3^0, \lambda^{-2v}U_T^{2v}(g)\rangle_{T,N^2p}}{\langle f_1^0\otimes f_2^0\otimes f_3^0, f_{1,0}\otimes f_{2,0}\otimes f_{3,0}\rangle_{N^2p}}\right)$$
$$= i_p\left(\lambda^{-2v}p^{3\cdot 2v(k-1)}\cdot\frac{\langle V^{2v}(f_1^0\otimes f_2^0\otimes f_3^0), g\rangle_{T,N^2p^{2v+1}}}{\langle f_1^0\otimes f_2^0\otimes f_3^0, f_{1,0}\otimes f_{2,0}\otimes f_{3,0}\rangle_{T,N^2p}}\right).$$

The scalar products in 5.12 can be computed using Theorem B.2, but we omit here the details. This implies Proposition 5.1 using the integral representation of Theorem B.2 for modular forms $\tilde{f}_{j,2v}(z) = \sum_{n=1}^{\infty} a_{j,n,2v} e(nz)$ as above:

$$\mathcal{D}^{\star}(f_1^{\rho} \otimes f_2^{\rho} \otimes f_3^{\rho}, 2k-2-r, \psi_1\psi_2\chi_1) \tag{5.13}$$

$$(Np^{2v})^{k-2r} \frac{N^2p^{2v}\varphi(N^2p^{2v})\varphi(Np^v)}{[\Gamma_0(N^2p^{2v}) : \Gamma(N^2p^{2v})]^3} \times \mathfrak{L}_{Np}(-r)$$

$$= \left\langle \tilde{f}_{1,2v} \otimes \tilde{f}_{2,2v} \otimes \tilde{f}_{3,2v}, \mathcal{E}(z_1, z_2, z_3; -r, k, N^2p^{2v}, \boldsymbol{\psi}, \chi_1, \chi_2, \chi_3) \right\rangle_{T, N^2p^{2v}},$$

where

$$\mathfrak{L}_{Np}(s)=\mathfrak{L}_{Np}(s; \tilde{f}_{1,2v} \otimes \tilde{f}_{2,2v} \otimes \tilde{f}_{3,2v}):=\sum_{n|N^{\infty}} G_N(\overline{\psi_1\psi_2\chi_1}, 2n) \frac{a_{n,1,2v}a_{n,2,2v}a_{n,3,2v}}{n^{2s+2k-2}}.$$

5.4 Proof of Theorem B

Let us use Propostion 5.1 and (5.13):

$$2^{-r} \int_Y \chi(y)\, y_p^r \,\mathrm{d}\tilde{\mu}^{\lambda}(y; f_1 \otimes f_2 \otimes f_3)(y) = 2^{-r} \ell_{T,\lambda} \left(U_T^{-2v} \left[\pi_{\lambda,T,1} U_T^{2v}(g) \right] \right) \tag{5.14}$$

$$= \frac{((Np)^3/N_1N_2N_3)^{k/2} \bar{\gamma}_1\bar{\gamma}_2\bar{\gamma}_3(\chi_1\chi_2\chi_3)(2)p^{3\cdot v(k-2)}}{\lambda^{2v} N_{1,1}N_{2,1}N_{3,1} G(\chi_{1,0})G(\chi_{2,0})G(\chi_{3,0})} \times$$

$$\times (Np^{2v})^{k-2r} \frac{N^2p^{2v}\varphi(N^2p^{2v})\varphi(Np^v)}{[\Gamma_0(N^2p^{2v}) : \Gamma(N^2p^{2v})]^3} \mathfrak{L}_{Np}(-r) \times$$

$$\times \frac{\mathcal{D}^{\star}(f_1^{\rho} \otimes f_2^{\rho} \otimes f_3^{\rho}, 2k-2-r, \psi_1\psi_2\chi_1)}{\langle f_1^0 \otimes f_2^0 \otimes f_3^0, f_{1,0} \otimes f_{2,0} \otimes f_{3,0} \rangle_{T,N^2p}}$$

Let us show that under the assumptions as above there exist an admissible $\mathbb{C}_p$-valued measure $\tilde{\mu}^{\lambda}_{f_1\otimes f_2 \otimes f_3}$ on $Y_{N,p}$, and a $\mathbb{C}_p$-analytic function

$$\mathcal{D}_{(p)}(x, f_1 \otimes f_2 \otimes f_3) : X_p \to \mathbb{C}_p,$$

given for all $x \in X_{N,p}$ by the integral

$$\mathcal{D}_{(p)}(x, f_1 \otimes f_2 \otimes f_3) = \int_{Y_{N,p}} x(y) \mathrm{d}\tilde{\mu}^{\lambda}_{f_1\otimes f_2\otimes f_3}(y),$$

and having the following properties: for all pairs (r, χ) such that for $\chi \in X_p^{\mathrm{tors}}$ the corresponding Dirichlet characters χ_j are Np-complete, and $r \in \mathbb{Z}$ with $0 \le r \le k-2$, the following equality holds:

$$\mathcal{D}_{(p)}(\chi x_p^r, f_1 \otimes f_2 \otimes f_3) = \tag{5.15}$$

$$i_p\Big(\frac{(\psi_1\psi_2)(2)C_\chi^{4(2k-3-r)}}{G(\chi_1)G(\chi_2)G(\chi_3)G(\psi_1\psi_2\chi_1)\lambda(p)^{2v}}$$

$$\frac{\mathcal{D}^\star(f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, 2k-2-r, \psi_1\psi_2\chi)}{\langle f_1^\rho \otimes f_2^\rho \otimes f_3^\rho, f_1^\rho \otimes f_2^\rho \otimes f_3^\rho\rangle_T}\Big)$$

where $v = \mathrm{ord}_p(C_\chi)$, $\chi_1 \bmod Np^v = \chi$, $\chi_2 \bmod Np^v = \psi_2\bar{\psi}_3\chi$, $\chi_3 \bmod Np^v = \psi_1\bar{\psi}_3\chi$, $G(\chi)$ denotes the Gauß sum of a primitive Dirichlet character χ_0 attached to χ (modulo the conductor of χ_0).
Indeed, we may write

$$\mathcal{D}_{(p)}(x, f_1 \otimes f_2 \otimes f_3) = C \cdot x(2) \int_Y x(y) \mathrm{d}\tilde{\mu}^\lambda(y; f_1 \otimes f_2 \otimes f_3)$$

with an appropriate constant, given by the RHS of (5.14), where $v = \mathrm{ord}_p(C_\chi)$. Moreover, it follows from the properties of the constructed measure

$$\tilde{\mu}^\lambda_{f_1\otimes f_2 \otimes f_3}(y) := C \cdot \tilde{\mu}_\lambda(2^{-1}y; f_1 \otimes f_2 \otimes f_3)$$

that

(ii) if $\mathrm{ord}_p\lambda(p) = 0$ then the holomorphic functions in (i), (ii) are bounded $\mathbb{C}_p$-analytic functions: it suffices to use the equality (2.5) with $r = 0$ in order to show that in this case the measure $\tilde{\Phi}^\lambda$ is bounded because of $|\lambda(p)|_p = 1$);

(iii) in the general case (but assuming that $\lambda(p) \neq 0$) the holomorphic functions in (i) belong to the type $o(\log(x_p^h))$ with $h = [2\mathrm{ord}_p\lambda(p)]+1$ and they can be represented as the Mellin transform of the h-admissible measure $\tilde{\mu}^\lambda_{f_1\otimes f_2\otimes f_3}$ (in the sense of Amice-Vélu);

(iv) if $h = [2\mathrm{ord}_p\lambda] + 1 \le k-2$ then the function $\mathcal{D}_{(p)}$ is uniquely determined by the above conditions (i). ▮

A Nearly-holomorphic Siegel-Eisenstein series

A.1 Fourier expansions of Siegel-Eisenstein series

In this section χ denotes a Dirichlet character modulo an *arbitrary integer* N (not to be confused with N in the Introduction). We recall some standard facts about the Fourier expansions of the Siegel-Eisenstein series defined by:

$$\begin{aligned} E(\mathcal{Z}, s; k, \chi, N) &= E(\mathcal{Z}, s) \qquad\qquad (A.1)\\ &= \det(y)^s \sum_{\gamma \in P\cap\Gamma\backslash\Gamma} \chi(\det(d_\gamma)) j(\gamma, \mathcal{Z})^{-k} |j(\gamma, \mathcal{Z})|^{-2s}, \end{aligned}$$

for $k + 2\mathrm{Re}(s) > m + 1$, $s \in \mathbb{C}$, $k \in \mathbb{Z}$, and by analytic continuation over s for other values of $s \in \mathbb{C}$ (see [Sh83]). It is assumed in the identity (A.1) that $N > 1$, χ is a Dirichlet character mod N (not necessarily primitive, e.g. trivial modulo $N > 1$), and

$$\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in \Gamma = \Gamma_0^m(N) \subset \Gamma^m = \mathrm{Sp}(m, \mathbb{Z}).$$

Recall an explicit computation of the Fourier expansion of the series

$$E^\star(\mathcal{Z}, s) = E^\star(\mathcal{Z}, s; k, \chi, N) := E(-\mathcal{Z}^{-1}, s) \det(\mathcal{Z})^{-k}, \qquad (A.2)$$

obtained from (A.1) by applying the involution

$$J_m = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m \end{pmatrix}.$$

Note that for $k > m + 1$ and $N = 1$ both series coincide and were studied by Siegel:

$$E(\mathcal{Z}) = E_k^m(\mathcal{Z}) = E(\mathcal{Z}, 0) = E^\star(\mathcal{Z}, 0).$$

The detailed study of the series $E^\star(\mathcal{Z}, s; k, \chi, N)$ was made by G. Shimura [Sh83] and P. Feit ([Fei86], §10).

On the other hand, it is convenient to use the following notation. Let ϕ be a Dirichlet character mod $Q > 1$ and consider the Eisenstein series of degree $m \geq 1$

$$\begin{aligned} F_{\alpha,\beta}(\mathcal{Z}, Q, \phi) &:= \det(y)^\beta \sum_{c,d} \phi(\det c) \det(c\mathcal{Z} + d)^{-\alpha,-\beta} \qquad (A.3)\\ &= \det(y)^\beta \sum_{c,d} \phi(\det c) \det(c\mathcal{Z} + d)^{-\alpha} \det(c\overline{\mathcal{Z}} + d)^{-\beta} \\ &= \det(y)^\beta \sum_{c,d} \phi(\det c) \det(c\mathcal{Z} + d)^{\beta-\alpha} |\det(c\mathcal{Z} + d)|^{-2\beta} \qquad (A.4) \end{aligned}$$

where (c, d) runs over all “non-associated coprime symmetric pairs” with $\det(c)$ coprime to Q. A more conceptual description would be to sum over

$\mathcal{T}^m(Q)_\infty\backslash\mathcal{T}^m(Q)$, where

$$\begin{aligned}
&\mathcal{T}^m(Q) = \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{Sp}(m,\mathbb{Z})\middle| A \equiv 0 \bmod Q\right\} = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}\Gamma_0^m(Q)\\
&\mathcal{T}^m(Q)_\infty = \left(\begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}\Gamma_0^m(Q)\begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}^{-1}\right)_\infty\\
&\quad\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{Sp}(m,\mathbb{Z})\middle| c = 0, b \equiv 0 \bmod Q\right\} \subset \Gamma^{m,0}(Q) \subset \mathrm{Sp}(m,\mathbb{Z}),
\end{aligned}$$

where $\Gamma^{m,0}(Q) = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}\Gamma_0^m(Q)\begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}^{-1} \subset \mathrm{Sp}(m,\mathbb{Z})$ is the stabilizer of $\mathcal{M} = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}\Gamma_0^m(Q)$, and more generally, for any set $\mathcal{M} \subset \mathrm{Sp}(m,\mathbb{Z})$ of symplectic matrices we denote by $\mathcal{M}_\infty$ the set of those matrices $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{Sp}(m,\mathbb{Z})$ satisfying the conditions $c = 0$ and $\gamma\mathcal{M} \subset \mathcal{M}$.

Action of $\sigma \in \mathrm{Sp}(m,\mathbb{Z})$ on the Eisenstein series

Note that for any $\sigma \in \mathrm{Sp}(m,\mathbb{Z})$ one has

$$\begin{aligned}
E(\mathcal{Z}, s; k, \chi, N)|_k\sigma &= \sum_{\gamma\in\Gamma_0^m(N)_\infty\backslash\Gamma_0^m(N)} \phi(\det d_\gamma)(1|_k\gamma\sigma)(\mathcal{Z})(\mathrm{Im}\,(\gamma\sigma(\mathcal{Z}))^s\\
&= \det(y)^s \sum_{\gamma\in\Gamma_0^m(N)_\infty\backslash\Gamma_0^m(N)} \phi(\det d_\gamma) j(\gamma\sigma, \mathcal{Z})^{-k}|j(\gamma\sigma,\mathcal{Z})|^{-2s}\\
&= \det(y)^s \sum_{\tilde\gamma\in(\Gamma_0^m(N))_\infty\backslash\Gamma_0^m(N)\sigma} \phi(\det d_{\sigma^{-1}\tilde\gamma}) j(\tilde\gamma, \mathcal{Z})^{-k}|j(\tilde\gamma,\mathcal{Z})|^{-2s},
\end{aligned}$$

by writing $\tilde\gamma = \sigma\gamma$, $\sigma^{-1}\tilde\gamma = \gamma$: $P\gamma_1 = P\gamma_2 \iff P\tilde\gamma_1 = P\tilde\gamma_2$.

In particular, for $\sigma = J_m = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix}$ one has $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) J_m = \left(\begin{smallmatrix} b & -a \\ d & -c\end{smallmatrix}\right) \in \Gamma_0^m(N)J_m$, hence

$$\begin{aligned}
&E(\mathcal{Z}, s; k, \chi, N)|\begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m\end{pmatrix} = E^\star(\mathcal{Z}, s; k, \chi, N)\\
&= \det(y)^s \sum_{\left(\begin{smallmatrix} b & -a \\ d & -c\end{smallmatrix}\right)\in(\Gamma_0^m(N))_\infty\backslash\Gamma_0^m(N)\sigma} \chi(\det d)\det(d\mathcal{Z} - c)^{-k}|\det(d\mathcal{Z} - c)|^{-2s}.
\end{aligned}$$

Notice that $J_m(N)\Gamma_0^m(N) = \Gamma_0^m(N)J_m(N)$, where $J_m(N) = \begin{pmatrix} 0_m & -1_m \\ N\cdot 1_m & 0_m\end{pmatrix}$, and

$$J_m(N)\begin{pmatrix} a\ b \\ c\ d\end{pmatrix} = \begin{pmatrix} -c\ -d \\ Na\ Nb\end{pmatrix} = \begin{pmatrix} a_1\ b_1 \\ c_1\ d_1\end{pmatrix} J_m(N) = \begin{pmatrix} Nb_1\ -a_1 \\ Nd_1\ -c_1\end{pmatrix}.$$

Therefore $(Nd_1, -c_1) = (Na, Nb)$, and (a, b) runs over all "non-associated coprime symmetric pairs" with $\det(a)$ coprime to N. We may therefore write $(Nd_1, -c_1) = (Na, Nb)$, and

$$\begin{aligned} & E^\star(N\mathcal{Z}, s; k, \chi, N) && \text{(A.5)} \\ & = \det(Ny)^s \sum_{\left(\begin{smallmatrix} b_1 & -a_1 \\ d_1 & -c_1 \end{smallmatrix}\right) \in (\Gamma_0^m(N))_\infty \backslash \Gamma_0^m(N)\sigma} \chi(\det d_1) \det(d_1 N\mathcal{Z} - c_1)^{-k} |\det(d_1 N\mathcal{Z} - c_1)|^{-2s} \\ & = N^{-m(k+s)} \det(y)^s \sum_{a,b} \chi(\det a) \det(a\mathcal{Z} + b)^{-k-s,-s} && \text{(A.6)} \\ & = N^{-m(k+s)} F_{k+s,s}(\mathcal{Z}, N, \chi) && \text{(A.7)} \end{aligned}$$

A.2 Arithmetical variables of nearly-holomorphic Siegel modular forms and differential operators

Consider a commutative ring A, the formal variables $q = (q_{i,j})_{i,j=1,\dots,m}$, $R = (R_{i,j})_{i,j=1,\dots,m}$, and the ring of *formal arithmetical Fourier series*

$$A[\![q^{B_m}]\!][R_{i,j}] = \left\{ f = \sum_{\mathcal{T} \in B_m} a(\mathcal{T}, R) q^{\mathcal{T}} \;\middle|\; a(\mathcal{T}, R) \in A[R_{i,j}] \right\} \tag{A.8}$$

using the semi-group

$$B_m = \left\{ \mathcal{T} = (\mathcal{T}_{ij}) \in \mathrm{M}_m(\mathbb{R}) \;\mid\; \mathcal{T} = {}^t\mathcal{T}, \mathcal{T} \geq 0, \mathcal{T}_{ij}, 2\mathcal{T}_{ii} \in \mathbb{Z} \right\}$$

and the symbols

$$q^{\mathcal{T}} = \prod_{i=1}^m q_{ii}^{\mathcal{T}_{ii}} \prod_{i<j} q_{ij}^{2\mathcal{T}_{ij}} \subset A[\![q_{11}, \dots, q_{mm}]\!][q_{ij}, q_{ij}^{-1}]_{i,j=1,\cdots,m}$$

(over the complex numbers this notation corresponds to $q^{\mathcal{T}} = \exp(2\pi i \mathrm{tr}(\mathcal{T}\mathcal{Z}))$, $R = (4\pi \mathrm{Im}(\mathcal{Z}))^{-1}$).

The formal Fourier expansion of a nearly-holomorphic Siegel modular form f with coefficients in A is an element of $A[\![q^{B_m}]\!][R_{i,j}]$. Let

$$\mathcal{M}_k^m(N, \psi) \subset \tilde{\mathcal{M}}_k^m(N, \psi) \subset \mathcal{M}_k^m(N, \psi)^\infty$$

denote the complex vector spaces of holomorphic, nearly-holomorphic, and $\mathcal{C}^\infty$-Siegel modular forms of weight k and character ψ for $\Gamma_0^m(N)$, see [ShiAr], [CourPa] so that $\mathcal{M}_k^m(N, \psi) \subset \mathbb{C}[\![q^{B_m}]\!]$, $\tilde{\mathcal{M}}_k^m(N, \psi) \subset \mathbb{C}[\![q^{B_m}]\!][R_{i,j}]$, and $\mathcal{M}_k^m(N, \psi)^\infty \subset \mathcal{C}^\infty(\mathbb{H}_m)$.

A.3 Formal Fourier expansions of nearly-holomorphic Siegel-Eisenstein series

In the Siegel modular case $\Gamma^m = \mathrm{Sp}_{2m}(\mathbb{Z}) \supset \Gamma_0^m(N)$ the series

$$\begin{aligned} & E(\mathcal{Z}, s; k, \chi, N) = E(\mathcal{Z}, s) \qquad\qquad (\mathrm{A}.9)\\ & = \det(y)^s \sum_{\gamma \in P\cap\Gamma\backslash\Gamma} \chi(\det(d_\gamma)) j(\gamma, \mathcal{Z})^{-k} |j(\gamma,\mathcal{Z})|^{-2s} \in \mathcal{M}_k^\infty(\Gamma_0(N), \bar{\chi}) \end{aligned}$$

is absolutely convergent for $k + 2\mathrm{Re}(s) > m+1$, but can be continued to all $s \in \mathbb{C}$. However, for $N > 1$, the Fourier expansion is known only for *the involuted series* $E(\cdot, s)|W(N)$, where $W(N) = \begin{pmatrix} 0_m & -1_m \\ N\cdot 1_m & 0_m \end{pmatrix}$, and for some critical values $s \in \mathbb{Z}$ (for $N = 1$ both series coincide). Here $\mathcal{Z} \in \mathbb{H}_m$ is in the Siegel upper half-space:

$$\mathbb{H}_m = \left\{ \mathcal{Z} = {}^t\mathcal{Z} \in \mathrm{M}_m(\mathbb{C}) | \operatorname{Im} \mathcal{Z} > 0 \right\}, \quad \text{and} \quad P = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in Sp_{2m}(\mathbb{R}) \right\}$$

is the Siegel parabolic subgroup.

Example A.1 (Involuted Siegel-Eisenstein series) *Let χ be a Dirichlet character modulo N. Recall that by (A.5)*

$$\begin{aligned} & E^\star(N\mathcal{Z}, s; k, \chi, N) = N^{-m(k+s)} F_{k+s,s}(\mathcal{Z}, N, \chi) \qquad\qquad (\mathrm{A}.10)\\ & = N^{-m(k+s)} \det(y)^s \sum_{a,b} \chi(\det a) \det(a\mathcal{Z} + b)^{-k-s,-s}, \ \textit{where} \end{aligned}$$

$$E^\star(N\mathcal{Z}, s) = E(-(N\mathcal{Z})^{-1}, s) \det(N\mathcal{Z})^{-k} = N^{-km/2} E|W(N), \qquad (\mathrm{A}.11)$$

$$\begin{aligned} & G^\star(\mathcal{Z}, s) = G^*(\mathcal{Z}, s; k, \chi, N) = N^{m(k+s)} E^*(N\mathcal{Z}, s)\cdot \qquad\qquad (\mathrm{A}.12)\\ & \cdot \tilde{\Gamma}(k,s) L_N(k+2s, \chi) \left(\prod_{i=1}^{[m/2]} L_N(2k+4s-2i, \chi^2) \right) \end{aligned}$$

$\kappa = (m+1)/2$, and for m odd the Γ-factor has the form:

$$\begin{aligned} \tilde{\Gamma}(k,s) &= i^{mk} 2^{-m(k+1)} \pi^{-m(s+k)} \Gamma_m(k+s), \\ \textit{where } \Gamma_m(s) &= \pi^{m(m-1)/4} \prod_{j=0}^{m-1} \Gamma(s - (j/2))). \end{aligned}$$

In order to describe the formal Fourier expansions explicitly let us consider the Maass differential operator Δ_m, acting on $\mathcal{C}^\infty$-functions over $V \otimes \mathbb{C}$ of degree m, which is defined by the equality:

$$\Delta_m = \det(\partial_{ij}), \qquad \partial_{ij} = 2^{-1}(1 + \delta_{ij})\partial/\partial_{ij}. \qquad (\mathrm{A}.13)$$

For an integer $n \geq 0$ and a complex number β consider the polynomial

$$R_m(\mathcal{Z}; n, \beta) = (-1)^{mn} e^{\mathrm{tr}(\mathcal{Z})} \det(\mathcal{Z})^{n+\beta} \Delta_m^n \left[e^{-\mathrm{tr}(\mathcal{Z})} \det(\mathcal{Z})^{-\beta} \right], \tag{A.14}$$

with $\mathcal{Z} \in V \otimes \mathbb{C}$, where the exponentiation is well defined by

$$\det(y)^\beta = \exp\left(\beta \log[\det(y)]\right),$$

for $\det(y) > 0$, $y \in Y \otimes \mathbb{C}$. According to definition (A.14) the degree of the polynomial $R_m(\mathcal{Z}; n, \beta)$ is equal to mn and the term of the highest degree coincides with $\det(\mathcal{Z})^n$. We have also that for $\beta \in \mathbb{Q}$ the polynomial $R_m(\mathcal{Z}; n, \beta)$ has rational coefficients.

Theorem A.2 *Let m be an odd integer such that $2k > m$, and $N > 1$ be an integer, then:*
For an integer s such that $s = -r \leq 0$, $0 \leq r \leq k - \kappa$, there is the following Fourier expansion

$$G^\star(\mathcal{Z}, -r) = G^\star(\mathcal{Z}, -r; k, \chi, N) = \sum_{A_m \ni \mathcal{T} \geq 0} b^\star(\mathcal{T}, y, -r) q^{\mathcal{T}} = \sum_{A_m \ni \mathcal{T} \geq 0} a(\mathcal{T}, R) q^{\mathcal{T}}, \tag{A.15}$$

where for $s > (m + 2 - 2k)/4$ in (A.15) the only non-zero terms occur for positive definite $\mathcal{T} > 0$, and for all $s = -r$ with $0 \leq r \leq k - \kappa$, and for all $\mathcal{T} > 0$, $\mathcal{T} \in A_m$, where

$$\begin{aligned} b^\star(\mathcal{T}, y, -r) &= a(\mathcal{T}, R) = W^\star(y, \mathcal{T}, -r) M(\mathcal{T}, \chi, k - 2r), \qquad (A.16)\\ W^\star(y, \mathcal{T}, -r) &= 2^{-m\kappa} \det(\mathcal{T})^{k-2r-\kappa} Q(R, \mathcal{T}; k - 2r, r). \end{aligned}$$

Here $a(\mathcal{T}, R) = a(\mathcal{T}, R; r, N, \chi)$ is a homogeneous polynomial with rational coefficients in the variables R_{ij} and $\mathcal{T}_{ij}$, and

$$M(\mathcal{T}, k - 2r, \chi) = \prod_{\ell | \det(2\mathcal{T})} M_\ell(\mathcal{T}, \chi(\ell) \ell^{-k+2r}) \tag{A.17}$$

is a finite Euler product, in which $M_\ell(\mathcal{T}, x) \in \mathbb{Z}[x]$; we use the notation $q^{\mathcal{T}} = \exp(2\pi i \mathrm{tr}(\mathcal{T}\mathcal{Z}))$, $R = (4\pi \mathrm{Im}(\mathcal{Z}))^{-1}$ as above, and polynomials $Q(R, \mathcal{T}; k - 2r, r)$ are given by (3.1).

Proof: see [Sh83], [Fei86], Theorem 2.14 and formulas (2.137) in [CourPa]. The use of definitions gives

$$W^\star(y, \mathcal{T}, -r) = 2^{-m\kappa} \det(\mathcal{T})^{k-2r-\kappa} \det(4\pi y)^{-r} R_m(4\pi \mathcal{T} y; r, \kappa - k + r)$$

where $R_m(y; n, \beta)$ is defined by (A.14). Moreover, let us use the polynomials (3.1):

$$Q(R, \mathcal{T}; k - 2r, r) \det(\mathcal{T})^{-r} = \det(4\pi \mathcal{T} y)^{-r} R_m(4\pi \mathcal{T} y; r, \kappa - k + r),$$

it follows

$$\begin{aligned} W^\star(y, \mathcal{T}, -r) =& 2^{-m\kappa} \det(\mathcal{T})^{k-2r-\kappa} \det(4\pi y)^{-r} R_m(4\pi \mathcal{T} y; r, \kappa - k + r)\\ &= 2^{-m\kappa} \det(\mathcal{T})^{k-2r-\kappa} Q(R, \mathcal{T}; k - 2r, r). \quad \blacksquare \end{aligned}$$

B An integral representation for the triple product

B.1 Summary of analytic results

In this section we use the following data :

- Three equal weights $k = k_1 = k_2 = k_3$
- Three Dirichlet characters modN_j with $\psi_j(-1) = (-1)^k$
- Three cusp forms $\tilde{f}_j(z) = \sum_{n=1}^{\infty} \tilde{a}_{n,j} e(nz) \in \mathcal{S}_k(\tilde{N}_j, \psi_j)$, $(j = 1, 2, 3)$ with $N_j | \tilde{N}_j$, assumed to be eigenforms for all Hecke operators T_q, with q prime to N. In our construction we use as $\tilde{f}_j$ some "easy transforms" of primitive cusp forms $f_j \in \mathcal{S}_k(N_j, \psi_j)$ in the Introduction, so that they have the same eigenvalues for all Hecke operators T_q, for q prime to N. For example, $\tilde{f}_j$ could be chosen as eigenfunctions $\tilde{f}_j = f_j^0$ of the conjugate Atkin's operator U_p^* given by (0.10), in this case we denote by $f_{j,0}$ the corresponding eigenfunctions of U_p.
- Assume that $\tilde{N} | Np^v$, where $\tilde{N} := \mathrm{LCM}\{\tilde{N}_1, \tilde{N}_2, \tilde{N}_3\}$
- Consider a non necessary primitive Dirichlet character χ mod Np^v, and the Dirichlet characters as in (0.12).

Using the notation $z_j = x_j + iy_j \in \mathbb{H}$, one associates to this data the following function

$$\mathcal{E}(z_1, z_2, z_3) = \mathcal{E}(z_1, z_2, z_3; s, k, \boldsymbol{\psi}, \chi_1, \chi_2, \chi_3) := \tag{B.1}$$

$$i^{3k} 2^{-3(k+1)-2s-2k+2} \pi^{3(s+k)+2} \Gamma(2s + 2k - 1)\Gamma(s + k - 1) \times$$

$$\times L^{(Np)}(k + 2s, \boldsymbol{\psi}) L^{(Np)}(4s + 2k - 2, \boldsymbol{\psi}^2) \sum_{\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23} \bmod Np^v} \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23})$$

$$F_{k+s,s}(\star, N^2p^{2v}, \boldsymbol{\psi}) \Bigg| \begin{pmatrix} 1 & 0 & 0 & 0 & \frac{\varepsilon_{12}}{Np^v} & \frac{\varepsilon_{13}}{Np^v} \\ & 1 & 0 & \frac{\varepsilon_{12}}{Np^v} & 0 & \frac{\varepsilon_{23}}{Np^v} \\ & & 1 & \frac{\varepsilon_{13}}{Np^v} & \frac{\varepsilon_{23}}{Np^v} & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix} (z_1, z_2, z_3) y_1^s y_2^s y_3^s.$$

Note that the product of the normalizing Gamma-factor and of the two Dirichlet L-functions come from the definitions (A.11) and (A.10) of the Siegel-Eisenstein series.

B.2 Fourier expansion of the Eisenstein series (B.1)

Consider again the Dirichlet characters (0.12), and the corresponding function (B.1) of level Np^v.
We wish to express the series (B.1), evaluated at $s = -r$, through the series (1.2) in the case of Np-complete conductors.

Proposition B.1 *For* $F(\mathcal{Z}) = \sum_{\mathcal{T}} a(\mathcal{T}, R) q^{\mathcal{T}}$ *one has* $F^{\phi}(\mathcal{Z}) = \sum_{\mathcal{T}} g_t(\phi, \mathcal{T}) a(\mathcal{T}, R) q^{\mathcal{T}}$, *where* $\boldsymbol{\varepsilon} = \begin{pmatrix} 0 & \varepsilon_{12} & \varepsilon_{13} \\ \varepsilon_{12} & 0 & \varepsilon_{23} \\ \varepsilon_{13} & \varepsilon_{23} & 0 \end{pmatrix}$, $\phi(\boldsymbol{\varepsilon}) = \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23})$, $\mathcal{T}$ *denotes the (half integral) block matrix and*

$$g_t(\phi, \mathcal{T}) = \sum_{\boldsymbol{\varepsilon} \in S_{N,p}/Np^v S_{N,p}} \phi(\boldsymbol{\varepsilon}) \exp(2\pi i \mathrm{tr}(\frac{1}{Np^v} \mathcal{T} \boldsymbol{\varepsilon})), \text{ where } \phi(\boldsymbol{\varepsilon}) = \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23}).$$

Proof. Indeed,
$F|t_{\boldsymbol{\varepsilon}, Np^v} = \sum_{\mathcal{T}} a(\mathcal{T}, R) q^{\mathcal{T}} |t_{\boldsymbol{\varepsilon}, Np^v} = \sum_{\mathcal{T}} \exp(2\pi i \mathrm{tr}(\boldsymbol{\varepsilon}\mathcal{T})/Np^v) a(\mathcal{T}, R) q^{\mathcal{T}}$, and it suffices to notice again that

$$\mathrm{tr}(\boldsymbol{\varepsilon}\mathcal{T}) = \mathrm{tr}\left(\begin{pmatrix} 0 & \varepsilon_{12} & \varepsilon_{13} \\ \varepsilon_{12} & 0 & \varepsilon_{23} \\ \varepsilon_{13} & \varepsilon_{23} & 0 \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{12} & t_{22} & t_{23} \\ t_{13} & t_{23} & t_{33} \end{pmatrix}\right) = 2(\varepsilon_{12} t_{12} + \varepsilon_{13} t_{13} + \varepsilon_{23} t_{23}).$$

∎

Using this formula for $F = G^{\star}(\mathcal{Z}, s; k - 2r, (Np^v)^2, \boldsymbol{\psi})$ at $s = -r$ (see (A.3)), gives:

$$\mathcal{E}(z_1, z_2, z_3; -r, k, \boldsymbol{\psi}, \chi_1, \chi_2, \chi_3) = \tag{B.2}$$

$$\sum_{\boldsymbol{\varepsilon} \in S/Np^v S} \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23}) G^{\star}(\mathcal{Z}, -r; k - 2r, (Np^v)^2, \boldsymbol{\psi})|t_{\boldsymbol{\varepsilon}, Np^v}(z_1, z_2, z_3)$$

$$= \left(\sum_{\mathcal{T}} \sum_{\boldsymbol{\varepsilon} \in S/Np^v S} \chi_1(\varepsilon_{12})\chi_2(\varepsilon_{13})\chi_3(\varepsilon_{23}) \exp(2\pi i \mathrm{tr}(\boldsymbol{\varepsilon}\mathcal{T})/Np^v) a(\mathcal{T}, R) q^{\mathcal{T}}\right) \circ \mathrm{diag}$$

then the sum over $\boldsymbol{\varepsilon} \in S/Np^v S$ transforms simply to the product

$$G_{Np^v}(\chi_1, 2t_{12}) G_{Np^v}(\chi_2, 2t_{13}) G_{Np^v}(\chi_3, 2t_{23}),$$

which is easily evaluated by the general formula for a generalized Gauss sum $G_N(\chi, c) = \sum_{b \bmod N} \chi(b) e(bcN^{-1})$. This last sum admits the following known expression in terms of the usual Gauss sums (see for example [PaTV], Section

2, (2.20)): let χ_0 denote the primitive Dirichlet character modulo N_0 associated with χ, $N_1 = NN_0^{-1}$, then

$$G_N(\chi, c) = G(\chi_0)N_1 \sum_{d|N_1} \mu(d)\chi_0(d)d^{-1}\delta\Big(\frac{c}{N_1d^{-1}}\Big)\bar\chi_0\Big(\frac{c}{N_1d^{-1}}\Big).$$

Writing $\chi_{0,j}$ for the primitive Dirichlet character modulo $N_{0,j}$ associated with χ_j mod Np^v, and using the notation $Np^v = N_{0,j}N_{1,j}$, gives

$$\begin{aligned}
&G_{Np^v}(\chi_1, 2t_{12})\\
&= G(\chi_{0,1})N_{1,1} \sum_{d_1|N_{1,1}} \mu(d_1)\chi_{0,1}(d_1)d_1^{-1}\delta\Big(\frac{2t_{12}}{N_{1,1}d_1^{-1}}\Big)\bar\chi_{0,1}\Big(\frac{2t_{12}}{N_{1,1}d_1^{-1}}\Big)\\
&G_{Np^v}(\chi_2, 2t_{13})\\
&= G(\chi_{0,2})N_{1,2} \sum_{d_2|N_{1,2}} \mu(d_2)\chi_{0,2}(d_2)d_2^{-1}\delta\Big(\frac{2t_{12}}{N_{1,2}d_2^{-1}}\Big)\bar\chi_{0,2}\Big(\frac{2t_{13}}{N_{1,2}d_2^{-1}}\Big)\\
&G_{Np^v}(\chi_3, 2t_{23})\\
&= G(\chi_{0,3})N_{1,3} \sum_{d_3|N_{1,3}} \mu(d_3)\chi_{0,3}(d_3)d_3^{-1}\delta\Big(\frac{2t_{23}}{N_{1,3}d_3^{-1}}\Big)\bar\chi_{0,3}\Big(\frac{2t_{23}}{N_{1,3}d_3^{-1}}\Big)
\end{aligned}$$

Let us take the product of these expressions using the notation

$$\begin{aligned}
2t'_{12} &= \frac{2t_{12}}{N_{1,1}/d_1}(\mathrm{mod} N_{0,1}d_1),\\
2t'_{13} &= \frac{2t_{13}}{N_{1,2}/d_2}(\mathrm{mod} N_{0,2}d_2),\\
2t'_{23} &= \frac{2t_{23}}{N_{1,3}/d_3}(\mathrm{mod} N_{0,3}d_3)
\end{aligned}$$

It follows

$$\begin{aligned}
&G_{Np^v}(\chi_1, 2t_{12})G_{Np^v}(\chi_2, 2t_{13})G_{Np^v}(\chi_3, 2t_{23})\\
&= N_{1,1}N_{1,2}N_{1,3} \sum_{\substack{d_1|N_{1,1}\\ d_2|N_{1,2}\\ d_3|N_{1,3}}} \mu(d_1)\mu(d_2)\mu(d_3)\chi_{0,1}(d_1)\chi_{0,2}(d_2)\chi_{0,3}(d_3)(d_1d_2d_3)^{-1}\\
&G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3})\bar\chi_{0,1}(2t'_{12})\bar\chi_{0,2}(2t'_{13})\bar\chi_{0,3}(2t'_{23}).
\end{aligned}$$

The formula (B.3) transforms to

$$\begin{aligned}
&\mathcal{E}(z_1, z_2, z_3; -r, k, \boldsymbol{\psi}, \chi_1, \chi_2, \chi_3) \qquad\qquad \text{(B.3)}\\
&= \Bigg(\sum_{\mathcal{T}} G_{Np^v}(\chi_1, 2t_{12})G_{Np^v}(\chi_2, 2t_{13})G_{Np^v}(\chi_3, 2t_{23})a(\mathcal{T}, R)q^{\mathcal{T}}\Bigg) \circ \mathrm{diag}
\end{aligned}$$

$$= N_{1,1}N_{1,2}N_{1,3} \sum_{\substack{d_1|N_{1,1}\\ d_2|N_{1,2}\\ d_3|N_{1,3}}} \mu(d_1)\mu(d_2)\mu(d_3)\chi_{0,1}(d_1)\chi_{0,2}(d_2)\chi_{0,3}(d_3)(d_1d_2d_3)^{-1}$$

$$G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3}) \sum_{\substack{\mathcal{T}:t_{12}=d_1t'_{12},\\ t_{13}=d_2t'_{13},t_{23}=d_3t'_{23},}} \bar\chi_{0,1}(2t'_{12})\bar\chi_{0,2}(2t'_{13})\bar\chi_{0,3}(2t'_{23})a(\mathcal{T},R)q_1^{t_{11}}q_2^{t_{22}}q_3^{t_{33}}.$$

Later on we impose the condition that the conductors of $\chi_{0,1}, \chi_{0,2}, \chi_{0,3}$ are complete (i.e. have the same prime divisors as those of Np), when $\chi_{0,j}(d_j) = 0$ unless all $d_j = 1$, when $\chi_{0,j}(d_j) = 1$. In this *complete* case $\chi_{0,j}(n) = \chi_j(n)$ for all $n \in \mathbb{Z}$, hence the equality (B.3) simplifies to the following:

$$\mathcal{E}(z_1, z_2, z_3; -r, k, \boldsymbol{\psi}, \chi_1, \chi_2, \chi_3) \tag{B.4}$$

$$= \left(\sum_{\mathcal{T}} G_{Np^v}(\chi_1, 2t_{12})G_{Np^v}(\chi_2, 2t_{13})G_{Np^v}(\chi_3, 2t_{23})a(\mathcal{T}, R)q^{\mathcal{T}}\right) \circ \mathrm{diag}$$

$$= N_{1,1}N_{1,2}N_{1,3}G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3})$$

$$\left(\sum_{\mathcal{T}} \bar\chi_1(2t_{12})\bar\chi_2(2t_{13})\bar\chi_3(2t_{23})a(\mathcal{T}, R)q^{\mathcal{T}}\right) \circ \mathrm{diag}$$

$$= N_{1,1}N_{1,2}N_{1,3}(\bar\chi_1\bar\chi_2\bar\chi_3)(2)G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3})$$

$$\left(\sum_{\mathcal{T}} a(\mathcal{T}, R)\bar\chi_1(t_{12})\bar\chi_2(t_{13})\bar\chi_3(t_{23})q^{\mathcal{T}}\right) \circ \mathrm{diag}\,.$$

Thus we have expressed the series (B.1) through the series (1.2) in the case of Np-complete conductors:

$$\mathcal{E}(z_1, z_2, z_3; -r, k, Np^v, \boldsymbol{\psi}, \chi_1, \chi_2, \chi_3) \tag{B.5}$$

$$= N_{1,1}N_{1,2}N_{1,3}(\bar\chi_1\bar\chi_2\bar\chi_3)(2)G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3})F_{\chi,r}^{\bar\chi_1,\bar\chi_2,\bar\chi_3} \circ \mathrm{diag}$$

$$= N_{1,1}N_{1,2}N_{1,3}(\bar\chi_1\bar\chi_2\bar\chi_3)(2)G(\chi_{0,1})G(\chi_{0,2})G(\chi_{0,3})2^{-r}\Phi_r(\chi).$$

B.3 The integral representation

Consider three auxilliary modular forms as in (0.16):

$$\tilde f_j(z) = \sum_{n=1}^{\infty} \tilde a_{n,j}e(nz) \in S_k(\Gamma_0(N_jp^{\nu_j}), \psi_j) \quad (1 \le i \le 3)$$

with the same eigenvalues, as those of (0.1), for all Hecke operators T_q, with q prime to Np.

Theorem B.2 *Under the assumptions and notations as in section B.1, the following integral representation holds:*

$$\iiint_{(\Gamma_0(N^2p^{2v})\backslash\mathbb{H})^3} \overline{\tilde{f}_1(z_1)\tilde{f}_2(z_2)\tilde{f}_3(z_3)}\mathcal{E}(z_1,z_2,z_3;s,k,N^2p^{2v},\boldsymbol{\psi},\chi_1,\chi_2,\chi_3)) \times$$

$$\prod_j y_j^k(\frac{dx_jdy_j}{y_j^2})$$

$$= i^{-3k+3}(2\pi)^{-4s}\Gamma(s+2k-2)\Gamma(s+k-1)^3$$

$$(Np^v)^{k+2s}\frac{N^2p^{2v}\varphi(N^2p^{2v})\varphi(Np^v)}{[\Gamma_0(N^2p^{2v}):\Gamma(N^2p^{2v})]^3}\times\mathfrak{L}_{Np}(s)$$

$$L^{(Np)}(f_1^\rho\otimes f_2^\rho\otimes f_3^\rho,s+2k-2,\psi_1\psi_2\chi_1),$$

where

$$(2\pi)^{-4s}\Gamma(s+2k-2)\Gamma(s+k-1)^3 = 2^{-4}\Gamma_{\mathbb{C}}(s+2k-2)\Gamma_{\mathbb{C}}(s+k-1)^3,$$
$$\Gamma_{\mathbb{C}}(s)=2(2\pi)^{-s}\Gamma(s)$$

is the motivic Gamma-factor,

$$\mathfrak{L}_{Np}(s)=\mathfrak{L}_{Np}(s;\tilde{f}_1\otimes\tilde{f}_2\otimes\tilde{f}_3):=\sum_{n|(Np)^\infty}G_{Np^v}(\overline{\psi_1\psi_2\chi_1},2n)\frac{\tilde{a}_{n,1}\tilde{a}_{n,2}\tilde{a}_{n,3}}{n^{2s+2k-2}}. \tag{B.6}$$

Remark. *In the special case when the character $\psi_1\psi_2\chi$ has Np-complete conductor, or if it is primitive* mod Np^v*, and $\tilde{f}_1,\tilde{f}_2,\tilde{f}_3$ are primitive normalized cusp eigenforms, one can show that $\mathfrak{L}_{Np}(s)=(\psi_1\psi_2\chi_1)(2)G(\overline{\psi_1\psi_2\chi_1})$.*

Theorem B.2 follows from a computation, similar to that in [BoeSP], Theorem 4.2, (triple product, no twisting character) and [Boe-Schm], Section 2 (standard L-function, with twisting character). Details will appear elsewhere.

Corollary B.3 *Under the notations and assumptions, for all critical values $s=2k-2-r$, $r=0,\cdots,k-2$ the following integral representation holds*

$$(2\pi)^{4r}\Gamma(-r+2k-2)\Gamma(-r+k-1)^3L^{(N)}(f_1^\rho\otimes f_2^\rho\otimes f_3^\rho,2k-2-r,\psi_1\psi_2\chi_1)$$

$$(Np^v)^{k-2r}\frac{N^2p^{2v}\varphi(N^2p^{2v})\varphi(Np^v)}{[\Gamma_0(N^2p^{2v}):\Gamma(N^2p^{2v})]^3}\times\mathfrak{L}_{Np}(s)$$

$$=\left\langle\tilde{f}_1\otimes\tilde{f}_2\otimes\tilde{f}_3,\mathcal{E}(z_1,z_2,z_3;-r,k,k,N^2p^{2v},\boldsymbol{\psi},\chi_1,\chi_2,\chi_3)\right\rangle_{T,N^2p^{2v}}. \quad \blacksquare$$

References

[Am-V] Amice, Y. and Vélu, J., *Distributions p-adiques associées aux séries de Hecke*, Journées Arithmétiques de Bordeaux (Conf. Univ. Bordeaux, 1974), Astérisque no. 24/25, Soc. Math. France, Paris 1975, 119 - 131.

[Boe1] Böcherer, S., *Über die Funktionalgleichung automorpher L–Funktionen zur Siegelscher Modulgruppe*, J. reine angew. Math. 362 (1985) 146–168.

[Boe2] Böcherer S., *Über die Fourier–Jacobi Entwickelung Siegelscher Eisensteinreihen. I.II.*, Math. Z. 183 (1983) 21-46; 189 (1985) 81–100.

[BHam] Böcherer, S., *Ein Rationalitätssatz für formale Heckereihen zur Siegelschen Modulgruppe.* Abh. Math. Sem. Univ. Hamburg 56, 35–47 (1986)

[Boe-Ha] Boecherer, S., Heim, B. *L-functions for $GSp_2 \times Gl_2$ of mixed weights.* Math. Z. 235, 11-51(2000).

[BSY] Böcherer, S., Satoh, T., and Yamazaki, T., *On the pullback of a differential operator and its application to vector valued Eisenstem series,* Comm. Math. Univ. S. Pauli, 41 (1992), 1-22.

[Boe-Schm] Böcherer, S., and Schmidt, C.-G., *p-adic measures attached to Siegel modular forms*, Ann. Inst. Fourier 50, N°5, 1375-1443 (2000).

[BoeSP] Böcherer, S. and Schulze-Pillot, R., *On the central critical value of the triple product L-function.* David, Sinnou (ed.), Number theory. Séminaire de Théorie des Nombres de Paris 1993–94. Cambridge: Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 235, 1-46 (1996).

[Co] Coates, J. *On p–adic L–functions.* Sem. Bourbaki, 40eme annee, 1987-88, n° 701, Asterisque (1989) 177–178.

[Co-PeRi] Coates, J. and Perrin-Riou, B., *On p-adic L-functions attached to motives over* $\mathbb{Q}$, Advanced Studies in Pure Math. 17, 23–54 (1989).

[Colm98] Colmez, P. *Fonctions L p-adiques*, Séminaire Bourbaki, exposé n° 851, novembre 1998.

[Colm03] Colmez, P. La conjecture de Birch et Swinnerton-Dyer p-adique. Séminaire Bourbaki, exposé n° 919, juin 2003.

[CourPa] Courtieu M., Panchishkin A.A., *Non-Archimedean L-Functions and Arithmetical Siegel Modular Forms*, Lecture Notes in Mathematics 1471, Springer-Verlag, 2004 (2nd augmented ed.)

[De69] Deligne P., *Formes modulaires et reprèsentations l-adiques*, Sem. Bourb. 1968/69 ,exp. no 335. Springer-Verlag, Lect. Notes in Math. N°179 (1971) 139 - 172.

[De79] Deligne P., *Valeurs de fonctions L et périodes d'intégrales*, Proc. Symp. Pure Math AMS 33 (part 2) (1979) 313–342.

[Fei86] Feit, P., *Poles and Residues of Eisenstein Series for Symplectic and Unitary Groups*, Memoir AMS 61 N°346 (1986), 89 p.

[Ga87] Garrett, P.B., *Decomposition of Eisenstein series: Rankin triple products*, Ann. of Math. 125 (1987), 209–235.

[GaHa] Garrett, P.B. and Harris, M., *Special values of triple product L–functions*, Amer. J. Math 115 (1993) 159–238.

[Go02] Gorsse, B., Carrés symétriques de formes modulaires et intégration p-adique. Mémoire de DEA de l'Institut Fourier, juin 2002.

[Go-Ro] Gorsse B., Robert G., Computing the Petersson product $\langle f^0, f_0\rangle$. Prépublication de l'Institut Fourier, N°654, (2004).

[Ha93] Harris, M., *Hodge–de Rham structures and periods of automorphic forms*, Proceedings of the Joint AMS Summer Conference on Motives, Seattle, July 20–August 2 1991, Seattle, Providence, R.I., 1993.

[Ha93] Harris, M., and Kudla, S., *The central critical value of a triple product L – functions*, Ann. Math. 133 (1991), 605–672.

[Hasse] Hasse, H., *Vorlesungen über Zahlentheorie.* Zweite neubearbeitete Auflage. Die Grundlehren der Mathematischen Wissenschaften, Band 59 Springer-Verlag, Berlin-New York 1964 xv+504 pp.

[Hi85] Hida, H., *A p-adic measure attached to the zeta functions associated with two elliptic cusp forms. I*, Invent. Math. 79 (1985) 159–195.

[Hi86] Hida, H., *Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. 85 (1986) 545–613.

[Hi90] Hida, H., *Le produit de Petersson et de Rankin p-adique*, Séminaire de Théorie des Nombres, Paris 1988–1989, 87–102, Progr. Math., 91, Birkhäuser Boston, Boston, MA, 1990.

[Hi93] Hida, H., *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts. 26 Cambridge: Cambridge University Press. ix, 386 p. (1993).

[JoH05] Jory–Hugue, F., *Unicité des h–mesures admissibles p-adiques données par des valeurs de fonctions L sur les caractères*, Prépublication de l'Institut Fourier (Grenoble), N°676, 1-33, 2005.

[Iw] Iwasawa, K., *Lectures on p–adic L–functions*, Ann. of Math. Studies, N°74. Princeton University Press, 1972.

[Ibu] Ibukiyama, T. *On differential operators on automorphic forms and invariant pluriharmonic polynomials*, Comm. Math. Univ. S. Pauli 48 (1999), 103-118.

[Ka76] Katz, N.M., *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. 104 (1976) 459–571

[Ka78] Katz, N.M., *p-adic L-functions for CM–fields*, Invent. Math. 48 (1978) 199–297.

[KiK] Kitagawa,Koji, *On standard p-adic L-functions of families of elliptic cusp forms*, Mazur, Barry (ed.) et al.: p-adic monodromy and the Birch and Swinnerton-Dyer conjecture. A workshop held August 12-16, 1991 in Boston, MA, USA. Providence, R: American Mathematical Society. Contemp. Math. 165, 81-110, 1994

[Ku-Le] Kubota T. and Leopoldt H.-W. , *Eine p-adische Theorie der Zetawerte*, J. reine angew. Math. 214/215 (1964) 328–339.

[La] Lang S., *Introduction to Modular Forms*, Springer Verlag, 1976.

[Man73] Manin, Yu.I., *Periods of cusp forms and p-adic Hecke series*, Mat. Sbornik 92 (1973) 378–401(in Russian); Math. USSR, Sb. 21(1973), 371-393 (1975) (English translation).

[Man74] Manin, Yu.I., *The values of p–adic Hecke series at integer points of the critical strip.* Mat. Sbornik 93 (1974) 621 - 626 (in Russian).

[Man76] Manin, Yu.I., *Non–Archimedean integration and p-adic L-functions of Jacquet – Langlands*, Uspekhi Mat. Nauk 31 (1976) 5–54 (in Russian); Russ. Math. Surv. 31, No.1, 5-57 (1976) (English translation).

[Man-Pa] Manin, Yu.I. and Panchishkin, A.A. , *Convolutions of Hecke series and their values at integral points*, Mat. Sbornik, 104 (1977) 617–651 (in Russian); Math. USSR, Sb. 33, 539-571 (1977) (English translation).

[MTT] Mazur, B., Tate, J. and Teitelbaum, J., *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. 84, 1-48 (1986).

[Miy] Miyake, Toshitsune, *Modular forms.* Transl. from the Japanese by Yoshitaka Maeda. Berlin etc.: Springer-Verlag. viii, 335 p. (1989).

[Or] Orloff T., *Special values and mixed weight triple products (with an Appendix by D.Blasius)*, Invent. Math. 90 (1987) 169–180.

[Pa94] Panchishkin, A.A., *Admissible Non-Archimedean standard zeta functions of Siegel modular forms*, Proceedings of the Joint AMS Summer Conference on Motives, Seattle, July 20–August 2 1991, Seattle, Providence, R.I., 1994, vol.2, 251 – 292.

[PaViet] Panchishkin, A. A. *Non-Archimedean Mellin transform and p-adic L-Functions*, Vietnam Journal of Mathematics, 1997, N3, 179–202.

[PaSE] Panchishkin, A.A., *On the Siegel–Eisenstein measure. Israel Journal of Mathematics*, Vol. 120, Part B(2000), 467–509.

[PaIAS] Panchishkin, A.A., *On p-adic integration in spaces of modular forms and its applications*, J. Math. Sci., New York 115, No.3, 2357-2377 (2003).

[PaMMJ] Panchishkin, A.A., *A new method of constructing p-adic L-functions associated with modular forms*, Moscow Mathematical Journal, 2 (2002), Number 2, 1-16.

[PaTV] Panchishkin, A.A., *Two variable p-adic L functions attached to eigenfamilies of positive slope*, Invent. Math. v. 154, N3 (2003), pp. 551 - 615.

[PaB1] Panchishkin, A.A., *The Maass–Shimura differential operators and congruences between arithmetical Siegel modular forms,* (accepted in Moscow Mathematical Journal in October 2005 (39 p.).

[PaB2] Panchishkin, A.A., *Admissible measures for standard L-functions and nearly holomorphic Siegel modular forms* , Preprint MPI 2002 - 42, 1-65.

[PaJTNB] Panchishkin A.A., *Sur une condition suffisante pour l'existence des mesures p-adiques admissibles*, Journal de Théorie des Nombres de Bordeaux, v. 15 (2003), pp. 1-24.

[PSRa] Piatetski–Shapiro, I.I., and Rallis, S., *Rankin triple L–functions*, Compositio Math. 64 (1987) 333–399.

[Puy] Puydt, J., *Valeurs spéciales de fonctions L de formes modulaires adéliques*, Thèse de Doctorat, Institut Fourier (Grenoble), 19 décembre 2003.

[Ran39] Rankin, R.A., *Contribution to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. I.II*, Proc. Camb. Phil. Soc 35 (1939) 351–372.

[Ran52] Rankin, R.A., *The scalar product of modular forms*, Proc. London math. Soc. 2 (3) (1952) 198-217.

[Ran90] Rankin, R.A., *The adjoint Hecke operator.* Automorphic functions and their applications, Int. Conf., Khabarovsk/USSR 1988, 163-166 (1990).

[Sa] Satoh,T., Some remarks on triple L-functions. Math.Ann.276, 687-698(1987).

[Schm] Schmidt, C.–G., *The p-adic L-functions attached to Rankin convolutions of modular forms*, J. reine angew. Math. 368 (1986) 201–220.

[Scho] Scholl, A., *Motives for modular forms*, Inv. Math. 100 (1990), 419–430.

[SchEu] Scholl, A.J., *An introduction to Kato's Euler systems*, Scholl, A. J. (ed.) et al., Galois representations in arithmetic algebraic geometry. Proceedings of the symposium, Durham, UK, July 9-18, 1996. Cambridge: Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 254, 379-460 (1998).

[Se73] Serre, J.–P., *Formes modulaires et fonctions zêta p-adiques*, Lect Notes in Math. 350 (1973) 191–268 (Springer Verlag).

[Shi71] Shimura G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.

[Shi75] Shimura G., *On the holomorphy of certain Dirichlet series*, Proc. Lond. Math. Soc. 31 (1975) 79–98.

[Shi76] Shimura G., *The special values of the zeta functions associated with cusp forms.* Comm. Pure Appl. Math. 29 (1976), no. 6, 783–804.

[Shi77] Shimura G., *On the periods of modular forms*, Math. Annalen 229 (1977) 211–221.

[Shi82] Shimura, G., *Confluent Hypergeometric Functions on Tube Domains*, Math. Ann. 260 (1982), p. 269-302.

[Sh83] Shimura, G., *On Eisenstein Series*, Duke Math. J; 50 (1983), p. 417-476.

[ShiAr] Shimura, G., *Arithmeticity in the theory of automorphic forms*, Mathematical Surveys and Monographs. 82. Providence, RI: American Mathematical Society (AMS) . x, 302 p. (2000).

[V] Visik, M.M., *Non-Archimedean measures connected with Dirichlet series*, Math. USSR Sb. 28 (1976), 216-228 (1978).

[MV] Vishik, M.M. and Manin, Yu.I., *p-adic Hecke series of imaginary quadratic fields*, Math. USSR, Sbornik 24 (1974), 345-371 (1976).

[We56] Weil, A., *On a certain type of characters of the idèle-class group of an algebraic number-field*, Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 1–7, Science Council of Japan, Tokyo, 1956.

[Wi95] Wiles A., *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math., II. Ser. 141, No.3 (1995) 443–55.

Siegfried Böcherer
Kunzenhof 4B,
79117 Freiburg,
Germany
boech@siegel.math.uni-mannheim.de

A. A. Panchishkin
Institut Fourier, B.P.74
38402 St.-Martin d'Hères
France
panchish@mozart.ujf-grenoble.fr

On the Equivariant Tamagawa Number Conjecture for Tate Motives, Part II.

Dedicated to John Coates

David Burns and Matthias Flach

Received: October 26, 2005
Revised: May 1, 2006

Abstract. Let K be any finite abelian extension of $\mathbb{Q}$, k any subfield of K and r any integer. We complete the proof of the equivariant Tamagawa Number Conjecture for the pair $(h^0(\mathrm{Spec}(K))(r), \mathbb{Z}[\mathrm{Gal}(K/k)])$.

2000 Mathematics Subject Classification: Primary 11G40; Secondary 11R65 19A31 19B28

1. Introduction

Let K/k be a Galois extension of number fields with group G. For each complex character χ of G denote by $L(\chi, s)$ the Artin L-function of χ and let $\hat{G}$ be the set of irreducible characters. We call

$$\zeta_{K/k}(s) = (L(\chi, s))_{\chi\in\hat{G}}$$

the equivariant Dedekind Zeta function of K/k. It is a meromorphic function with values in the center $\prod_{\chi\in\hat{G}}\mathbb{C}$ of $\mathbb{C}[G]$. The 'equivariant Tamagawa number conjecture' that is formulated in [9, Conj. 4], when specialized to the motive $M := \mathbb{Q}(r)_K := h^0(\mathrm{Spec}(K))(r)$ and the order $\mathfrak{A} := \mathbb{Z}[G]$, gives a cohomological interpretation of the leading Taylor coefficient of $\zeta_{K/k}(s)$ at any integer argument $s = r$. We recall that this conjecture is a natural refinement of the seminal 'Tamagawa number conjecture' that was first formulated by Bloch and Kato in [5] and then both extended and refined by Fontaine and Perrin-Riou [18] and Kato [27]. If $K = k$ and $r \in \{0, 1\}$ then the conjecture specializes to the analytic class number formula and is therefore already a theorem.

The most succinct formulation of the equivariant Tamagawa number conjecture asserts the vanishing of a certain element $T\Omega(M, \mathfrak{A}) = T\Omega(\mathbb{Q}(r)_K, \mathbb{Z}[G])$ in the relative algebraic K-group $K_0(\mathbb{Z}[G],\mathbb{R})$. Further, the functional equation of Artin L-functions is reflected by an equality

$$(1)\quad T\Omega(\mathbb{Q}(r)_K,\mathbb{Z}[G])+\psi^*(T\Omega(\mathbb{Q}(1-r)_K,\mathbb{Z}[G]^{\mathrm{op}}))=T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$$

where ψ^* is a natural isomorphism $K_0(\mathbb{Z}[G]^{\mathrm{op}},\mathbb{R})\cong K_0(\mathbb{Z}[G],\mathbb{R})$ and $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ is an element of $K_0(\mathbb{Z}[G],\mathbb{R})$ of the form

$$(2)\ T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])=L^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])+\delta_{K/k}(r)+R\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G]).$$

Here $L^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ is an 'analytic' element constructed from the archimedean Euler factors and epsilon constants associated to both $\mathbb{Q}(r)_K$ and $\mathbb{Q}(1-r)_K$, the element $\delta_{K/k}(r)$ reflects sign differences between the regulator maps used in defining $T\Omega(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ and $T\Omega(\mathbb{Q}(1-r)_K,\mathbb{Z}[G]^{\mathrm{op}})$ and $R\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ is an 'algebraic' element constructed from the various realisations of $\mathbb{Q}(r)_K$. (We caution the reader that the notation in (1) and (2) is slightly different from that which is used in [9] - see §3.1 for details of these changes.)
In this article we shall further specialize to the case where K is an *abelian* extension of $\mathbb{Q}$ and prove that $T\Omega(\mathbb{Q}(r)_K,\mathbb{Z}[G])=0$ for all integers r and all subgroups G of $\mathrm{Gal}(K/\mathbb{Q})$. In fact, taking advantage of previous work in this area, the main new result which we prove here is the following refinement of the results of Benois and Nguyen Quang Do in [1].

Theorem 1.1. *If K is any finite abelian extension of $\mathbb{Q}$, G any subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ and r any strictly positive integer, then $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])=0$.*

We now discuss some interesting consequences of Theorem 1.1. The first consequence we record is the promised verification of the equivariant Tamagawa number conjecture for Tate motives over absolutely abelian fields. This result therefore completes the proof of [17, Th. 5.1] and also refines the main result of Huber and Kings in [25] (for more details of the relationship between our approach and that of [25] see [11, Intro.]).

Corollary 1.2. *If K is any finite abelian extension of $\mathbb{Q}$, G any subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ and r any integer, then $T\Omega(\mathbb{Q}(r)_K,\mathbb{Z}[G])=0$.*

Proof. If $r\leq 0$, then the vanishing of $T\Omega(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ is proved modulo powers of 2 by Greither and the first named author in [11, Cor. 8.1] and the argument necessary to cover the 2-primary part is provided by the second named author in [17]. For any $r>0$, the vanishing of $T\Omega(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ then follows by combining Theorem 1.1 with the equality (1). □

Corollary 1.3. *The conjecture of Bloch and Kato* [5, Conj. (5.15)] *is valid for the Riemann-Zeta function at each integer strictly bigger than* 1.

Proof. If r is any integer strictly bigger than 1, then [5, Th. (6.1)] proves the validity of [5, Conj. (5.15)] for the leading term of the Riemann Zeta function at $s=r$, modulo powers of 2 and a certain compatibility assumption [5, Conj. (6.2)] concerning the 'cyclotomic elements' of Deligne and Soulé in algebraic

K-theory. But the latter assumption was verified by Huber and Wildeshaus in [26] and Corollary 1.2 for $K = k = \mathbb{Q}$ now resolves the ambiguity at 2. □

For any finite group G the image of the homomorphism $\delta_G : K_0(\mathbb{Z}[G], \mathbb{R}) \to K_0(\mathbb{Z}[G])$ that occurs in the long exact sequence of relative K-theory is equal to the locally-free class group $\mathrm{Cl}(\mathbb{Z}[G])$. In the following result we use the elements $\Omega(K/k, 1), \Omega(K/k, 2), \Omega(K/k, 3)$ and $w(K/k)$ of $\mathrm{Cl}(\mathbb{Z}[\mathrm{Gal}(K/k)])$ that are defined by Chinburg in [13].

Corollary 1.4. *If K is any finite abelian extension of $\mathbb{Q}$ and k is any subfield of K, then one has $\Omega(K/k, 1) = \Omega(K/k, 2) = \Omega(K/k, 3) = w(K/k) = 0$. In particular, the Chinburg conjectures are all valid for K/k.*

Proof. In this first paragraph we do not assume that K is Galois over $\mathbb{Q}$ or that $G := \mathrm{Gal}(K/k)$ is abelian. We recall that from [10, (31)] one has

$$\delta_G(\psi^*(T\Omega(\mathbb{Q}(0)_K, \mathbb{Z}[G]^{\mathrm{op}}))) = \Omega(K/k, 3) - w(K/k).$$

Further, [4, Prop. 3.1] implies δ_G sends $L^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[G]) + \delta_{K/k}(1)$ to $-w(K/k)$ whilst the argument used in [4, §4.3] shows that $R\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[G])$ is equal to the element $R\Omega^{\mathrm{loc}}(K/k, 1)$ defined in [7, §5.1.1]. Hence, from [7, Rem. 5.5], we may deduce that

$$(3) \qquad \delta_G(T\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[G])) = -w(K/k) + \Omega(K/k, 2).$$

We now assume that G is abelian. Then G has no irreducible complex symplectic characters and so the very definition of $w(K/k)$ ensures that $w(K/k) = 0$. Hence by combining the above displayed equalities with Theorem 1.1 (with $r = 1$) and Corollary 1.2 (with $r = 0$) we may deduce that $\Omega(K/k, 2) = \Omega(K/k, 3) = 0$. But from [13, (3.2)] one has $\Omega(K/k, 1) = \Omega(K/k, 2) - \Omega(K/k, 3)$, and so this also implies that $\Omega(K/k, 1) = 0$. □

For finite abelian extensions $K/\mathbb{Q}$ in which 2 is unramified, an alternative proof of the equality $\Omega(K/k, 2) = 0$ in Corollary 1.4 was first obtained by Greither in [21].

Before stating our next result we recall that, ever since the seminal results of Fröhlich in [19], the study of Quaternion extensions has been very important to the development of leading term conjectures in non-commutative settings. In the following result we provide a natural refinement of the main result of Hooper, Snaith and Tran in [24] (and hence extend the main result of Snaith in [35]).

Corollary 1.5. *Let K be any Galois extension of $\mathbb{Q}$ for which $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the Quaternion group of order 8 and k any subfield of K. Then one has $T\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[\mathrm{Gal}(K/k)]) = 0$.*

Proof. We set $G := \mathrm{Gal}(K/\mathbb{Q})$ and let Γ denote the maximal abelian quotient of G with E the subfield of K such that $\Gamma = \mathrm{Gal}(E/\mathbb{Q})$ (so $E/\mathbb{Q}$ is biquadratic). We set $T\Omega^{\mathrm{loc}} := T\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[G])$ and $T\Omega^{\mathrm{loc}}_E := T\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_E, \mathbb{Z}[\Gamma])$.

Then from [9, Th. 5.1 and Prop. 4.1] we know that $T\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[\mathrm{Gal}(K/k)])$ and $T\Omega^{\mathrm{loc}}_E$ are equal to the images of $T\Omega^{\mathrm{loc}}$ under the natural homomorphisms

$K_0(\mathbb{Z}[G],\mathbb{R}) \to K_0(\mathbb{Z}[\mathrm{Gal}(K/k)],\mathbb{R})$ and $K_0(\mathbb{Z}[G],\mathbb{R}) \to K_0(\mathbb{Z}[\Gamma],\mathbb{R})$ respectively. In particular, it suffices to prove that $T\Omega^{\mathrm{loc}} = 0$.
Now [4, Cor. 6.3(i)] implies that $T\Omega^{\mathrm{loc}}$ is an element of finite order in the subgroup $K_0(\mathbb{Z}[G],\mathbb{Q})$ of $K_0(\mathbb{Z}[G],\mathbb{R})$ and so [10, Lem. 4] implies that $T\Omega^{\mathrm{loc}} = 0$ if and only if both $T\Omega^{\mathrm{loc}}_E = 0$ and $\delta_G(T\Omega^{\mathrm{loc}}) = 0$. But Theorem 1.1 implies $T\Omega^{\mathrm{loc}}_E = 0$ and, since $\delta_G(T\Omega^{\mathrm{loc}}) = -w(K/\mathbb{Q}) + \Omega(K/\mathbb{Q},2)$ (by (3)), the main result of Hooper, Snaith and Tran in [24] implies that $\delta_G(T\Omega^{\mathrm{loc}}) = 0$. □

The following result provides the first generalization to wildly ramified extensions of the algebraic characterization of tame symplectic Artin root numbers that was obtained by Cassou-Noguès and Taylor in [12].

Corollary 1.6. *Let K be any Galois extension of $\mathbb{Q}$ for which $G := \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the Quaternion group of order 8. Then the Artin root number of the (unique) irreducible 2-dimensional complex character of G is uniquely determined by the algebraic invariant $R\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K,\mathbb{Z}[G])$ in $K_0(\mathbb{Z}[G],\mathbb{R})$.*

Proof. This is a direct consequence of combining Corollary 1.5 with a result of Breuning and the first named author [7, Th. 5.8] and the following facts: $L^{\mathrm{loc}}(\mathbb{Q}(1)_K,\mathbb{Z}[G])+\delta_{K/\mathbb{Q}}(1)$ is equal to -1 times the element $\hat{\partial}^1_G(\epsilon_{K/\mathbb{Q}}(0))$ used in [7, §5.1.1] and $R\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K,\mathbb{Z}[G])$ is equal to the element $R\Omega^{\mathrm{loc}}(K/\mathbb{Q},1)$ defined in loc. cit. □

To prove Theorem 1.1 we shall combine some classical and rather explicit computations of Hasse (concerning Gauss sums) and Leopoldt (concerning integer rings in cyclotomic fields) with a refinement of some general results proved in [9, §5] and a systematic use of the Iwasawa theory of complexes in the spirit of Kato [27, 3.1.2] and Nekovář [32] and of the generalization of the fundamental exact sequence of Coleman theory obtained by Perrin-Riou in [34].
We would like to point out that, in addition to the connections discussed above, there are also links between our approach and aspects of the work of Kato [28], Fukaya and Kato [20] and Benois and Berger [2]. In particular, the main technical result that we prove (the validity of equality (16)) is closely related to [28, Th. 4.1] and hence also to the material of [20, §3]. Indeed, Theorem 1.1 (in the case $r = 1$) provides a natural generalization of the results discussed in [20, §3.6]. However, the arguments of both loc. cit. and [28] do not cover the prime 2 and also leave open certain sign ambiguities, and much effort is required in the present article to deal with such subtleties.
Both authors were introduced to the subject of Tamagawa number conjectures by John Coates. It is therefore a particular pleasure for us to dedicate this paper to him on the occasion of his sixtieth birthday.

Acknowledgements The authors are grateful to Denis Benois for several very helpful conversations regarding this project and also to Laurent Berger and Manuel Breuning for some very helpful advice. Much of the research for this article was completed when the authors held visiting positions in the Mathematics Department of Harvard University and they are very grateful to Dick Gross for making that visit possible.

2. Equivariant local Tamagawa numbers

In this article we must compute explicitly certain equivariant local Tamagawa numbers, as defined in [9]. For the reader's convenience, we therefore first quickly review the general definition of such invariants. All further details of this construction can be found in loc. cit.

2.1. We fix a motive M that is defined over $\mathbb{Q}$ (if M is defined over a general number field as in [9], then we use induction to reduce to the base field $\mathbb{Q}$) and we assume that M is endowed with an action of a finite dimensional semisimple $\mathbb{Q}$-algebra A.

We write $H_{dR}(M)$ and $H_B(M)$ for the de Rham and Betti realisations of M and for each prime number p we denote by $V_p = H_p(M)$ the p-adic realisation of M. We fix a $\mathbb{Z}$-order $\mathfrak{A}$ in A such that, for each prime p, if we set $\mathfrak{A}_p := \mathfrak{A}\otimes_{\mathbb{Z}}\mathbb{Z}_p$, then there exists a full projective Galois stable $\mathfrak{A}_p$-sublattice T_p of V_p. We also fix a finite set S of places of $\mathbb{Q}$ containing ∞ and all primes of bad reduction for M and then set $S_p := S \cup \{p\}$ and $S_{p,f} := S_p \setminus \{\infty\}$.

For any associative unital ring R we write $D^{\mathrm{perf}}(R)$ for the derived catgeory of perfect complexes of R-modules. We also let $\mathrm{Det}_R : D^{\mathrm{perf}}(R) \to V(R)$ denote the universal determinant functor to the Picard category of virtual objects of R (which is denoted by $P \mapsto [P]$ in [9]) and $\otimes_R$ the product functor in $V(R)$ (denoted by $\boxtimes$ in [9]). In particular, if R is commutative, then Det_R is naturally isomorphic to the Knudsen-Mumford functor to graded invertible R-modules. We denote by $\mathbf{1}_R$ a unit object of $V(R)$ and recall that the group $K_1(R)$ can be identified with $\mathrm{Aut}_{V(R)}(L)$ for any object L of $V(R)$ (and in particular therefore with $\pi_1(V(R)) := \mathrm{Aut}_{V(R)}(\mathbf{1}_R)$). For each automorphism $\alpha : W \to W$ of a finitely generated projective R-module W we denote by $\mathrm{Det}_R(\alpha|W)$ the element of $K_1(R)$ that is represented by α. We let $\zeta(R)$ denote the centre of R.

If X is any R-module upon which complex conjugation acts as an endomorphism of R-modules, then we write X^+ and X^- for the R-submodules of X upon which complex conjugation acts as multiplication by 1 and -1 respectively.

For any $\mathbb{Q}$-vector space W we set $W_{\mathbb{C}} = W \otimes_{\mathbb{Q}} \mathbb{C}$, $W_{\mathbb{R}} = W \otimes_{\mathbb{Q}} \mathbb{R}$ and $W_p = W \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for each prime p.

2.2. The virtual object

$$\Xi^{\mathrm{loc}}(M) := \mathrm{Det}_A(H_{dR}(M)) \otimes_A \mathrm{Det}_A^{-1}(H_B(M))$$

is endowed with a canonical morphism

$$\vartheta_\infty^{\mathrm{loc}} : A_{\mathbb{R}} \otimes_A \Xi^{\mathrm{loc}}(M) \cong \mathbf{1}_{A_{\mathbb{R}}}.$$

To describe this morphism we note that the canonical period isomorphism $H_{dR}(M)_{\mathbb{C}} \cong H_B(M)_{\mathbb{C}}$ induces an isomorphism of $A_{\mathbb{R}}$-modules

$$H_{dR}(M)_{\mathbb{R}} = (H_{dR}(M)_{\mathbb{C}})^+ \cong (H_B(M)_{\mathbb{C}})^+ \tag{4}$$

and that there is also a canonical isomorphism of $A_{\mathbb{R}}$-modules

$$(5)\quad (H_B(M)_{\mathbb{C}})^+ = (H_B(M)^+ \otimes_{\mathbb{Q}} \mathbb{R}) \oplus (H_B(M)^- \otimes_{\mathbb{Q}} \mathbb{R}(2\pi i)^{-1}) \\ \cong (H_B(M)^+ \otimes_{\mathbb{Q}} \mathbb{R}) \oplus (H_B(M)^- \otimes_{\mathbb{Q}} \mathbb{R}) = H_B(M)_{\mathbb{R}}$$

where the central map results from identifying $\mathbb{R}(2\pi i)^{-1}$ with $\mathbb{R}$ by sending $(2\pi i)^{-1}$ to 1.

By applying $\mathrm{Det}_{A_{\mathbb{R}}}$ to the composite of (4) and (5) one obtains a morphism $(\vartheta_\infty^{\mathrm{loc}})' : A_{\mathbb{R}} \otimes_A \Xi^{\mathrm{loc}}(M) \cong \mathbf{1}_{A_{\mathbb{R}}}$ and $\vartheta_\infty^{\mathrm{loc}}$ is defined in [9, (57)] to be the composite of $(\vartheta_\infty^{\mathrm{loc}})'$ and the 'sign' elements $\epsilon_B := \mathrm{Det}_A(-1 \mid H_B(M)^+)$ and $\epsilon_{dR} := \mathrm{Det}_A(-1 \mid F^0 H_{dR}(M))$ of $\pi_1(V(A_{\mathbb{R}})) \cong K_1(A_{\mathbb{R}})$.

2.3. Following [9, (66), (67)], we set

$$\Lambda_p(S, V_p) := \left(\bigotimes_{\ell \in S_{p,f}} \mathrm{Det}_{A_p}^{-1} R\Gamma(\mathbb{Q}_\ell, V_p) \right) \otimes_{A_p} \mathrm{Det}_{A_p}^{-1}(V_p),$$

and let

$$\theta_p : A_p \otimes_A \Xi^{\mathrm{loc}}(M) \cong \Lambda_p(S, V_p)$$

denote the morphism in $V(A_p)$ obtained by taking the product of the morphisms $\theta_p^{\ell\text{-part}}$ for $\ell \in S_{p,f}$ that are discussed in the next subsection.

2.4. There exists a canonical morphism in $V(A_p)$ of the form

$$\theta_p^{p\text{-part}} : A_p \otimes_A \Xi^{\mathrm{loc}}(M) \to \mathrm{Det}_{A_p}^{-1} R\Gamma(\mathbb{Q}_p, V_p) \otimes_{A_p} \mathrm{Det}_{A_p}^{-1}(V_p).$$

This morphism results by applying Det_{A_p} to each of the following: the canonical comparison isomorphism $H_B(M)_p \cong V_p$; the (Poincaré duality) exact sequence $0 \to (H_{dR}(M^*(1))/F^0)^* \to H_{dR}(M) \to H_{dR}(M)/F^0 \to 0$; the canonical comparison isomorphisms $(H_{dR}(M)/F^0)_p \cong t_p(V_p)$ and $(H_{dR}(M^*(1))/F^0)_p^* \cong t_p(V_p^*(1))^*$; the exact triangle

$$(6)\qquad R\Gamma_f(\mathbb{Q}_p, V_p) \to R\Gamma(\mathbb{Q}_p, V_p) \to R\Gamma_f(\mathbb{Q}_p, V_p^*(1))^*[-2] \to$$

which results from [9, (18) and Lem. 12a)]; the exact triangle

$$(7)\qquad t_p(W)[-1] \to R\Gamma_f(\mathbb{Q}_p, W) \to \big(D_{\mathrm{cris}}(W) \xrightarrow{1-\varphi_v} D_{\mathrm{cris}}(W)\big) \to$$

of [9, (22)] for both $W = V_p$ and $W = V_p^*(1)$, where the first term of the last complex is placed in degree 0 and $\mathrm{Det}_{A_p}\big(D_{\mathrm{cris}}(W) \xrightarrow{1-\varphi_v} D_{\mathrm{cris}}(W)\big)$ is identified with $\mathbf{1}_{A_p}$ via the canonical morphism $\mathrm{Det}_{A_p}(D_{\mathrm{cris}}(W)) \otimes_{A_p} \mathrm{Det}_{A_p}^{-1}(D_{\mathrm{cris}}(W)) \to \mathbf{1}_{A_p}$.

For each $\ell \in S_{p,f} \setminus \{p\}$ there exists a canonical morphism in $V(A_p)$ of the form

$$\theta_p^{\ell\text{-part}} : \mathbf{1}_{A_p} \cong \mathrm{Det}_{A_p}^{-1} R\Gamma(\mathbb{Q}_\ell, V_p).$$

For more details about this morphism see Proposition 7.1.

2.5. From [9, (71), (78)] we recall that there exists a canonical object $\Lambda_p(S,T_p)$ of $V(\mathfrak{A}_p)$ and a canonical morphism in $V(A_p)$ of the form

$$\theta'_p : \Lambda_p(S,V_p) \cong A_p \otimes_{\mathfrak{A}_p} \Lambda_p(S,T_p)$$

(the definitions of $\Lambda_p(S,T_p)$ and θ'_p are to be recalled further in §7.2). We set

$$\vartheta_p^{\mathrm{loc}} := \epsilon(S,p)\circ\theta'_p\circ\theta_p : A_p\otimes_A \Xi^{\mathrm{loc}}(M) \cong A_p\otimes_{\mathfrak{A}_p}\Lambda_p(S,T_p)$$

where $\epsilon(S,p)$ is the element of $\pi_1(V(A_p))$ that corresponds to multiplication by -1 on the complex $\bigoplus_{\ell\in S_{p,f}} R\Gamma_{/f}(\mathbb{Q}_\ell,V_p)$ which is defined in [9, (18)].
If M is a direct factor of $h^n(X)(t)$ for any non-negative integer n, smooth projective variety X and integer t, then [9, Lem. 15b)] implies that the data

$$(\prod_p \Lambda_p(S,T_p), \Xi^{\mathrm{loc}}(M), \prod_p \vartheta_p^{\mathrm{loc}}; \vartheta_\infty^{\mathrm{loc}}),$$

where p runs over all prime numbers, gives rise (conjecturally in general, but unconditionally in the case of Tate motives) to a canonical element $R\Omega^{\mathrm{loc}}(M,\mathfrak{A})$ of $K_0(\mathfrak{A},\mathbb{R})$. For example, if A is commutative, then $\mathbf{1}_{A_\mathbb{R}} = (A_\mathbb{R},0)$ and $K_0(\mathfrak{A},\mathbb{R})$ identifies with the multiplicative group of invertible $\mathfrak{A}$-sublattices of $A_\mathbb{R}$ and, with respect to this identification, $R\Omega^{\mathrm{loc}}(M,\mathfrak{A})$ corresponds to the (conjecturally invertible) $\mathfrak{A}$-sublattice Ξ of $A_\mathbb{R}$ that is defined by the equality

$$\vartheta_\infty^{\mathrm{loc}}\left(\bigcap_p(\Xi^{\mathrm{loc}}(M)\cap(\vartheta_p^{\mathrm{loc}})^{-1}(\Lambda_p(S,T_p)))\right) = (\Xi,0),$$

where the intersection is taken over all primes p.

2.6. We write $L_\infty({}_AM,s)$ and $\epsilon({}_AM,0)$ for the archimedean Euler factor and epsilon constant that are defined in [9, §4.1]. Also, with $\rho\in\mathbb{Z}^{\pi_0(\mathrm{Spec}(\zeta(A_\mathbb{R})))}$ denoting the algebraic order at $s=0$ of the completed $\zeta(A_\mathbb{C})$-valued L-function $\Lambda({}_{A^{op}}M^*(1),s)$ that is defined in loc. cit., we set

$$\mathcal{E}({}_AM) := (-1)^\rho\epsilon({}_AM,0)\frac{L_\infty^*({}_{A^{op}}M^*(1),0)}{L_\infty^*({}_AM,0)} \in \zeta(A_\mathbb{R})^\times.$$

Following [9, §5.1], we define

$$L^{\mathrm{loc}}(M,\mathfrak{A}) := \hat\delta^1_{\mathfrak{A},\mathbb{R}}(\mathcal{E}({}_AM)) \in K_0(\mathfrak{A},\mathbb{R})$$

where $\hat\delta^1_{\mathfrak{A},\mathbb{R}} : \zeta(A_\mathbb{R})^\times \to K_0(\mathfrak{A},\mathbb{R})$ is the 'extended boundary homomorphism' of [9, Lem. 9] (so, if A is commutative, then $L^{\mathrm{loc}}(M,\mathfrak{A}) = \mathfrak{A}\cdot\mathcal{E}({}_AM)\subset A_\mathbb{R}$). Finally, we let

$$T\Omega^{\mathrm{loc}}(M,\mathfrak{A})' := L^{\mathrm{loc}}(M,\mathfrak{A}) + R\Omega^{\mathrm{loc}}(M,\mathfrak{A}) \in K_0(\mathfrak{A},\mathbb{R}) \tag{8}$$

denote the 'equivariant local Tamagawa number' that is defined in [9, just prior to Th. 5.1].

3. Normalizations and notation

3.1. Normalizations. In this section we fix an arbitrary Galois extension of number fields K/k, set $G := \mathrm{Gal}(K/k)$ and for each integer t write $T\Omega(\mathbb{Q}(t)_K, \mathbb{Z}[G])'$ for the element of $K_0(\mathbb{Z}[G], \mathbb{R})$ that is defined (unconditionally) by [9, Conj. 4(iii)] in the case $M = \mathbb{Q}(t)_K$ and $\mathfrak{A} = \mathbb{Z}[G]$.

Let r be a strictly positive integer. Then the computations of [10, 17] show that [9, Conj. 4(iv)] requires that the morphism $\vartheta_\infty : \mathbb{R}\otimes_{\mathbb{Q}} \Xi(\mathbb{Q}(1-r)_K) \to \mathbf{1}_{V(\mathbb{R}[G])}$ constructed in [9, §3.4] should be normalized by using -1 times the Dirichlet (resp. Beilinson if $r > 1$) regulator map, rather than the Dirichlet (resp. Beilinson) regulator map itself as used in [9]. To incorporate this observation we set

$$T\Omega(\mathbb{Q}(1-r)_K, \mathbb{Z}[G]) := T\Omega(\mathbb{Q}(1-r)_K, \mathbb{Z}[G])' + \delta_{K/k}(r) \tag{9}$$

where $\delta_{K/k}(r)$ is the image under the canonical map $K_1(\mathbb{R}[G]) \to K_0(\mathbb{Z}[G], \mathbb{R})$ of the element $\mathrm{Det}_{\mathbb{Q}[G]}(-1 \mid K_{2r-1}(\mathcal{O}_K)^* \otimes_{\mathbb{Z}} \mathbb{Q})$. To deduce the validity of (1) from the result of [9, Th. 5.3] it is thus also necessary to renormalise the definition of either $T\Omega(\mathbb{Q}(r)_K, \mathbb{Z}[G])'$ or of the element $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])'$ defined by (8). Our proof of Theorem 1.1 now shows that the correct normalization is to set

$$T\Omega(\mathbb{Q}(r)_K, \mathbb{Z}[G]) := T\Omega(\mathbb{Q}(r)_K, \mathbb{Z}[G])'$$

and

$$T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G]) := T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])' + \delta_{K/k}(r). \tag{10}$$

Note that the elements defined in (9) and (10) satisfy all of the functorial properties of $T\Omega(\mathbb{Q}(1-r)_K, \mathbb{Z}[G])'$ and $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])'$ that are proved in [9, Th. 5.1, Prop. 4.1]. Further, with these definitions, the equalities (1) and (2) are valid and it can be shown that the conjectural vanishing of $T\Omega^{\mathrm{loc}}(\mathbb{Q}(1)_K, \mathbb{Z}[G])$ is compatible with the conjectures discussed in both [4] and [7].

Thus, in the remainder of this article we always use the notation $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])$ as defined in (10).

3.2. The abelian case. Until explicitly stated otherwise, in the sequel we consider only abelian groups. Thus, following [9, §2.5], we use the graded determinant functor of [29] in place of virtual objects (for a convenient review of all relevant properties of the determinant functor see [11, §2]). However, we caution the reader that for reasons of typographical clarity we sometimes do not distinguish between a graded invertible module and the underlying invertible module.

We note that, when proving Theorem 1.1, the functorial properties of the elements $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[\mathrm{Gal}(K/k)])$ allow us to assume that $k = \mathbb{Q}$ and also that K is generated by a primitive N-th root of unity for some natural number $N \not\equiv 2 \mod 4$. Therefore, until explicitly stated otherwise, we henceforth fix the following notation:

$$K := \mathbb{Q}(e^{2\pi i/N}); \quad G := \mathrm{Gal}(K/\mathbb{Q}); \quad M := \mathbb{Q}(r)_K, \quad r \geq 1; \quad A := \mathbb{Q}[G].$$

For any natural number n we also set $\zeta_n := e^{2\pi i/n}$ and denote by σ_n the resulting complex embedding of the field $\mathbb{Q}(\zeta_n)$.
For each complex character η of G we denote by $e_\eta = \frac{1}{|G|}\sum_{g\in G}\eta(g^{-1})g$ the associated idempotent in $A_{\mathbb{C}}$. For each $\mathbb{Q}$-rational character (or equivalently, $\mathrm{Aut}(\mathbb{C})$-conjugacy class of $\mathbb{C}$-rational characters) χ of G we set $e_\chi = \sum_{\eta\in\chi} e_\eta \in A$ and denote by $\mathbb{Q}(\chi) = e_\chi A$ the field of values of χ. There is a ring decomposition $A = \prod_\chi \mathbb{Q}(\chi)$ and a corresponding decomposition $Y = \prod_\chi e_\chi Y$ for any A-module Y. We make similar conventions for $\mathbb{Q}_p$-rational characters of G.

4. An explicit analysis of $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])$

In this section we reduce the proof of Theorem 1.1 to the verification of an explicit local equality (cf. Proposition 4.4).

4.1. The archimedean component of $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])$. In this subsection we explicate the morphism $\vartheta_\infty^{\mathrm{loc}}$ defined in §2.2 and the element $\mathcal{E}({}_AM) \in A_{\mathbb{R}}^\times$ defined in §2.6.
The de Rham realization $H_{dR}(M)$ of M identifies with K, considered as a free A-module of rank one (by means of the normal basis theorem). The Betti realisation $H_B(M)$ of M identifies with the $\mathbb{Q}$-vector space Y_Σ with basis equal to the set $\Sigma := \mathrm{Hom}(K, \mathbb{C})$ of field embeddings and is therefore also a free A-module of rank one (with basis σ_N). We set $Y_\Sigma^{-1} := \mathrm{Hom}_A(Y_\Sigma, A)$. Then, by [9, Th. 5.2], we know that $(\vartheta_\infty^{\mathrm{loc}})^{-1}((\mathcal{E}({}_AM)^{-1}, 0))$ belongs to $\Xi^{\mathrm{loc}}(M) = (K \otimes_A Y_\Sigma^{-1}, 0)$ and we now describe this element explicitly.

Proposition 4.1. *We define an element $\epsilon_\infty := \sum_\chi \epsilon_{\infty,\chi} e_\chi$ of $A^\times$ by setting*

$$\epsilon_{\infty,\chi} := \begin{cases} -2 & \text{if } \chi(-1) = (-1)^r \\ -\frac{1}{2} & \text{if } \chi(-1) = -(-1)^r \text{ and } (\chi \neq 1 \text{ or } r > 1) \\ \frac{1}{2} & \text{if } \chi = 1 \text{ and } r = 1. \end{cases}$$

Then

$$(\vartheta_\infty^{\mathrm{loc}})^{-1}((\mathcal{E}({}_AM)^{-1}, 0)) = (\epsilon_\infty \beta_N \otimes \sigma_N^{-1}, 0) \in (K \otimes_A Y_\Sigma^{-1}, 0)$$

where σ_N^{-1} is the (unique) element of Y_Σ^{-1} which satisfies $\sigma_N^{-1}(\sigma_N) = 1$ and β_N is the (unique) element of $K = \prod_\chi e_\chi K$ which satisfies

$$e_\chi \beta_N := [K : \mathbb{Q}(\zeta_{f_\chi})]^{-1}(r-1)!f_\chi^{r-1} \cdot e_\chi \zeta_{f_\chi}$$

for all $\mathbb{Q}$-rational characters χ of G.

Proof. For each Dirichlet character η of G the functional equation of $L(\eta, s)$ is

$$L(\eta, s) = \frac{\tau(\eta)}{2i^\delta}\left(\frac{2\pi}{f_\eta}\right)^s \frac{1}{\Gamma(s)\cos(\frac{\pi(s-\delta)}{2})} L(\bar{\eta}, 1-s)$$

where f_η is the conductor of η and

$$\tau(\eta) = \sum_{a=1}^{f_\eta} \eta(a) e^{2\pi i a/f_\eta}; \quad \eta(-1) = (-1)^\delta,\ \delta \in \{0, 1\} \tag{11}$$

(cf. [36, Ch. 4]). Thus, by its very definition in §2.6, the η-component of the element $\mathcal{E}({}_AM)^{-1}$ of $A_{\mathbb{C}} = \prod_\eta \mathbb{C}$ is the leading Taylor coefficient at $s = r$ of the meromorphic function

$$(-1)^{\rho_\eta} \frac{2i^\delta}{\tau(\eta)} \left(\frac{f_\eta}{2\pi}\right)^s \Gamma(s) \cos(\frac{\pi(s-\delta)}{2}); \qquad \rho_\eta = \begin{cases} 1 & r=1, \eta=1 \\ 0 & \text{else.} \end{cases}$$

Hence we have

$$\mathcal{E}({}_AM)_\eta^{-1} = \begin{cases} \frac{2i^\delta}{\tau(\eta)} \left(\frac{f_\eta}{2\pi}\right)^r (r-1)!(-1)^{\frac{r-\delta}{2}}, & r-\delta \text{ even} \\ (-1)^{\rho_\eta} \frac{2i^\delta}{\tau(\eta)} \left(\frac{f_\eta}{2\pi}\right)^r (r-1)!(-1)^{\frac{r-\delta+1}{2}} \frac{\pi}{2}, & r-\delta \text{ odd} \end{cases}$$

which, after collecting powers of i and using the relation $\tau(\eta)\tau(\bar\eta) = \eta(-1)f_\eta$, can be written as

$$\mathcal{E}({}_AM)_\eta^{-1} = \begin{cases} 2\,\tau(\bar\eta)(2\pi i)^{-r} f_\eta^{r-1}(r-1)!, & r-\delta \text{ even} \\ (-1)^{\rho_\eta+1}\frac{1}{2}\,\tau(\bar\eta)(2\pi i)^{-(r-1)} f_\eta^{r-1}(r-1)!, & r-\delta \text{ odd.} \end{cases}$$

Lemma 4.2. *The isomorphism $Y_{\Sigma,\mathbb{C}}^+ = (H_B(M)_{\mathbb{C}})^+ \cong H_B(M)_{\mathbb{R}} = Y_{\Sigma,\mathbb{R}}$ in (5) is given by*

$$\sum_{g\in G} \alpha_g g^{-1}\sigma_N \mapsto \sum_{g\in G/<c>} \big(\Re(\alpha_g)(1+(-1)^r c) - 2\pi\Im(\alpha_g)(1-(-1)^r c)\big) g^{-1}\sigma_N$$

where $c \in G$ is complex conjugation, G acts on Σ via $(g\sigma)(x) = \sigma(g(x))$ and $\Re(\alpha)$, resp. $\Im(\alpha)$, denotes the real, resp. imaginary, part of $\alpha \in \mathbb{C}$.

Proof. An element $x := \sum_{g\in G} \alpha_g g^{-1}\sigma_N$ of $Y_{\Sigma,\mathbb{C}}$ belongs to the subspace $Y_{\Sigma,\mathbb{C}}^+$ if and only if one has $\alpha_{gc} = (-1)^r \bar\alpha_g$ for all $g \in G$. Writing

$$\alpha_g = \Re(\alpha_g) - (2\pi i)^{-1}(2\pi)\Im(\alpha_g), \quad \bar\alpha_g = \Re(\alpha_g) + (2\pi i)^{-1}(2\pi)\Im(\alpha_g)$$

we find that

$$x = \sum_{g\in G/<c>} \big(\Re(\alpha_g)(1+(-1)^r c) - (2\pi i)^{-1}2\pi\Im(\alpha_g)(1-(-1)^r c)\big) g^{-1}\sigma_N.$$

But $\sum_{g\in G/<c>} (2\pi i)^{-1}2\pi\Im(\alpha_g)(1-(-1)^r c) g^{-1}\sigma_N \in H_B(M)^- \otimes_{\mathbb{Q}} \mathbb{R}\cdot i$ and the central map in (5) sends $(2\pi i)^{-1}$ to 1. This implies the claimed result. □

The canonical comparison isomorphism $K_{\mathbb{C}} = H_{dR}(M)_{\mathbb{C}} \cong H_B(M)_{\mathbb{C}} = Y_{\Sigma,\mathbb{C}}$ which occurs in (4) sends any element β of K to

$$\sum_{g\in G} \sigma_N(g\beta)(2\pi i)^{-r} g^{-1}\sigma_N = \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times} \sigma_N\tau_a(\beta)(2\pi i)^{-r}\tau_a^{-1}\sigma_N$$

where $\tau_a(\zeta) = \zeta^a$ for each N-th root of unity ζ. In particular, after composing this comparison isomorphism with the isomorphism of Lemma 4.2 we find that ζ_f is sent to the following element of $Y_{\Sigma,\mathbb{R}}$

$$\sum_a \big(\Re(e^{2\pi i a/f}(2\pi i)^{-r})(1+(-1)^r c) - 2\pi\Im(e^{2\pi i a/f}(2\pi i)^{-r})(1-(-1)^r c)\big)\tau_a^{-1}\sigma_N$$

where the summation runs over all elements a of $(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1$. For each Dirichlet character η the η-component of this element is equal to $e_\eta\sigma_N$ multiplied by

$$\begin{aligned}&\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1}(2\pi)^{-r}\Re(e^{2\pi ia/f}i^{-r})\overline{\eta(a)}\cdot 2\\ =&\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1}(2\pi i)^{-r}(e^{2\pi ia/f}+(-1)^r e^{-2\pi ia/f})\overline{\eta(a)}\\ =&(2\pi i)^{-r}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}e^{2\pi ia/f}\overline{\eta(a)}\end{aligned}$$

if $\eta(-1)=(-1)^r$ (so $\delta-r$ is even), resp. by

$$\begin{aligned}&-2\pi\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1}(2\pi)^{-r}\Im(e^{2\pi ia/f}i^{-r})\overline{\eta(a)}\cdot 2\\ =&-2\pi\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1}(2\pi i)^{-r}\frac{e^{2\pi ia/f}-(-1)^r e^{-2\pi ia/f}}{i}\overline{\eta(a)}\\ =&(2\pi i)^{-(r-1)}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}e^{2\pi ia/f}\overline{\eta(a)}\end{aligned}$$

if $\eta(-1)=-(-1)^r$ (so $\delta-r$ is odd). Taking $f=f_\eta$ we find that the (η-part of the) morphism $(\vartheta_\infty^{\mathrm{loc}})':A_\mathbb{R}\otimes_A\Xi^{\mathrm{loc}}(M)\cong(A_\mathbb{R},0)$ defined in §2.2 sends

$$(12)\quad e_\eta\zeta_{f_\eta}\otimes_\mathbb{C}e_\eta\sigma_N^{-1}\mapsto\begin{cases}(2\pi i)^{-r}[K:\mathbb{Q}(f_\eta)]\tau(\bar\eta) & \text{if } \eta(-1)=(-1)^r\\ (2\pi i)^{-(r-1)}[K:\mathbb{Q}(f_\eta)]\tau(\bar\eta) & \text{if } \eta(-1)=-(-1)^r.\end{cases}$$

Now $\vartheta_\infty^{\mathrm{loc}}$ is defined to be the composite of $(\vartheta_\infty^{\mathrm{loc}})'$ and the sign factors ϵ_{dR} and ϵ_B that are defined at the end of §2.2. But it is easily seen that $e_{dR}=1$, that $(\epsilon_B)_\chi=-1$ for $\chi(-1)=(-1)^r$ and that $(\epsilon_B)_\chi=1$ otherwise. Thus, upon comparing (12) with the description of $\mathcal{E}({}_AM)_\eta^{-1}$ before Lemma 4.2 one verifies the statement of Proposition 4.1. □

4.2. Reduction to the p-primary component. By [9, Th. 5.2] we know that $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ belongs to the subgroup $K_0(\mathbb{Z}[G],\mathbb{Q})$ of $K_0(\mathbb{Z}[G],\mathbb{R})$. Recalling the direct sum decomposition $K_0(\mathbb{Z}[G],\mathbb{Q})\cong\bigoplus_\ell K_0(\mathbb{Z}_\ell[G],\mathbb{Q}_\ell)$ over all primes ℓ from [9, (13)], we may therefore prove Theorem 1.1 by showing that, for each prime ℓ, the projection $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])_\ell$ of $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ to $K_0(\mathbb{Z}_\ell[G],\mathbb{Q}_\ell)$ vanishes. Henceforth we therefore fix a prime number p and shall analyze $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])_p$.

We denote by

$$T_p:=\mathrm{Ind}_K^\mathbb{Q}\mathbb{Z}_p(r)\subset V_p:=\mathrm{Ind}_K^\mathbb{Q}\mathbb{Q}_p(r)=H_p(M)$$

the natural lattice in the p-adic realisation V_p of M. Then by combining the definition of $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K,\mathbb{Z}[G])$ from (10) (and (8)) together with the explicit description of Proposition 4.1 one finds that $T\Omega^{\rm loc}(\mathbb{Q}(r)_K, \mathbb{Z}[G])_p = 0$ if and only if

$$\mathbb{Z}_p[G]\cdot\epsilon(r)\epsilon(S,p)\cdot\theta'_p\circ\theta_p((\epsilon_\infty\beta_N\otimes\sigma_N^{-1},0)) = \Lambda_p(S,T_p)$$

where θ_p is as defined in §2.3, $\Lambda_p(S,T_p)$, θ'_p and $\epsilon(S,p)\in A_p^\times$ are as discussed in §2.5 and we have set $\epsilon(r) := \mathrm{Det}_A(-1 \mid K_{2r-1}(\mathcal{O}_K)^*\otimes_{\mathbb{Z}}\mathbb{Q})\in A^\times$.

Lemma 4.3. *We set*

$$\epsilon_p := \mathrm{Det}_{A_p}(2|V_p^+)\,\mathrm{Det}_{A_p}(2|V_p^-)^{-1}\in A_p^\times.$$

Then, with ϵ_∞ as defined in Proposition 4.1, there exists an element $u(r)$ of $\mathbb{Z}_p[G]^\times$ such that $\epsilon(r)\epsilon(S,p)\epsilon_\infty = u(r)\epsilon_p$.

Proof. We recall that $\epsilon(S,p)$ is a product of factors $\mathrm{Det}_{A_p}(-1|R\Gamma_{/f}(\mathbb{Q}_\ell,V_p))$. Further, the quasi-isomorphism $R\Gamma_{/f}(\mathbb{Q}_\ell,V_p)\cong R\Gamma_f(\mathbb{Q}_\ell,V_p^*(1))^*[-2]$ from [9, Lem. 12a)] implies that each such complex is quasi-isomorphic to a complex of the form $W\to W$ (indeed, this is clear if $\ell\neq p$ and is true in the case $\ell = p$ because the tangent space of the motive $\mathbb{Q}(1-r)_K$ vanishes for $r\geq 1$) and so one has $\epsilon(S,p)=1$.

We next note that if $\epsilon(r) := \sum_\chi \epsilon(r)_\chi e_\chi$ with $\epsilon(r)_\chi\in\{\pm1\}$, then the explicit structure of the $\mathbb{Q}[G]$-module $K_{2r-1}(\mathcal{O}_K)^*\otimes_{\mathbb{Z}}\mathbb{Q}$ (cf. [17, p. 86, p. 105]) implies that $\epsilon(r)_\chi = 1$ if either $r=1$ and χ is trivial or if $\chi(-1)=(-1)^r$, and that $\epsilon(r)_\chi = -1$ otherwise.

Thus, after recalling the explicit definitions of ϵ_∞ and ϵ_p, it is straightforward to check that the claimed equality $\epsilon(r)\epsilon(S,p)\epsilon_\infty = u(r)\epsilon_p$ is valid with $u(r) = -(-1)^r c$ where $c\in G$ is complex conjugation. □

The element ϵ_p in Lemma 4.3 is equal to the element ϵ_{V_p} that occurs in Proposition 7.2 below (with $V_p = \mathrm{Ind}_K^{\mathbb{Q}}\mathbb{Q}_p(r)$). Hence, upon combining Lemma 4.3 with the discussion which immediately precedes it and the result of Proposition 7.2 we may deduce that $T\Omega^{\rm loc}(\mathbb{Q}(r)_K,\mathbb{Z}[G])_p = 0$ if and only if

$$(13)\quad \mathbb{Z}_p[G]\cdot\theta_p((\beta_N\otimes\sigma_N^{-1},0)) = \left(\bigotimes_{\ell|Np}\mathrm{Det}^{-1}_{\mathbb{Z}_p[G]}R\Gamma(\mathbb{Q}_\ell,T_p)\right)\otimes_{\mathbb{Z}_p[G]}(T_p^{-1},-1).$$

Here we have set $T_p^{-1} := \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p,\mathbb{Z}_p[G])$ and also used the fact that, since T_p is a free rank one $\mathbb{Z}_p[G]$-module, one has $\mathrm{Det}^{-1}_{\mathbb{Z}_p[G]}(T_p) = (T_p^{-1},-1)$.

Now Shapiro's Lemma allows us to identify the complexes $R\Gamma(\mathbb{Q}_\ell,T_p)$ and $R\Gamma(\mathbb{Q}_\ell,V_p)$ with $R\Gamma(K_\ell,\mathbb{Z}_p(r))$ and $R\Gamma(K_\ell,\mathbb{Q}_p(r))$ respectively. Further, the complex $R\Gamma(K_p,\mathbb{Q}_p(r))$ is acyclic outside degree 1 for $r>1$, and for $r=1$ one has a natural exact sequence of $\mathbb{Q}_p[G]$-modules

$$(14)\qquad 0\to\hat{\mathcal{O}}_{K_p}^\times\to\hat{K}_p^\times\cong H^1(K_p,\mathbb{Q}_p(1))\xrightarrow{\rm val}\prod_{v|p}\mathbb{Q}_p\cong H^2(K_p,\mathbb{Q}_p(1))\to 0$$

where the first isomorphism is induced by Kummer theory and the second by the invariant map on the Brauer group. Our notation here is that $\hat{M} :=$

$(\varprojlim_n M/p^nM)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ for any abelian group M. We let

$$K_p = D_{dR}(V_p) \xrightarrow{\exp} H^1_f(K_p, \mathbb{Q}_p(r))$$

denote the exponential map of Bloch and Kato for the representation V_p of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. This map is bijective (since $r > 0$) and $H^1_f(K_p, \mathbb{Q}_p(r))$ coincides with $\hat{\mathcal{O}}^\times_{K_p}$ for $r = 1$ and with $H^1(K_p, \mathbb{Q}_p(r))$ for $r > 1$ (cf. [5]). Also, both source and target for the map exp are free A_p-modules of rank one. By using the sequence (14) for $r = 1$ we therefore find that for each $r \geq 1$ there exists an isomorphism of graded invertible A_p-modules of the form

$$\widetilde{\exp} : (K_p, 1) \xrightarrow{\exp} (H^1_f(K_p, \mathbb{Q}_p(r)), 1) \cong \mathrm{Det}^{-1}_{A_p} R\Gamma(K_p, \mathbb{Q}_p(r)). \tag{15}$$

For any subgroup $H \subseteq G$ we set

$$e_H := \sum_{\chi(H)=1} e_\chi = \frac{1}{|H|}\sum_{g\in H} g.$$

Also, for each prime ℓ we denote by J_ℓ and D_ℓ the inertia and decomposition groups of ℓ in G. For $x \in A_p$ we then set

$$e_\ell(x) := 1 + (x-1)e_{J_\ell} \in A_p$$

(so $x \mapsto e_\ell(x)$ is a multiplicative map that preserves the maximal $\mathbb{Z}_p$-order in A_p) and we denote by $\mathrm{Fr}_\ell \in G \subset A$ any choice of a Frobenius element.

Proposition 4.4. *We define an element $e_p^*(1 - p^{r-1}\,\mathrm{Fr}_p^{-1})$ of $A_p^\times$ by setting*

$$e_\chi e_p^*(1 - p^{r-1}\,\mathrm{Fr}_p^{-1}) = \begin{cases} e_\chi e_p(1 - p^{r-1}\,\mathrm{Fr}_p^{-1}), & \textit{if } r > 1 \textit{ or } \chi(D_p) \neq 1 \\ |D_p/J_p|^{-1} e_\chi, & \textit{otherwise.}\end{cases}$$

Then one has $T\Omega^{\mathrm{loc}}(\mathbb{Q}(r)_K, \mathbb{Z}[G])_p = 0$ if and only if

$$\mathbb{Z}_p[G] \cdot \prod_{\substack{\ell | N\\ \ell\neq p}} e_\ell(-\mathrm{Fr}_\ell^{-1})\, e_p(1 - \frac{\mathrm{Fr}_p}{p^r})^{-1} e_p^*(1 - p^{r-1}\,\mathrm{Fr}_p^{-1})\,\widetilde{\exp}((\beta_N, 1)) = \mathrm{Det}^{-1}_{\mathbb{Z}_p[G]} R\Gamma(K_p, \mathbb{Z}_p(r)). \tag{16}$$

Proof. It suffices to prove that (16) is equivalent to (13).
Now, by its definition in §2.3, the morphism θ_p which occurs in (13) is induced by taking the tensor product of the morphisms

$$\theta_p^{p\text{-part}} : A_p \otimes_A \Xi^{\mathrm{loc}}(M) \cong \mathrm{Det}^{-1}_{A_p} R\Gamma(K_p, \mathbb{Q}_p(r)) \otimes_{A_p} (V_p^{-1}, -1),$$

where we set $V_p^{-1} := \mathrm{Hom}_{A_p}(V_p, A_p)$, and for each prime $\ell \mid N$ with $\ell \neq p$

$$\theta_p^{\ell\text{-part}} : (A_p, 0) \cong \mathrm{Det}^{-1}_{A_p} R\Gamma(K_\ell, \mathbb{Q}_p(r)).$$

In addition, for $W = V_p$ the exact triangle (7) identifies with

$$K_p[-1] \to R\Gamma_f(\mathbb{Q}_p, V_p) \to \left(D_{\mathrm{cris}}(V_p) \xrightarrow{1-p^{-r}\,\mathrm{Fr}_p} D_{\mathrm{cris}}(V_p)\right)$$

(with this last complex concentrated in degrees 0 and 1), and there is a canonical quasi-isomorphism

$$R\Gamma_f(\mathbb{Q}_p, V_p^*(1))^*[-2] \cong \left(D_{\mathrm{cris}}(V_p) \xrightarrow{1-p^{r-1}\,\mathrm{Fr}_p^{-1}} D_{\mathrm{cris}}(V_p) \right),$$

where the latter complex is concentrated in degrees 1 and 2. The identity map on $D_{\mathrm{cris}}(V_p)$ therefore induces isomorphisms of graded invertible A_p-modules

$$(17)\quad (K_p, 1) \cong \mathrm{Det}_{A_p}^{-1} R\Gamma_f(\mathbb{Q}_p, V_p); \quad (A_p, 0) \cong \mathrm{Det}_{A_p} R\Gamma_f(\mathbb{Q}_p, V_p^*(1))^*[-2].$$

The morphism $\theta_p^{p\text{-part}}$ is thus induced by (17) and (6) together with the (elementary) comparison isomorphism

$$\gamma : Y_{\Sigma,p} = H_B(M)_p \cong H_p(M) = V_p$$

between the Betti and p-adic realizations of M. On the other hand, the isomorphism $\widetilde{\exp}$ arises by passing to the cohomology sequence of (6) and then also using the identifications in (14) if $r = 1$. Hence, from [8, Lem. 1, Lem. 2], one has

$$(18)\qquad \theta_p^{p\text{-part}} = e_p(1 - p^{-r}\,\mathrm{Fr}_p)^{-1} e_p^*(1 - p^{r-1}\,\mathrm{Fr}_p^{-1})\widetilde{\exp} \otimes_{A_p} \gamma^{-1}.$$

Now if $\ell \neq p$, then Proposition 7.1 below implies that

$$\mathrm{Det}_{A_p}(-\sigma_\ell \ell^{-1} | (V_p)_{I_\ell})^{-1} \cdot \theta_p^{\ell\text{-part}}((\mathbb{Z}_p[G], 0)) = \mathrm{Det}_{\mathbb{Z}_p[G]}^{-1} R\Gamma(K_\ell, \mathbb{Z}_p(r)).$$

Thus, since $\gamma(\sigma_N)$ is a $\mathbb{Z}_p[G]$-basis of T_p, we find that (13) holds if and only if the element

$$\prod_{\substack{\ell | N \\ \ell \neq p}} \mathrm{Det}_{A_p}(-\sigma_\ell \ell^{-1} | (V_p)_{I_\ell})\, e_p(1 - p^{-r}\,\mathrm{Fr}_p)^{-1} e_p^*(1 - p^{r-1}\,\mathrm{Fr}_p^{-1})\, \widetilde{\exp}((\beta_N, 1))$$

is a $\mathbb{Z}_p[G]$-basis of $\mathrm{Det}_{\mathbb{Z}_p[G]}^{-1} R\Gamma(K_p, \mathbb{Z}_p(r))$. But

$$\mathrm{Det}_{A_p}(-\sigma_\ell \ell^{-1} | (V_p)_{I_\ell}) = \mathrm{Det}_{A_p}(-\mathrm{Fr}_\ell^{-1}\, \ell^{r-1} | A_p \cdot e_{J_\ell}) = e_\ell(-\mathrm{Fr}_\ell^{-1}) e_\ell(\ell^{r-1})$$

and so Proposition 4.4 is implied by Lemma 4.5 below with u equal to the function which sends 0 to ℓ^{r-1} and all non-zero integers to 1. □

Lemma 4.5. *Fix a prime number $\ell \neq p$. If $u : \mathbb{Z} \to \mathbb{Z}_p[G]^\times$ is any function such that $\ell - 1$ divides $u(0) - u(1)$ in $\mathbb{Z}_p[G]$, then the element $\sum_\chi u(\mathrm{ord}_\ell(f_\chi))e_\chi$ is a unit of $\mathbb{Z}_p[G]$.*

Proof. If $\ell - 1$ divides $u(0) - u(1)$, then $\ell - 1$ divides $(u(1) - u(0))/u(1)u(0) = u(0)^{-1} - u(1)^{-1}$. It follows that the function u^{-1} also satisfies the hypothesis of the lemma and so it suffices to prove that the element $x_u := \sum_\chi u(\mathrm{ord}_\ell(f_\chi))e_\chi$ belongs to $\mathbb{Z}_p[G]$.

To this end, we let $J_\ell = J_{\ell,0} \subseteq G$ denote the inertia subgroup at ℓ and $J_{\ell,k} \subseteq J_{\ell,k-1} \subseteq \cdots \subseteq J_{\ell,1} \subseteq J_{\ell,0}$ its canonical filtration, so that a character χ satisfies $\mathrm{ord}_\ell(f_\chi) = k$ if and only if $\chi(J_{\ell,k}) = 1$ (and $\chi(J_{\ell,k-1}) \neq 1$ if $k > 0$). Then

$$x_u = \sum_{k=0}^{k=K} u(k)(e_{J_{\ell,k}} - e_{J_{\ell,k-1}}) = \sum_{k=0}^{k=K-1} (u(k) - u(k+1))e_{J_{\ell,k}} + u(K)e_{J_{\ell,K}}$$

where $K = \mathrm{ord}_\ell(N)$ and we have set $e_{J_{\ell,-1}} := 0$. For $k \geq 1$ one has $e_{J_{\ell,k}} \in \mathbb{Z}_p[G]$ since $J_{\ell,k}$ is an ℓ-group and $\ell \neq p$. If $K = 0$, then $e_{J_{\ell,0}} = e_{J_{\ell,K}} = 1$ also lies in $\mathbb{Z}_p[G]$. Otherwise the assumptions that $\ell - 1$ divides $u(0) - u(1)$ and that $\ell \neq p$ combine to imply that

$$(u(0) - u(1))e_{J_{\ell,0}} = \frac{u(0) - u(1)}{(\ell - 1)\ell^{K-1}} \sum_{g \in J_{\ell,0}} g \in \mathbb{Z}_p[G],$$

as required. □

5. Local Iwasawa theory

As preparation for our proof of (16) we now prove a result in Iwasawa theory. We write

$$N = N_0 p^\nu; \qquad \nu \geq 0,\ p \nmid N_0.$$

For any natural number n we set $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. We also let $\mathbb{Q}(\zeta_{Np^\infty})$ denote the union of the fields $\mathbb{Q}(\zeta_{Np^m})$ over $m \geq 0$ and set $G_{Np^\infty} := \mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})$. We then define

$$\Lambda := \mathbb{Z}_p[[G_{Np^\infty}]] = \varprojlim_n \mathbb{Z}_p[G_{Np^n}] \cong \mathbb{Z}_p[G_{N_0\tilde{p}}][[T]].$$

Here we have set $\tilde{p} := p$ for odd p and $\tilde{p} := 4$ for $p = 2$, and the isomorphism depends on a choice of topological generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q}(\zeta_{N_0\tilde{p}})) \cong \mathbb{Z}_p$. We also set

$$T_p^\infty := \varprojlim_n \mathrm{Ind}_{\mathbb{Q}(\zeta_{Np^n})}^{\mathbb{Q}} \mathbb{Z}_p(r).$$

This is a free rank one Λ-module upon which the absolute Galois group $G_\mathbb{Q} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts by the character $(\chi_{\mathrm{cyclo}})^r\tau^{-1}$ where $\chi_{\mathrm{cyclo}} : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ is the cyclotomic character and $\tau : G_\mathbb{Q} \to G_{Np^\infty} \subseteq \Lambda^\times$ is the tautological character. In this section we shall describe (in Proposition 5.2) a basis of the invertible Λ-module $\mathrm{Det}_\Lambda^{-1} R\Gamma(\mathbb{Q}_p, T_p^\infty)$.

We note first that the cohomology of $R\Gamma(\mathbb{Q}_p, T_p^\infty)$ is naturally isomorphic to

$$H^i(\mathbb{Q}_p, T_p^\infty) \cong \begin{cases} (\varprojlim_n \mathbb{Q}(\zeta_{Np^n})_p^\times/p^n) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(r-1) & i = 1 \\ \prod_{v|p} \mathbb{Z}_p(r-1) & i = 2 \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

where the limit is taken with respect to the norm maps (and $\mathbb{Q}(\zeta_{Np^n})_p = \mathbb{Q}(\zeta_{Np^n}) \otimes_\mathbb{Q} \mathbb{Q}_p$ is a finite product of local fields). The valuation map induces a natural short exact sequence

$$0 \to \tilde{Z} := \varprojlim_n \mathcal{O}^\times_{\mathbb{Q}(\zeta_{Np^n})_p}/p^n \to \varprojlim_n \mathbb{Q}(\zeta_{Np^n})_p^\times/p^n \xrightarrow{\mathrm{val}} \prod_{v|p} \mathbb{Z}_p \to 0 \tag{20}$$

and in addition Perrin-Riou has constructed an exact sequence [34, Prop. 4.1.3]

$$0 \to \prod_{v|p} \mathbb{Z}_p(r) \to \tilde{Z}(r-1) \xrightarrow{\theta_r^{PR}} R \to \prod_{v|p} \mathbb{Z}_p(r) \to 0 \tag{21}$$

where

$$R := \{f \in \mathbb{Z}[\zeta_{N_0}]_p[[X]] \mid \psi(f) := \sum_{\zeta^p=1} f(\zeta(1+X)-1) = 0\}$$

and $\mathbb{Z}[\zeta_{N_0}]_p$ denotes the finite étale $\mathbb{Z}_p$-algebra $\mathbb{Z}[\zeta_{N_0}] \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We remark that, whilst p is assumed to be odd in [34] the same arguments show that the sequence (21) exists and is exact also in the case $p = 2$. The $\mathbb{Z}_p$-module R carries a natural continuous G_{Np^∞}-action [34, 1.1.4], and with respect to this action all maps in (19), (20) and (21) are Λ-equivariant. In addition, if $r = 1$, then the exact sequence (21) is due to Coleman and the map θ_1^{PR} is given by

$$\theta_1^{PR}(u) = \left(1 - \frac{\phi}{p}\right) \log(f_u) \tag{22}$$

where f_u is the (unique) Coleman power series of the norm compatible system of units u with respect to $(\zeta_{p^n})_{n\geq 1}$ and one has $\phi(f_u)(X) = f_u^{\mathrm{Fr}_p}((1+X)^p - 1)$.

Lemma 5.1. *The Λ-module R is free of rank one with basis*

$$\beta_{N_0}^\infty := \xi_{N_0}(1+X); \qquad \xi_{N_0} := \sum_{N_1|d|N_0} \zeta_d$$

where $N_1 := \prod_{\ell|N_0} \ell$.

Proof. The element ξ_{N_0} is a $\mathbb{Z}_p[G_{N_0}]$-basis of $\mathbb{Z}[\zeta_{N_0}]_p$. Indeed, this observation (which is due originally to Leopoldt [30]) can be explicitly deduced from [31, Th. 2] after observing that the idempotents ε_d of loc. cit. belong to $\mathbb{Z}_p[G_{N_0}]$. On the other hand, Perrin-Riou shows in [33, Lem. 1.5] that if W is the ring of integers in any finite unramified extension of $\mathbb{Z}_p$, then $W[[X]]^{\psi=0}$ is a free rank one $W[[G_{p^\infty}]]$-module with basis $1+X$ (her proof applies for all primes p, including $p = 2$). Since $\mathbb{Z}[\zeta_{N_0}]_p$ is a finite product of such rings W and $G_{Np^\infty} \cong G_{N_0} \times G_{p^\infty}$, the result follows. □

Proposition 5.2. *Let Q be the total ring of fractions of Λ (so Q is a finite product of fields). Using Lemma 5.1, we regard $\beta_{N_0}^\infty$ as a Q-basis of*

$$R \otimes_\Lambda Q \cong \tilde{Z}(r-1) \otimes_\Lambda Q \cong H^1(\mathbb{Q}_p, T_p^\infty) \otimes_\Lambda Q \cong (\mathrm{Det}_\Lambda^{-1} R\Gamma(\mathbb{Q}_p, T_p^\infty)) \otimes_\Lambda Q,$$

where the first isomorphism is induced by $(\theta_r^{PR} \otimes_\Lambda Q)^{-1}$, the second by (19) and the $(r-1)$-fold twist of (20) and the third by (19). Then one has

$$\Lambda \cdot \beta_{N_0}^\infty = \mathrm{Det}_\Lambda^{-1} R\Gamma(\mathbb{Q}_p, T_p^\infty) \subset (\mathrm{Det}_\Lambda^{-1} R\Gamma(\mathbb{Q}_p, T_p^\infty)) \otimes_\Lambda Q.$$

Proof. We note first that, since Λ is noetherian, Cohen-Macauley and semilocal, it is enough to prove that $\beta_{N_0}^\infty$ is a $\Lambda_{\mathfrak{q}}$-basis of $\mathrm{Det}_{\Lambda_{\mathfrak{q}}}^{-1} R\Gamma(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}}$ for all height one prime ideals $\mathfrak{q}$ of Λ (see, for example, [17, Lem. 5.7]). In view of (19), (20) and (21) this claim is immediate for prime ideals $\mathfrak{q}$ which are not in the support of the (torsion) Λ-modules $\prod_{v|p} \mathbb{Z}_p(r-1)$ and $\prod_{v|p} \mathbb{Z}_p(r)$. On the other hand, since these modules are each p-torsion free, any prime $\mathfrak{q}$ which does lie in their support is *regular* in the sense that $p \notin \mathfrak{q}$ (see, for example, [17, p. 90]). In particular, in any such case $\Lambda_{\mathfrak{q}}$ is a discrete valuation ring and so it suffices to check cancellation of the Fitting ideals of the occurring torsion modules. But the Fitting ideal of $H^2(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}}$ cancels against that of the module $(\prod_{v|p}\mathbb{Z}_p(r-1))_{\mathfrak{q}}$ which occurs in the $(r-1)$-fold twist of (20), whilst the Fitting ideals of the kernel and cokernel of θ_r^{PR} obviously cancel against each other. □

6. Descent calculations

In this section we deduce equality (16) as a consequence of Proposition 5.2 and thereby finish the proof of Theorem 1.1.

At the outset we note that the natural ring homomorphism

$$\Lambda \to \mathbb{Z}_p[G] \subseteq \mathbb{Q}_p[G] = \prod_\chi \mathbb{Q}_p(\chi) \tag{23}$$

induces an isomorphism of perfect complexes of $\mathbb{Z}_p[G]$-modules

$$R\Gamma(\mathbb{Q}_p, T_p^\infty) \otimes^{\mathbb{L}}_\Lambda \mathbb{Z}_p[G] \cong R\Gamma(\mathbb{Q}_p, T_p)$$

and hence also an isomorphism of determinants

$$\operatorname{Det}^{-1}_\Lambda R\Gamma(\mathbb{Q}_p, T_p^\infty) \otimes_\Lambda \mathbb{Z}_p[G] \cong \operatorname{Det}^{-1}_{\mathbb{Z}_p[G]} R\Gamma(\mathbb{Q}_p, T_p).$$

Taken in conjunction with Proposition 5.2, this shows that $(\beta_{N_0}^\infty \otimes_\Lambda 1, 1)$ is a $\mathbb{Z}_p[G]$-basis of the graded module $\operatorname{Det}^{-1}_{\mathbb{Z}_p[G]} R\Gamma(\mathbb{Q}_p, T_p)$. Hence, if we define an element u of $\mathbb{Q}_p[G]^\times$ by means of the equality

$$\prod_{\ell | N_0} e_\ell(-\operatorname{Fr}_\ell^{-1})\, e_p(1 - \frac{\operatorname{Fr}_p}{p^r})^{-1} e_p^*(1 - p^{r-1}\operatorname{Fr}_p^{-1})\, \widetilde{\exp}((\beta_N, 1)) \tag{24}$$
$$= (u \cdot \beta_{N_0}^\infty \otimes_\Lambda 1, 1)$$

then it is clear that the equality (16) is valid if and only if $u \in \mathbb{Z}_p[G]^\times$.

6.1. The unit u'. To prove that the element u defined in (24) belongs to $\mathbb{Z}_p[G]^\times$ we will compare it to the unit described by the following result.

Lemma 6.1. *There exists a unit $u' \in \mathbb{Z}_p[G]^\times$ such that for any integer k with $0 \le k \le \nu$ and any $\mathbb{Q}_p$-rational character χ of G the element $e_\chi(\zeta_{p^k}\xi_{N_0}^{\operatorname{Fr}_p^{-k}})$ is equal to*

$$\begin{cases} \chi(u')\prod_{\ell|N_0, \ell\nmid f_\chi}\frac{1}{\ell-1}\prod_{\ell|N_0} e_\ell(-\operatorname{Fr}_\ell^{-1}) e_\chi\zeta_{f_\chi}, & \text{if } k = \operatorname{ord}_p(f_\chi) \\ \chi(u')(-\operatorname{Fr}_p^{-1})\prod_{\ell|N, \ell\nmid f_\chi}\frac{1}{\ell-1}\prod_{\ell|N_0} e_\ell(-\operatorname{Fr}_\ell^{-1}) e_\chi\zeta_{f_\chi}, & \text{if } k=1,\ \operatorname{ord}_p(f_\chi)=0 \\ 0, & \text{otherwise.} \end{cases}$$

Proof. For $d \mid N_0$ and $k \ge 0$ we set $d_k := p^k d$ and

$$a(d) := (d, 1) \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times \times (\mathbb{Z}/N_0\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \cong G$$

so that $\zeta_{p^k}\zeta_d^{\mathrm{Fr}_p^{-k}} = \zeta_{d_k}^{a(d)}$. Since $\xi_{N_0} = \sum_{N_1|d|N_0} \zeta_d$ Lemma 6.2 below implies

$$e_\chi(\zeta_{p^k}\xi_{N_0}^{\mathrm{Fr}_p^{-k}}) = \sum_{N_1|d|N_0, f_\chi|d_k} \frac{\phi(f_\chi)}{\phi(d_k)}\mu(\frac{d_k}{f_\chi})\chi^{-1}(\frac{d_k}{f_\chi})\chi(a(d))e_\chi\zeta_{f_\chi}. \tag{25}$$

The only non-vanishing summands in (25) are those for which the quotient d_k/f_χ is both square-free and prime to f_χ. Given the nature of the summation condition there is a unique such summand corresponding to

$$d_k/f_\chi = \begin{cases} \prod_{\ell|N_0, \ell\nmid f_\chi} \ell, & \text{if } k = \mathrm{ord}_p(f_\chi) \\ \prod_{\ell|N, \ell\nmid f_\chi} \ell, & \text{if } k = 1 \text{ and } \mathrm{ord}_p(f_\chi) = 0. \end{cases}$$

If neither of these conditions on k and $\mathrm{ord}_p(f_\chi)$ is satisfied, then $e_\chi(\zeta_{p^k}\xi_{N_0}^{\mathrm{Fr}_p^{-k}}) = 0$. By using the multiplicativity of μ, ϕ and χ and the equalities $\mu(\ell) = -1$ and $\phi(\ell) = \ell - 1$ we then compute that (25) is equal to

$$\begin{cases} \chi(a(d_\chi))\prod_{\ell|N_0,\ell\nmid f_\chi}\left(\frac{1}{\ell-1}(-\chi^{-1}(\ell))\right)e_\chi\zeta_{f_\chi}, & \text{if } k = \mathrm{ord}_p(f_\chi) \\ \chi(a(d_\chi))\prod_{\ell|N,\ell\nmid f_\chi}\left(\frac{1}{\ell-1}(-\chi^{-1}(\ell))\right)e_\chi\zeta_{f_\chi}, & \text{if } k = 1, \mathrm{ord}_p(f_\chi) = 0 \\ 0, & \text{otherwise} \end{cases}$$

where d_χ is the index of the unique nonvanishing summand in (25), i.e. $d_\chi = f_{\chi,0}\prod_{\ell|N_0,\ell\nmid f_\chi}\ell$ with $f_{\chi,0}$ the prime to p-part of f_χ. Now the element

$$u' := \sum_\chi \chi\big(a(d_\chi)\big)e_\chi \in \mathbb{Q}_p[G]^\times$$

belongs to $\mathbb{Z}_p[G]^\times$ by Lemma 4.5 (indeed the function $d \mapsto a(d)$ is multiplicative, $d_\chi = d(\mathrm{ord}_\ell(f_\chi))$ is a function of $\mathrm{ord}_\ell(f_\chi)$ only and satisfies $d(0) = d(1)$ as such). From here the explicit description of Lemma 6.1 follows because the definition of e_ℓ ensures that $\prod_{\ell|N_0,\ell\nmid f_\chi}\big(-\chi^{-1}(\ell)\big) = \prod_{\ell|N_0} e_\ell(-\mathrm{Fr}_\ell^{-1})e_\chi$. □

Lemma 6.2. *For any $\mathbb{Q}$-rational (resp. $\mathbb{Q}_p$-rational) character χ of $G \cong (\mathbb{Z}/N\mathbb{Z})^\times$, any $d \mid N$ and any* primitive *d-th root of unity ζ_d^a we have*

$$e_\chi\zeta_d^a = \begin{cases} 0, & \text{if } f_\chi \nmid d \\ \dfrac{\phi(f_\chi)}{\phi(d)}\mu(\dfrac{d}{f_\chi})\chi^{-1}(\dfrac{d}{f_\chi})\chi(a)e_\chi\zeta_{f_\chi}, & \text{if } f_\chi \mid d \end{cases} \tag{26}$$

in K (resp. K_p). Here $\phi(m)$ is Euler's ϕ-function, $\mu(m)$ is the Möbius function and $\chi(m) = 0$ if $(m, f_\chi) > 1$.

Proof. Recall that we view a $\mathbb{Q}$-rational character χ as the tautological homomorphism $G \to A^\times \to \mathbb{Q}(\chi)^\times$ to the field $\mathbb{Q}(\chi) := e_\chi A$ which is a direct ring factor of A. Thus, any complex embedding $j : \mathbb{Q}(\chi) \to \mathbb{C}$ induces a complex character $j\chi = \eta : G \to \mathbb{C}^\times$. We set $b := N/d$. Then under the $\mathbb{C}$-linear map $\sigma_N : K_\mathbb{C} \to \mathbb{C}$ the element

$$(j\,e_\chi)\zeta_d^a = e_\eta\zeta_N^{ab} = \frac{1}{|G|}\sum_{g\in G}\eta(g^{-1})g\,\zeta_N^{ab} = \frac{1}{\phi(N)}\sum_{x \bmod N}\bar{\eta}(x)\zeta_N^{xab} \in K_\mathbb{C}$$

is sent to the general Gaussian sum $\phi(N)^{-1}\tau(\bar{\eta}_N|\zeta_N^{ab})$ in the notation of Hasse [22, §20.1]. By [22, §20.2.IV] we have

$$\tau(\bar{\eta}_N|\zeta_N^{ab}) = \begin{cases} 0, & f_\eta \nmid d \\ \frac{\phi(N)}{\phi(d)}\mu(\frac{d}{f_\chi})\bar{\eta}(\frac{d}{f_\chi})\eta(a)\tau(\bar{\eta}), & f_\eta \mid d \end{cases}$$

where the Gaussian sum $\tau(\eta)$ attached to the character η is as defined in (11). For $d = f_\chi$ and $\zeta_d^a = \zeta_{f_\chi}$ we find $\tau(\bar{\eta}) = \phi(f_\chi)\sigma_N((j\, e_\chi)\zeta_{f_\chi})$. This yields the image of (26) under σ_N. Note that $K_{\mathbb{C}} \cong \prod_{g\in G}\mathbb{C}$ via $x \mapsto (\sigma_N gx)_{g\in G}$ and both sides of (26) are multiplied by $\chi(g)$ after applying g. Since $j\chi(g) = \eta(g)$ is a scalar and σ_N is $\mathbb{C}$-linear we find that (26) holds in $K_{\mathbb{C}}$, hence in K, hence also in K_p for all p. □

Given Lemma 6.1, our proof of Theorem 1.1 will be complete if we can show that $uu' \in \mathbb{Z}_p[G]^\times$. Recalling Lemma 4.5 it thus suffices to prove that for each $\mathbb{Q}_p$-rational character χ one has

$$\chi(uu') = \frac{f_{\chi,0}^{r-1}\prod_{\ell|N_0,\ell\nmid f_\chi}(\ell-1)}{[\mathbb{Q}(\zeta_{N_0}):\mathbb{Q}(\zeta_{f_{\chi,0}})]} \tag{27}$$

where $f_{\chi,0}$ denotes for the prime to p-part of f_χ. (In this regard note that the expression on the right hand side of (27) belongs to $\mathbb{Z}_p^\times$.)

We shall use explicit descent computations to prove that (27) is a consequence of the definition of u in (24). To this end, for each $\mathbb{Q}_p$-character χ of G we let $\mathfrak{q}_\chi$ denote the kernel of the homomorphism $\Lambda \to \mathbb{Q}_p(\chi)$ in (23). Then $\mathfrak{q}_\chi$ is a regular prime ideal of Λ and $\Lambda_{\mathfrak{q}_\chi}$ is a discrete valuation ring with residue field $\mathbb{Q}_p(\chi)$. To apply [17, Lem. 5.7] we need to describe a $\Lambda_{\mathfrak{q}_\chi}$-basis of $H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}$ and for this purpose we find it convenient to split the argument into several different cases.

6.2. THE CASE $r > 1$ OR $\chi(D_p) \neq 1$. In this subsection we shall prove (27) for all characters χ except those which are trivial on D_p in the case that $r = 1$. In particular, the material of this section completes the proof of Theorem 1.1 in the case $r > 1$.

We note first that if either $r > 1$ or $\chi(D_p) \neq 1$, then $\mathfrak{q}_\chi$ does not lie in the support of either $\prod_{v|p}\mathbb{Z}_p(r-1)$ or $\prod_{v|p}\mathbb{Z}_p(r)$. Hence, modulo the identifications made in Proposition 5.2, it follows from (19), (20) and (21) that $\beta_{N_0}^\infty$ is a $\Lambda_{\mathfrak{q}_\chi}$-basis of $H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi} = (\mathrm{Det}_\Lambda^{-1} R\Gamma(\mathbb{Q}_p, T_p^\infty))_{\mathfrak{q}_\chi}$ and that $\beta_{N_0}^\infty \otimes_{\Lambda_{\mathfrak{q}_\chi}} 1$ is equal to the image of $\beta_{N_0}^\infty$ under the composite map

$$H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi} \to H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi} \otimes_{\Lambda_{\mathfrak{q}_\chi}} \mathbb{Q}_p(\chi) \cong H^1(K_p, \mathbb{Q}_p(r)) \otimes_{A_p} \mathbb{Q}_p(\chi)$$

where the isomorphism is induced by the vanishing of $H^2(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}$ (cf. [17, Lem. 5.7]).

6.2.1. *The descent diagram.* By an obvious semi-local generalization of the argument of [1, §2.3.2] there exists a commutative diagram of Λ-modules

(28)
$$\begin{tikzcd}
\tilde{Z}(r-1) \arrow[r, "\theta_r^{PR}"] \arrow[d] & R \arrow[d, "\Xi_{r,\nu}"'] \\
H^1(K_p, \mathbb{Q}_p(r)) & K_p \arrow[l, "(r-1)!\exp"']
\end{tikzcd}$$

where $\nu = \operatorname{ord}_p(N)$ is as defined at the beginning of §5,

$$\Xi_{r,\nu}(f) = \begin{cases} \sum\limits_{k=1}^{\nu} p^{rk-\nu} f^{\mathrm{Fr}_p^{-k}}(\zeta_{p^k}-1) + p^{-\nu}(1-\frac{\mathrm{Fr}_p}{p^r})^{-1} f(0), & \nu \geq 1 \\ \mathrm{Tr}_{K(\zeta_p)/K}(\Xi_{r,1}(f)), & \nu = 0 \end{cases}$$

is the map of [1, Lem. 2.2.2] and the choice of Frobenius element $\mathrm{Fr}_p \in G \cong G_{N_0} \times G_{p^\nu}$ is that which acts trivially on p-power roots of unity. (We are grateful to Laurent Berger for pointing out that the methods of [3] show that the diagram (28) commutes even in the case $p = 2$.)
Now for $f = \beta_{N_0}^\infty = \xi_{N_0}(1+X)$ this formula gives

$$\Xi_{r,\nu}(\beta_{N_0}^\infty) = \begin{cases} \sum\limits_{k=1}^{\nu} p^{rk-\nu}\zeta_{p^k}\,\mathrm{Fr}_p^{-k}\,\xi_{N_0} + p^{-\nu}(1-\dfrac{\mathrm{Fr}_p}{p^r})^{-1}\xi_{N_0}, & \nu \geq 1 \\ \mathrm{Tr}_{K(\zeta_p)/K}\left(p^{r-1}\zeta_p\,\mathrm{Fr}_p^{-1} + \dfrac{1}{p}(1-\dfrac{\mathrm{Fr}_p}{p^r})^{-1}\right)\xi_{N_0} = & \\ \left(-p^{r-1}\,\mathrm{Fr}_p^{-1} + \dfrac{p-1}{p}(1-\dfrac{\mathrm{Fr}_p}{p^r})^{-1}\right)\xi_{N_0} = & \\ (1-\dfrac{\mathrm{Fr}_p}{p^r})^{-1}(1-p^{r-1}\,\mathrm{Fr}_p^{-1})\xi_{N_0}, & \nu = 0. \end{cases}$$

In addition, since either $r > 1$ or $\chi(D_p) \neq 1$, one has $e_\chi \exp = e_\chi \widetilde{\exp}$ and so the commutativity of (28) implies that the e_χ-projection of the defining equality (24) is equivalent to an equality in $e_\chi K_p$ of the form

$$\begin{aligned} (29)\qquad & \prod_{\ell \mid N_0} e_\ell(-\mathrm{Fr}_\ell^{-1})\, e_p(1-\frac{\mathrm{Fr}_p}{p^r})^{-1} e_p(1-p^{r-1}\,\mathrm{Fr}_p^{-1}) e_\chi \beta_N \\ &= \chi(u)(r-1)!\left(\sum_{k=1}^{\nu} p^{rk-\nu} e_\chi(\zeta_{p^k}\xi_{N_0}^{\mathrm{Fr}_p^{-k}}) + p^{-\nu}\left(1-\frac{\mathrm{Fr}_p}{p^r}\right)^{-1} e_\chi \xi_{N_0}\right) \end{aligned}$$

if $\nu \geq 1$, resp.

$$(30)\qquad \prod_{\ell \mid N_0} e_\ell(-\mathrm{Fr}_\ell^{-1}) e_\chi \beta_N = \chi(u)(r-1)! e_\chi \xi_{N_0}$$

if $\nu = 0$.

6.2.2. *The case* $\mathrm{ord}_p(f_\chi) > 0$. In this case $\nu > 0$ and $e_p(x)e_\chi = e_\chi$ for all $x \in A_p^\times$ and so we may leave out all factors of the form $e_p(-)$ on the left hand side of (29). In addition, Lemma 6.1 implies that the only non-vanishing term in the summation on the right hand side of (29) is that corresponding to $k = \mathrm{ord}_p(f_\chi)$ and moreover that (29) is equivalent to an equality

$$e_\chi\beta_N = \chi(uu')(r-1)!p^{rk-\nu} \prod_{\ell | N_0, \ell\nmid f_\chi} \frac{1}{\ell - 1} e_\chi \zeta_{f_\chi}.$$

Now, since $k = \mathrm{ord}_p(f_\chi)$ and $\nu = \mathrm{ord}_p(N)$, we have

$$p^{rk-\nu} \prod_{\ell | N_0, \ell\nmid f_\chi} \frac{1}{\ell-1} = \frac{[\mathbb{Q}(\zeta_{N_0}) : \mathbb{Q}(\zeta_{f_{\chi,0}})]}{f_{\chi,0}^{r-1} \prod_{\ell|N_0,\ell\nmid f_\chi}(\ell-1)} \frac{f_\chi^{r-1}}{[K : \mathbb{Q}(\zeta_{f_\chi})]}.$$

To deduce the required equality (27) from the last two displayed formulas one need only substitute the expression for $e_\chi\beta_N$ given in Proposition 4.1.

6.2.3. *The case* $\mathrm{ord}_p(f_\chi) = 0$ *and* $\nu > 0$. In this case Lemma 6.1 shows that the only non-zero terms in the summation on the right hand side of (29) are those which correspond to $k = 0$ and $k = 1$. Moreover, one has $e_p(x)e_\chi = xe_\chi$ for $x \in A_p^\times$. By Lemma 6.1, equation (29) is thus equivalent to

$$(31) \quad \left(1 - \frac{\mathrm{Fr}_p}{p^r}\right)^{-1} (1 - p^{r-1}\,\mathrm{Fr}_p^{-1}) e_\chi\beta_N =$$
$$\chi(uu')(r-1)! \prod_{\ell|N_0,\ell\nmid f_\chi} \frac{1}{\ell-1} \left(\frac{p^{r-\nu}}{p-1}(-\,\mathrm{Fr}_p^{-1}) + p^{-\nu}\left(1 - \frac{\mathrm{Fr}_p}{p^r}\right)^{-1}\right) e_\chi\zeta_{f_\chi}.$$

But

$$\begin{aligned} &\frac{p^{r-\nu}}{p-1}(-\,\mathrm{Fr}_p^{-1}) + p^{-\nu}\left(1 - \frac{\mathrm{Fr}_p}{p^r}\right)^{-1} \\ =&\frac{p^{-\nu+1}}{p-1}\left(1 - \frac{\mathrm{Fr}_p}{p^r}\right)^{-1}\left(p^{r-1}(-\,\mathrm{Fr}_p^{-1})\left(1 - \frac{\mathrm{Fr}_p}{p^r}\right) + \frac{p-1}{p}\right) \\ =&\frac{1}{\phi(p^\nu)}\left(1 - \frac{\mathrm{Fr}_p}{p^r}\right)^{-1}(1 - p^{r-1}\,\mathrm{Fr}_p^{-1}) \end{aligned}$$

and so (31) implies that

$$e_\chi\beta_N = \chi(uu')(r-1)!\frac{1}{\phi(p^\nu)} \prod_{\ell|N_0,\ell\nmid f_\chi} \frac{1}{\ell-1} e_\chi\zeta_{f_\chi}.$$

The required equality (27) follows from this in conjunction with the equality

$$\frac{1}{\phi(p^\nu)} \prod_{\ell|N_0,\ell\nmid f_\chi} \frac{1}{\ell-1} = \frac{[\mathbb{Q}(\zeta_{N_0}) : \mathbb{Q}(\zeta_{f_{\chi,0}})]}{f_{\chi,0}^{r-1} \prod_{\ell|N_0,\ell\nmid f_\chi}(\ell-1)} \frac{f_\chi^{r-1}}{[K : \mathbb{Q}(\zeta_{f_\chi})]}$$

and the expression for $e_\chi\beta_N$ given in Proposition 4.1.

6.2.4. *The case* $\nu = \mathrm{ord}_p(N) = 0$. In this case (27) results directly upon substituting the formulas of Proposition 4.1 and Lemma 6.1 (with $k = 0$) into (30).

6.3. The case $r = 1$ and $\chi(D_p) = 1$. In this case $\mathfrak{q}_\chi$ lies in the support of $\prod_{v|p} \mathbb{Z}_p(r-1)$ (but not of $\prod_{v|p} \mathbb{Z}_p(r)$) and $\beta^\infty_{N_0}$ is not a $\Lambda_{\mathfrak{q}_\chi}$-basis of $H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}$. We fix a generator γ of $\mathbb{Z}_p \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})/K(\zeta_p)) \subseteq G_{Np^\infty}$ and then define a uniformizer of $\Lambda_{\mathfrak{q}_\chi}$ by setting

$$\varpi := 1 - \gamma.$$

The p-adic places of the fields $K = \mathbb{Q}(\zeta_{N_0 p^\nu})$ and $\mathbb{Q}(\zeta_{N_0 p^\infty})$ are in natural bijection. We fix one such place v_0 and set

$$\begin{aligned}\eta^\infty := (1 - \zeta_{p^n})_{n \geq 1} \in \ & \varprojlim_n (\mathbb{Q}(\zeta_{N_0 p^n})^\times_{v_0})/p^n \\ & \subseteq \varprojlim_n \prod_{v|p} (\mathbb{Q}(\zeta_{N_0 p^n})^\times_v)/p^n = H^1(\mathbb{Q}_p, T_p^\infty).\end{aligned}$$

Then the image $\bar{\eta}^\infty$ of η^∞ in

$$H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}/\varpi \subseteq H^1(K_p, \mathbb{Q}_p(1)) \otimes_{A_p} \mathbb{Q}_p(\chi) =: H^1(K_p, \mathbb{Q}_p(1))_\chi$$

coincides with that of $p \in \mathbb{Q}(\zeta_{N_0})^\times_{v_0}$ and so is non-zero. In particular therefore, η^∞ is a $\Lambda_{\mathfrak{q}_\chi}$-basis of $H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}$. Now, by [17, Lem. 5.7] there is an exact sequence

$$0 \to H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}/\varpi \to H^1(K_p, \mathbb{Q}_p(1))_\chi \xrightarrow{\beta} H^2(K_p, \mathbb{Q}_p(1))_\chi \to 0$$

where β is the χ-projection of the composite homomorphism

$$H^1(K_p, \mathbb{Q}_p(1)) \cong \hat{K}_p^\times \to \prod_{v|p} \mathbb{Q}_p \cong H^2(K_p, \mathbb{Q}_p(1)); \quad u_v \to \frac{\mathrm{Tr}_{K_v/\mathbb{Q}_p}(\log_p(u_v))}{\log_p(\chi_{\mathrm{cyclo}}(\gamma))}$$

(see [17, Lem. 5.8] and its proof). This exact sequence induces an isomorphism

$$\phi_\varpi : \mathrm{Det}^{-1}_{\mathbb{Q}_p(\chi)} R\Gamma(\mathbb{Q}_p, V_p)_\chi \cong H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi}/\varpi$$

and [17, Lem. 5.7] implies that, modulo the identifications made in Proposition 5.2, one has

$$\bar{\lambda} \cdot \beta^\infty_{N_0} \otimes_{\Lambda_{\mathfrak{q}_\chi}} 1 = \phi_\varpi^{-1}(\bar{\eta}^\infty) \tag{32}$$

where the elements $\lambda \in \Lambda^\times_{\mathfrak{q}_\chi}$ and $e \in \mathbb{Z}$ are defined by the equality

$$(\theta_1^{PR})^{-1}_{\mathfrak{q}_\chi}(\lambda \cdot \beta^\infty_{N_0}) = \varpi^e \eta^\infty \in H^1(\mathbb{Q}_p, T_p^\infty)_{\mathfrak{q}_\chi} \tag{33}$$

and $\bar{\lambda}$ denotes the image of λ in $\Lambda_{\mathfrak{q}_\chi}/\varpi$. This description of $\bar{\eta}^\infty$ implies that

$$\mathrm{val}(\bar{\eta}^\infty) = \beta(\exp(e_\chi b)),$$

where 'val' is the normalized valuation map which occurs in (14) and

$$b := |D_p|^{-1} \log_p(\chi_{\mathrm{cyclo}}(\gamma)) \in \mathbb{Q}_p \subseteq K_{v_0} \subseteq \prod_{v|p} K_v = K_p.$$

Lemma 6.3. *The element λ that is defined in (33) belongs to Λ and in $\mathbb{Q}(\zeta_{N_0})_p \cong \prod_{v|p} \mathbb{Q}(\zeta_{N_0})_v$ one has*

$$b = -|D_p|^{-1}\left(1-\frac{1}{p}\right)^{-1}\lambda\cdot\xi_{N_0}.$$

This formula uniquely determines the image $\bar{\lambda}$ of λ in $\mathbb{Q}_p(\chi)$.

Proof. Since $\beta_{N_0}^{\infty}$ is a basis of the free rank one Λ-module R (by Lemma 5.1) we have

$$\lambda\cdot\beta_{N_0}^{\infty} = \theta_1^{PR}((\eta^{\infty})^{\varpi}) \tag{34}$$

for some element λ of Λ, which then also satisfies the condition (33).
The map θ_1^{PR} is described explicitly by (22). Further, with respect to the system $(\zeta_{p^n})_{n\geq 1}$, the Coleman power series that is associated to the norm compatible system of units $(\eta^{\infty})^{\varpi} = (\eta^{\infty})^{(1-\gamma)}$ is equal to

$$f(X) := \frac{X}{(1+X)^{\chi_{\mathrm{cyclo}}(\gamma)}-1} \equiv \chi_{\mathrm{cyclo}}(\gamma)^{-1} \mod (X).$$

Thus, by computing constant terms in the power series identity (34) we obtain equalities

$$\begin{aligned}\lambda\cdot\xi_{N_0} &= (1-\frac{\phi}{p})\log(f(X))\Big|_{X=0}\\ &= (1-\frac{1}{p})\log_p(\chi_{\mathrm{cyclo}}(\gamma)^{-1})\\ &= -(1-\frac{1}{p})|D_p|b\end{aligned}$$

as required to finish the proof of the first sentence of the lemma. On the other hand, the second sentence of the lemma is clear because ξ_{N_0} is a $\mathbb{Q}_p[G_{N_0}]$-basis of $\mathbb{Q}(\zeta_{N_0})_p$ and $\mathbb{Q}_p(\chi) = \Lambda_{\mathfrak{q}_\chi}/\varpi$ is a quotient of $\mathbb{Q}_p[G_{N_0}]$. □

With $\widetilde{\exp}$ denoting the map in (15), the last lemma implies that

$$\begin{aligned}\phi_{\varpi}^{-1}(\bar{\eta}^{\infty}) &= \bar{\eta}^{\infty}\wedge\exp(e_\chi b)\otimes\beta(\exp(e_\chi b))^{-1}\\ &= -\exp(e_\chi b)\wedge\bar{\eta}^{\infty}\otimes\mathrm{val}(\bar{\eta}^{\infty})^{-1}\\ &=\widetilde{\exp}(-e_\chi b)\\ &=\widetilde{\exp}\left(|D_p|^{-1}\left(1-\frac{1}{p}\right)^{-1}\bar{\lambda}\cdot e_\chi\xi_{N_0}\right),\end{aligned}$$

and hence, using (32), that

$$\begin{aligned}
&\widetilde{\exp}^{-1}(\beta^{\infty}_{N_0}\otimes_{\Lambda_{\mathfrak{q}_\chi}}1)\\
=&|D_p|^{-1}(1-\frac{1}{p})^{-1}e_\chi(\xi_{N_0})\\
=&|D_p|^{-1}(1-\frac{1}{p})^{-1}\chi(u')\prod_{\ell|N_0,\ell\nmid f_\chi}\frac{1}{\ell-1}\prod_{\ell|N_0}e_\ell(-\mathrm{Fr}_\ell^{-1})e_\chi\zeta_{f_\chi}\\
=&|D_p|^{-1}(1-\frac{1}{p})^{-1}\chi(u')\prod_{\ell|N_0,\ell\nmid f_\chi}\frac{1}{\ell-1}\prod_{\ell|N_0}e_\ell(-\mathrm{Fr}_\ell^{-1})[K:\mathbb{Q}(\zeta_{f_\chi})]e_\chi\beta_N\\
=&|D_p/J_p|^{-1}(1-\frac{1}{p})^{-1}\chi(u')\frac{[\mathbb{Q}(\zeta_{N_0}):\mathbb{Q}(\zeta_{f_{\chi,0}})]}{f_{\chi,0}^{r-1}\prod_{\ell|N_0,\ell\nmid f_\chi}(\ell-1)}\prod_{\ell|N_0}e_\ell(-\mathrm{Fr}_\ell^{-1})e_\chi\beta_N
\end{aligned}$$

where the second equality follows from Lemma 6.1, the third from Proposition 4.1 and the fourth from the fact that $r=1$, $f_\chi=f_{\chi,0}$ and

$$\frac{[K:\mathbb{Q}(\zeta_{f_\chi})]}{|J_p|\prod_{\ell|N_0,\ell\nmid f_\chi}(\ell-1)}=\frac{[\mathbb{Q}(\zeta_{N_0}):\mathbb{Q}(\zeta_{f_{\chi,0}})]}{f_{\chi,0}^{r-1}\prod_{\ell|N_0,\ell\nmid f_\chi}(\ell-1)}.$$

The required equality (27) is now obtained by comparing the above formula for $\widetilde{\exp}^{-1}(\beta^{\infty}_{N_0}\otimes_{\Lambda_{\mathfrak{q}_\chi}}1)$ to the definition of u in (24).
This completes our proof of Theorem 1.1.

7. Some remarks concerning $T\Omega^{\mathrm{loc}}(M,\mathfrak{A})$

In this section we prove two results that were used in the proof of Theorem 1.1 but which are most naturally formulated in a more general setting. In particular, these results extend the computations made in [9, §5].
We henceforth fix notation as in §2. Thus, we stress, M is no longer assumed to be a Tate motive and the (finite dimensional semisimple) $\mathbb{Q}$-algebra A is not assumed to be either commutative or a group ring.

7.1. The contribution from primes $\ell\neq p$.

We first recall the following basic fact about the cohomology of the profinite group $\hat{\mathbb{Z}}$ (for distinction we shall denote the canonical generator $1\in\hat{\mathbb{Z}}$ by σ). Let R be either a pro-p ring, or a localization of such a ring, and let C be a perfect complex of R-modules with a continuous action of $\hat{\mathbb{Z}}$. Then

$$R\Gamma(\hat{\mathbb{Z}},C)\cong\mathrm{Tot}(C\xrightarrow{1-\sigma}C)$$

is a perfect complex of R-modules where 'Tot' denotes the total complex of a double complex. The identity map of C induces a morphism

$$\mathrm{id}_{C,\mathrm{triv}}:\mathbf{1}_R\cong\mathrm{Det}_R^{-1}R\Gamma(\hat{\mathbb{Z}},C)$$

in $V(R)$ which is functorial for exact triangles in the variable C and also commutes with scalar extension.

PROPOSITION 7.1. *For a prime number $\ell \neq p$ we let σ_ℓ denote the Frobenius automorphism in* $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$. *If*

$$\theta_p^{\ell\text{-}part} : \mathbf{1}_{A_p} \cong \mathrm{Det}_{A_p}^{-1} R\Gamma(\mathbb{Q}_\ell, V_p)$$

denotes the morphism in $V(A_p)$ which occurs in [9, (67)], *then*

$$\mathrm{Det}_{A_p}(-\sigma_\ell \ell^{-1} | (V_p)_{I_\ell})^{-1} \, \theta_p^{\ell\text{-}part}$$

is induced by a morphism $\mathbf{1}_{\mathfrak{A}_p} \cong \mathrm{Det}_{\mathfrak{A}_p}^{-1} R\Gamma(\mathbb{Q}_\ell, T_p)$ in $V(\mathfrak{A}_p)$.

Proof. Recall the exact triangle of complexes of A_p-modules

$$R\Gamma_f(\mathbb{Q}_\ell, V_p) \to R\Gamma(\mathbb{Q}_\ell, V_p) \to R\Gamma_{/f}(\mathbb{Q}_\ell, V_p) \tag{35}$$

from [9, (18)] as well as the isomorphism

$$\mathrm{AV} : R\Gamma_{/f}(\mathbb{Q}_\ell, V_p) \cong R\Gamma_f(\mathbb{Q}_\ell, V_p^*(1))^*[-2]$$

from [9, Lem. 12a)]. The triangle (35) is obtained by applying $R\Gamma(\hat{\mathbb{Z}}, -)$ to the exact triangle

$$H^0(I_\ell, V_p) \to R\Gamma(I_\ell, V_p) \to H^1(I_\ell, V_p)[-1] \tag{36}$$

together with the isomorphism

$$R\Gamma(\hat{\mathbb{Z}}, R\Gamma(I_\ell, V_p)) \cong R\Gamma(\mathbb{Q}_\ell, V_p).$$

According to the convention [9, (19)] the generator σ we use here is σ_ℓ^{-1}. The isomorphism AV is more explicitly given by the diagram

$$\begin{tikzcd}
(V_p)_{I_\ell}(-1) \arrow[r, "1-\sigma_\ell^{-1}"] \arrow[d, equal] & (V_p)_{I_\ell}(-1) \arrow[d, "-\sigma_\ell"] \\
(V_p)_{I_\ell}(-1) \arrow[r, "1-\sigma_\ell"] \arrow[d, "\cong"] & (V_p)_{I_\ell}(-1) \arrow[d, "\cong"] \\
((V_p^*)^{I_\ell}(1))^* \arrow[r, "1-\sigma_\ell^{-1}"] & ((V_p^*)^{I_\ell}(1))^*.
\end{tikzcd}$$

Note here that $H^1(I_\ell, V_p)$ is naturally isomorphic to $(V_p)_{I_\ell}(-1)$ and that in the isomorphism $((V_p^*)^{I_\ell})^* \cong (V_p)_{I_\ell}$ the first dual is the contragredient σ_ℓ-representation whereas the second is simply the dual. From this last diagram we deduce

$$\mathrm{id}_{(V_p)_{I_\ell}(-1),\mathrm{triv}} = \mathrm{Det}_{A_p}(-\sigma_\ell \ell^{-1} | (V_p)_{I_\ell}) \, \mathrm{id}_{((V_p^*)^{I_\ell}(1))^*,\mathrm{triv}}$$

and by the discussion above with $R = A_p$ the exact triangle (36) gives

$$\mathrm{id}_{V_p^{I_\ell},\mathrm{triv}} \otimes \mathrm{id}^{-1}_{(V_p)_{I_\ell}(-1),\mathrm{triv}} = \mathrm{id}_{R\Gamma(I_\ell, V_p),\mathrm{triv}} .$$

By the definition of [9, (67)] the morphism $\theta_p^{\ell\text{-part}}$ is induced by the triangle (35), the isomorphism AV and the morphisms $\mathrm{id}_{V_p^{I_\ell},\mathrm{triv}}$ and $\mathrm{id}_{((V_p^*)^{I_\ell}(1))^*,\mathrm{triv}}$. Hence

$$\mathrm{Det}_{A_p}(-\sigma_\ell \ell^{-1} | (V_p)_{I_\ell})^{-1} \, \theta_p^{\ell\text{-part}}$$

is the scalar extension of the morphism $\mathrm{id}_{R\Gamma(I_\ell,T_p),\mathrm{triv}}$ in $V(\mathfrak{A}_p)$ and this finishes the proof of the Proposition. □

7.2. Artin-Verdier Duality. In this subsection we extend [9, Lem. 14] to include the case $p=2$ and hence resolve the issue raised in [9, Rem. 16].
Before stating the main result we recall that [9, (78)] defines a morphism in $V(A_p)$ of the form

$$\theta_p' : \left(\bigotimes_{\ell\in S_{p,f}} \mathrm{Det}^{-1}_{A_p} R\Gamma(\mathbb{Q}_\ell, V_p)\right) \otimes_{A_p} \mathrm{Det}^{-1}_{A_p}(V_p) \cong A_p \otimes_{\mathfrak{A}_p} \Lambda_p(S,T_p) \tag{37}$$

where

$$\Lambda_p(S,T_p) := \mathrm{Det}_{\mathfrak{A}_p} C(\mathbb{Q},T_p)$$

with $C(\mathbb{Q},T_p)$ a certain canonical perfect complex of $\mathfrak{A}_p$-modules (as occurs in the diagram (39) below with $E=\mathbb{Q}$).
We set

$$\epsilon_{V_p} := \mathrm{Det}_{A_p}(2|V_p^+)\,\mathrm{Det}_{A_p}(2|V_p^-)^{-1} \in K_1(A_p).$$

Proposition 7.2. *The morphism $\epsilon_{V_p}\cdot\theta_p'$ is induced by a morphism in $V(\mathfrak{A}_p)$ of the form*

$$\left(\bigotimes_{\ell\in S_{p,f}} \mathrm{Det}^{-1}_{\mathfrak{A}_p} R\Gamma(\mathbb{Q}_\ell, T_p)\right) \otimes_{\mathfrak{A}_p} \mathrm{Det}^{-1}_{\mathfrak{A}_p}(T_p) \cong \Lambda_p(S,T_p). \tag{38}$$

The proof of this result will occupy the remainder of this subsection.
We note first that if p is odd, then $\epsilon_{V_p}\in \mathrm{im}(K_1(\mathfrak{A}_p)\to K_1(A_p))$ and so the above claim is equivalent to asserting that θ_p' itself is induced by a morphism in $V(\mathfrak{A}_p)$ of the form (38). Since this is precisely the statement of [9, Lem. 14] we shall assume henceforth that $p=2$.
Now if E is any number field, then [9, (81)] gives a true nine term diagram

$$\begin{tikzcd}
\bigoplus_{v\in S_\infty} R\Gamma_\Delta(E_v,T_p^*(1))^*[-4] \arrow[r, equal] \arrow[d] & \bigoplus_{v\in S_\infty} R\Gamma_\Delta(E_v,T_p^*(1))^*[-4] \arrow[d, "\alpha(E)"'] & \\
\tilde{R\Gamma}_c(\mathcal{O}_{E,S_p},T_p^*(1))^*[-4] \arrow[r] \arrow[d] & {}_3L(S_p,T_p)[-1] \arrow[r] \arrow[d] & R\Gamma_c(\mathcal{O}_{E,S_p},T_p) \arrow[d, equal] \\
R\Gamma_c(\mathcal{O}_{E,S_p},T_p^*(1))^*[-4] \arrow[r] & C(E,T_p) \arrow[r] & R\Gamma_c(\mathcal{O}_{E,S_p},T_p)
\end{tikzcd} \tag{39}$$

where the complex ${}_3L(S_p,T_p)$ is endowed with a natural quasi-isomorphism

$$\beta(E) : {}_3L(S_p,T_p) \cong \bigoplus_{v\in S_p} R\Gamma(E_v,T_p).$$

To prove the Proposition we shall make an explicit study of the composite morphism $\beta(\mathbb{Q})\circ\alpha(\mathbb{Q})$. To do this we observe that if E is any Galois extension of $\mathbb{Q}$ with group Γ, then (39), resp. $\beta(E)$, is a true nine-term diagram, resp. quasi-isomorphism, of complexes of $\mathfrak{A}_p[\Gamma]$-modules and the same arguments as used in [8, Lem. 11] show that application of $R\operatorname{Hom}_{\mathbb{Z}_p[\Gamma]}(\mathbb{Z}_p,-)$ to (39), resp. $\beta(E)$, renders a diagram which is naturally isomorphic to the corresponding diagram for $E=\mathbb{Q}$, resp. a quasi-isomorphism which identifies naturally with $\beta(\mathbb{Q})$.

We now fix E to be an imaginary quadratic field and set $\Gamma := \mathrm{Gal}(E/\mathbb{Q})$ and $R\Gamma_{\mathrm{Tate}}(E_v,-) := R\Gamma(E_v,-)$ for each non-archimedean place v. Then for each $v_0 \in S$ one has a natural morphism $R\Gamma_{\mathrm{Tate}}(E_{v_0},-) \to R\Gamma(E_{v_0},-)$ and we let $\gamma_{v_0}(E)$ denote the following composite morphism in $D(\mathfrak{A}_p[\Gamma])$

$$R\Gamma_\Delta(E_\infty,T_p^*(1))^*[-3] \xrightarrow{\beta(E)\circ\alpha(E)[1]} \bigoplus_{v\in S_p} R\Gamma(E_v,T_p) \to R\Gamma(E_{v_0},T_p).$$

Now if v_0 is non-archimedean, then $\gamma_{v_0}(E)$ is equal to the composite

$$(40)\qquad R\Gamma_\Delta(E_\infty,T_p^*(1))^*[-3] \to \bigoplus_{v\in S_p} R\Gamma_{\mathrm{Tate}}(E_v,T_p) \to R\Gamma(E_{v_0},T_p),$$

where the first arrow denotes the diagonal morphism in the following commutative diagram in $D(\mathfrak{A}_p[\Gamma])$

$$\begin{tikzcd}
R\Gamma_\Delta(E_\infty,T_p^*(1))^*[-3] \arrow[r] \arrow[d, equal] & \tilde{R}\Gamma_c(\mathcal{O}_{E,S_p},T_p^*(1))^*[-3] \arrow[d] & R\Gamma(\mathcal{O}_{E,S_p},T_p) \arrow[l, "\mathrm{AV}"'] \arrow[d] \\
R\Gamma_\Delta(E_\infty,T_p^*(1))^*[-3] \arrow[r] & \bigoplus_{v\in S_p} R\Gamma_{\mathrm{Tate}}(E_v,T_p^*(1))^*[-2] & \bigoplus_{v\in S_p} R\Gamma_{\mathrm{Tate}}(E_v,T_p) \arrow[l, "\oplus\,\mathrm{AV}_v"']
\end{tikzcd}$$

in which the left, resp. right, hand square comes directly from the definition of $R\Gamma_\Delta(E_\infty,T_p^*(1))$ in [9, (80)], resp. from the compatibility of local and global Artin-Verdier duality as in [9, Lem. 12]. Since (v_0 is assumed for the moment to be non-archimedean and) the image of the lower left hand arrow in this diagram is contained in the summand $R\Gamma_{\mathrm{Tate}}(E_\infty,T_p^*(1))^*[-2]$ it is therefore clear that (40) is the zero morphism. Hence, there exists a natural isomorphism in $D(\mathfrak{A}_p[\Gamma])$ of the form

$$C(E,T_p) \cong C_\infty(E,T_p)[-1] \oplus \bigoplus_{v\in S_{p,f}} R\Gamma(E_v,T_p)[-1]$$

where $C_\infty(E,T_p)$ is a complex which lies in an exact triangle in $D(\mathfrak{A}_p[\Gamma])$ of the form

$$(41)\qquad R\Gamma_\Delta(E_\infty,T_p^*(1))^*[-3] \xrightarrow{\gamma_\infty(E)} R\Gamma(E_\infty,T_p) \to C_\infty(E,T_p) \to .$$

Now, via the canonical identifications $R\Gamma_\Delta(E_\infty,T_p^*(1))^*[-3] \cong T_p(-1)[-3]$ and $R\Gamma(E_\infty,T_p) \cong T_p[0]$, we may regard $\gamma_\infty(E)$ as an element of

$$\mathrm{Hom}_{D(\mathfrak{A}_p[\Gamma])}(T_p(-1)[-3],T_p[0]) \cong \mathrm{Ext}^3_{\mathfrak{A}_p[\Gamma]}(T_p(-1),T_p).$$

With respect to this identification, $C_\infty(E,T_p)$ represents $\gamma_\infty(E)$ viewed as a Yoneda 3-extension and so can be obtained via a push-out diagram of $\mathfrak{A}_p[\Gamma]$-modules of the form

$$\begin{tikzcd} 0 \arrow[r] & T_p \arrow[r] \arrow[d, "\mu"'] & T_p[\Gamma] \arrow[r, "1-c"] \arrow[d] & T_p[\Gamma] \arrow[r, "1+c"] \arrow[d, equal] & T_p[\Gamma] \arrow[r] \arrow[d, equal] & T_p(-1) \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & T_p \arrow[r] & B_\mu \arrow[r] & T_p[\Gamma] \arrow[r, "1+c"] & T_p[\Gamma] \arrow[r] & T_p(-1) \arrow[r] & 0. \end{tikzcd} \tag{42}$$

Here we write c for the natural diagonal action of the generator τ of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, the second arrow in the upper row is the map $t \mapsto t + \tau(t)\cdot\gamma$ where γ is the generator of Γ and the fifth arrow in both rows is the map $t + t'\cdot\gamma \mapsto (t-\tau(t'))\otimes\xi^{-1}$ with $\xi := (\zeta_{p^n})_{n\geq 1}$ (regarded as a generator of $\mathbb{Z}_p(1)$).
For any $\mathfrak{A}_p[\Gamma]$-module X the above diagram induces a commutative diagram of the form

$$\begin{tikzcd} \mathrm{Ext}^i_{\mathfrak{A}_p[\Gamma]}(T_p,X) \arrow[r] & \mathrm{Ext}^{i+3}_{\mathfrak{A}_p[\Gamma]}(T_p(-1),X) \\ \mathrm{Ext}^i_{\mathfrak{A}_p[\Gamma]}(T_p,X) \arrow[r] \arrow[u, "\mu^{*,i}"] & \mathrm{Ext}^{i+3}_{\mathfrak{A}_p[\Gamma]}(T_p(-1),X). \arrow[u, equal] \end{tikzcd}$$

But $C_\infty(E,T_p)$ belongs to $D^{\mathrm{perf}}(\mathfrak{A}_p[\Gamma])$ (since the lower row of (39) belongs to $D^{\mathrm{perf}}(\mathfrak{A}_p[\Gamma])$) and so the projective dimension of the $\mathfrak{A}_p[\Gamma]$-module B_μ is finite and therefore at most 1. This implies that the upper (resp. lower) horizontal map in the last diagram is bijective for $i \geq 2$ and surjective for $i = 1$ (resp. bijective for $i \geq 1$). The map $\mu^{*,i}$ is therefore bijective for each $i \geq 2$ and surjective for $i = 1$ and so a result of Holland [23, Th. 3.1] implies that there exists an automorphism $\alpha \in \mathrm{Aut}_{\mathfrak{A}_p[\Gamma]}(T_p)$ and a projective $\mathfrak{A}_p[\Gamma]$-module P such that $\mu - \alpha$ is equal to a composite of the form $T_p \to P \to T_p$. Now the Γ-module

$$\mathrm{Hom}_{\mathfrak{A}_p}(T_p(-1),P) \cong \mathrm{Hom}_{\mathfrak{A}_p}(T_p(-1),\mathfrak{A}_p)\otimes_{\mathfrak{A}_p} P =: T^*\otimes_{\mathfrak{A}_p} P$$

is cohomologically trivial (indeed, it suffices to check this for $P = \mathfrak{A}_p[\Gamma]$ in which case $T^*\otimes_{\mathfrak{A}_p}\mathfrak{A}_p[\Gamma] = T^*\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[\Gamma] \cong \mathbb{Z}_p[\Gamma]^d$ with $d = \mathrm{rank}_{\mathbb{Z}_p}(T^*)$) and so $\mathrm{Ext}^3_{\mathfrak{A}_p[\Gamma]}(T_p(-1),P) \cong H^3(\Gamma, \mathrm{Hom}_{\mathfrak{A}_p}(T_p(-1),P)) = 0$. In the diagram (42) we may therefore assume that $\mu \in \mathrm{Aut}_{\mathfrak{A}_p[\Gamma]}(T_p)$ and hence can use this diagram to identify $C_\infty(E,T_p)$ with the complex

$$T_p[\Gamma] \xrightarrow{1-c} T_p[\Gamma] \xrightarrow{1+c} T_p[\Gamma],$$

where the first term is placed in degree 0 (and the cohomology is computed via the maps in upper row of (42)). Writing $C_\infty(T_p)$ for the complex

$$T_p \xrightarrow{1-c} T_p \xrightarrow{1+c} T_p$$

(where the first term is placed in degree 0), we may thus deduce the existence of a composite isomorphism in $D(\mathfrak{A}_p)$ of the form

$$\begin{aligned}
&C_\infty(T_p)[-1] \oplus \bigoplus_{\ell \in S_{p,f}} R\Gamma(\mathbb{Q}_\ell, T_p)[-1] \\
&\cong R\operatorname{Hom}_{\mathbb{Z}_p[\Gamma]}(\mathbb{Z}_p, C_\infty(E, T_p)[-1] \oplus \bigoplus_{v \in S_{p,f}} R\Gamma(E_v, T_p)[-1]) \\
&\cong R\operatorname{Hom}_{\mathbb{Z}_p[\Gamma]}(\mathbb{Z}_p, C(E, T_p)) \\
&\cong C(\mathbb{Q}, T_p).
\end{aligned}$$

When taken in conjunction with the natural morphism

$$\begin{aligned}
j(T_p) : \operatorname{Det}_{\mathfrak{A}_p} C_\infty(T_p)[-1] &= \operatorname{Det}^{-1}_{\mathfrak{A}_p}(T_p) \otimes_{\mathfrak{A}_p} (\operatorname{Det}_{\mathfrak{A}_p}(T_p) \otimes_{\mathfrak{A}_p} \operatorname{Det}^{-1}_{\mathfrak{A}_p}(T_p)) \\
&\cong \operatorname{Det}^{-1}_{\mathfrak{A}_p}(T_p) \otimes_{\mathfrak{A}_p} \mathbf{1}_{\mathfrak{A}_p} = \operatorname{Det}^{-1}_{\mathfrak{A}_p}(T_p)
\end{aligned}$$

the above composite isomorphism induces a morphism in $V(\mathfrak{A}_p)$ of the form

$$\theta''_p : \left(\bigotimes_{\ell \in S_{p,f}} \operatorname{Det}^{-1}_{\mathfrak{A}_p} R\Gamma(\mathbb{Q}_\ell, T_p) \right) \otimes_{\mathfrak{A}_p} \operatorname{Det}^{-1}_{\mathfrak{A}_p}(T_p) \cong \operatorname{Det}_{\mathfrak{A}_p} C(\mathbb{Q}, T_p) =: \Lambda_p(S, T_p).$$

Now $A_p \otimes_{\mathfrak{A}_p} \theta''_p$ differs from the morphism θ'_p in (37) only in the following respect: in place of $A_p \otimes_{\mathfrak{A}_p} j(T_p)$ the morphism θ'_p involves the composite morphism

$$\begin{aligned}
j(V_p) : A_p \otimes_{\mathfrak{A}_p} \operatorname{Det}_{\mathfrak{A}_p} C_\infty(T_p)[-1] \cong \\
\operatorname{Det}^{-1}_{A_p}(A_p \otimes_{\mathfrak{A}_p} H^0(C_\infty(T_p))) \otimes_{A_p} \operatorname{Det}^{-1}_{A_p}(A_p \otimes_{\mathfrak{A}_p} H^2(C_\infty(T_p))) \\
\cong \operatorname{Det}^{-1}_{A_p} V_p
\end{aligned}$$

where the first morphism is the canonical 'passage to cohomology' map and the second is induced by combining the isomorphisms $A_p \otimes_{\mathfrak{A}_p} H^0(C_\infty(T_p)) \cong V_p^+$ and $A_p \otimes_{\mathfrak{A}_p} H^2(C_\infty(T_p)) \cong V_p(-1)^+$ that are induced by the upper row of (42) with the isomorphism $V_p^+ \oplus V_p(-1)^+ \cong V_p^+ \oplus V_p^- = V_p$ (where the second component of the first map sends each element v of $V_p(-1)^+$ to $v \otimes \xi \in V_p^-$). But the complex $A_p \otimes_{\mathfrak{A}_p} C_\infty(T_p)$ identifies with

$$V_p^+ \oplus V_p^- \xrightarrow{(0,2)} V_p^+ \oplus V_p^- \xrightarrow{(2,0)} V_p^+ \oplus V_p^-$$

and so, by an explicit computation, one has $A_p \otimes_{\mathfrak{A}_p} j(T_p) = \epsilon_{V_p} \cdot j(V_p)$ where $\epsilon_{V_p} := \operatorname{Det}_{A_p}(2|V_p^+) \operatorname{Det}_{A_p}(2|V_p^-)^{-1} \in K_1(A_p)$. The induced equality

$$A_p \otimes_{\mathfrak{A}_p} \theta''_p = \epsilon_{V_p} \cdot \theta'_p$$

then completes the proof of the Proposition.

References

[1] D. Benois and Th. N. Quang Do, La conjecture de Bloch et Kato pour les motifs $\mathbb{Q}(m)$ sur un corps abélian, Ann. Sci. Éc. Norm. Sup. 35 (2002) 641-672.

[2] D. Benois and L. Berger, Théorie d'Iwasawa des Représentations Cristallines II, preprint 2005, http://arxiv.org/abs/math/0509623.

[3] L. Berger, Bloch and Kato's exponential map: three explicit formulas, Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday (2003) 99-129.

[4] W. Bley and D. Burns, Equivariant epsilon constants, discriminants and étale cohomology, Proc. London Math. Soc. 87 (2003) 545-590.

[5] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives, In: 'The Grothendieck Festschrift' vol. 1, Progress in Math. 86, Birkhäuser, Boston, (1990) 333-400.

[6] M. Breuning and D. Burns, Additivity of Euler characteristics in relative algebraic K-theory, Homology, Homotopy and Applications 7 (2005) No. 3 11-36.

[7] M. Breuning and D. Burns, Leading terms of Artin L-functions at $s = 0$ and $s = 1$, manuscript submitted for publication.

[8] D. Burns and M. Flach, On Galois structure invariants associated to Tate motives, Amer. J. Math. 120 (1998) 1343-1397.

[9] D. Burns and M. Flach, Equivariant Tamagawa numbers for motives with (non-commutative) coefficients, Documenta Math. 6 (2001) 501-570.

[10] D. Burns and M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients II, Amer. J. Math. 125 (2003) 475-512.

[11] D. Burns and C. Greither, On the Equivariant Tamagawa Number Conjecture for Tate motives, Inventiones Math. 153 (2003) 303-359.

[12] Ph. Cassou-Noguès and M.J. Taylor, Constante de l'équation fonctionnelle de la fonction L d'Artin d'une représentation symplectique et modérée, Ann. Inst. Fourier, Grenoble 33, 2 (1983), 1-17.

[13] T. Chinburg, Exact sequences and Galois module structure, Annals of Math. 121 (1985) 351-376.

[14] R. Coleman, Division values in local fields, Inventiones Math. 53 (1979) 91-116.

[15] P. Deligne, Valeurs de fonctions L et périods d'intégrales, Proc. Sym. Pure Math. 33 (2), (1979) 313-346.

[16] P. Deligne, Le déterminant de la cohomologie, Contemp. Math. 67 (1987) 313-346, Amer. Math. Soc.

[17] M. Flach, The equivariant Tamagawa number conjecture - A survey, Contemp. Math. 358 (2004) 79-126, Amer. Math. Soc.

[18] J.-M. Fontaine and B. Perrin-Riou, Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L, In: Motives (Seattle) Proc. Symp. Pure Math. 55, I, (1994) 599-706.

[19] A. Fröhlich, Artin root numbers and normal integral bases for quaternion fields, Inventiones Math. 17 (1972) 143-166.

[20] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory, Proc. St . Petersburg Math. Soc. 11 (2005).

[21] C. Greither, On Chinburg's second conjecture for abelian fields, J. reine angew. math. 479 (1996) 1-29.

[22] H. Hasse, Vorlesungen über Zahlentheorie, Grundl. der math. Wiss. 59, Springer, Berlin 1964.

[23] D. Holland, Homological equivalences of modules and their projective invariants, J. London Math. Soc. 43 (1991) 396-411.

[24] J. Hooper, V. P. Snaith and M. van Tran, The second Chinburg conjecture for quaternion fields, Mem. Amer. Math. Soc. 148 (2000).

[25] A. Huber and G. Kings, Bloch-Kato conjecture and main conjecture of Iwasawa theory for Dirichlet characters, Duke. Math. J. 119 (2003) 393-464.

[26] A. Huber and J. Wildeshaus, Classical Polylogarithms according to Beilinson and Deligne, Documenta Math. 3 (1998) 27-133.

[27] K. Kato, Lectures on the approach to Iwasawa theory of Hasse-Weil L-functions via B_{dR}, Part I, In: Arithmetical Algebraic Geometry (ed. E.Ballico), Lecture Notes in Math. 1553 (1993) 50-163, Springer, New York, 1993.

[28] K. Kato, Lectures on the approach to Iwasawa theory of Hasse-Weil L-functions via B_{dR}, Part II, preprint, 1993.

[29] F. Knudsen and D. Mumford, The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'Div', Math. Scand. 39 (1976) 19-55.

[30] H.-W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpes, J. reine angew. Math. 201 (1959) 119-149.

[31] G. Lettl, The ring of integers of an abelian number field, J. reine angew. Math. 404 (1990) 162-170.

[32] J. Nekovář, Selmer Complexes, to appear in Astérisque.

[33] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale, Inventiones Math. 99 (1990) 247-292.

[34] B. Perrin-Riou, Théorie d'Iwasawa des représentations p-adique sur un corps local, Inventiones Math. 115 (1994) 81-149.

[35] V. P. Snaith, Burns' Equivariant Tamagawa Invariant $T\Omega^{\mathrm{loc}}(N/\mathbb{Q},1)$ for some quaternion fields, J. London Math. Soc. 68 (2003) 599-614.

[36] L. C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics 83, Springer, New York 1982.

David Burns
King's College London
Dept. of Mathematics
London WC2R 2LS
United Kingdom

Matthias Flach
Dept. of Mathematics
Caltech
Pasadena CA 91125
USA

On the Leading Terms of Zeta Isomorphisms and p-Adic L-functions in Non-Commutative Iwasawa Theory

Dedicated to John Coates

David Burns and Otmar Venjakob

Received: September 30, 2005
Revised: April 24, 2006

Abstract. We discuss the formalism of Iwasawa theory descent in the setting of the localized K_1-groups of Fukaya and Kato. We then prove interpolation formulas for the 'leading terms' of the global Zeta isomorphisms that are associated to certain Tate motives and of the p-adic L-functions that are associated to certain critical motives.

2000 Mathematics Subject Classification: Primary 11G40; Secondary 11R65 19A31 19B28

1. Introduction

In the last few years there have been several significant developments in non-commutative Iwasawa theory.

Firstly, in [11], Coates, Fukaya, Kato, Sujatha and the second named author formulated a main conjecture for elliptic curves without complex multiplication. More precisely, if F_∞ is any Galois extension of a number field F which contains the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F and is such that $\text{Gal}(F_\infty/F)$ is a compact p-adic Lie group with no non-trivial p-torsion, then Coates et al. formulated a $\text{Gal}(F_\infty/F)$-equivariant main conjecture for any elliptic curve which is defined over F, has good ordinary reduction at all places above p and whose Selmer group (over F_∞) satisfies a certain natural torsion condition.

Then, in [16], Fukaya and Kato formulated a natural main conjecture for any compact p-adic Lie extension of F and any critical motive M which is defined over F and has good ordinary reduction at all places above p.

The key feature of [11] is the use of the localization sequence of algebraic K-theory with respect to a canonical Ore set. However, the more general approach of [16] is rather more involved and uses a notion of 'localized K_1-groups' together with Nekovář's theory of Selmer complexes and the (conjectural) existence of certain canonical p-adic L-functions. See [39] for a survey.

The p-adic L-functions of Fukaya and Kato satisfy an interpolation formula which involves both the 'non-commutative Tamagawa number conjecture' (this is a natural refinement of the 'equivariant Tamagawa number conjecture' formulated by Flach and the first named author in [7] and hence also implies the 'main conjecture of non-abelian Iwasawa theory' discussed by Huber and Kings in [19]) as well as a local analogue of the non-commutative Tamagawa number conjecture. Indeed, by these means, at each continuous finite dimensional p-adic representation ρ of $\mathrm{Gal}(F_\infty/F)$, the 'value at ρ' of the p-adic L-function is explicitly related to the value at the central critical point of the complex L-function associated to the 'ρ^*-twist' $M(\rho^*)$ of M, where ρ^* denotes the contragredient of the representation ρ. However, if the Selmer module of $M(\rho^*)$ has strictly positive rank (and by a recent result of Mazur and Rubin [21], which is itself equivalent to a special case of an earlier result of Nekovář [24, Th. 10.7.17], this should often be the case), then both sides of the Fukaya-Kato interpolation formula are equal to zero.

The main aim of the present article is therefore to extend the formalism of Fukaya and Kato in order to obtain an interesting interpolation formula for all representations ρ as above. To this end we shall introduce a notion of 'the leading term at ρ' for elements of suitable localized K_1-groups. This notion is defined in terms of the Bockstein homomorphisms that have already played significant roles (either implicitly or explicitly) in work of Perrin-Riou [27, 29], of Schneider [34, 33, 32, 31] and of Greither and the first named author [9, 4] and have been systematically incorporated into Nekovář's theory of Selmer complexes [24]. We then give two explicit applications of this approach in the setting of extensions F_∞/F with $F_{\mathrm{cyc}} \subseteq F_\infty$. We show first that the 'p-adic Stark conjecture at $s = 1$', as formulated by Serre [35] and interpreted by Tate in [37], can be reinterpreted as providing interpolation formulas for the leading terms of the global Zeta isomorphisms associated to certain Tate motives in terms of the leading terms at $s = 1$ (in the classical sense) of the p-adic Artin L-functions that are constructed by combining Brauer induction with the fundamental results of Deligne and Ribet and of Cassou-Nogués. We then also prove an interpolation formula for the leading terms of the Fukaya-Kato p-adic L-functions which involves the leading term at the central critical point of the associated complex L-function, the Neron-Tate pairing and Nekovář's p-adic height pairing.

In a subsequent article we shall apply the approach developed here to describe the leading terms of the 'algebraic p-adic L-functions' that are introduced by the first named author in [5], and we shall use the resulting description to prove that the main conjecture of Coates et al. for an extension F_∞/F and an elliptic curve E implies the equivariant Tamagawa number conjecture for the motive $h^1(E)(1)$ at each finite degree subextension of F_∞/F. We note that this result provides a partial converse to the theorem of Fukaya and Kato which shows that, under a natural torsion hypothesis on Selmer groups, the main conjecture of Fukaya and Kato specialises to recover the main conjecture of Coates et al.

The main contents of this article are as follows. In §2 we recall some basic facts regarding (non-commutative) determinant functors and the localized K_1-groups of Fukaya and Kato. In §3 we discuss the formalism of Iwasawa theory descent in the setting of localized K_1-groups and we introduce a notion of the leading terms at p-adic representations for the elements of such groups. We explain how this formalism applies in the setting of the canonical Ore sets introduced by Coates et al., we show that it can be interpreted as taking values after 'partial derivation in the cyclotomic direction', and we use it to extend several well known results concerning Generalized Euler-Poincaré characteristics. In §4 we recall the 'global Zeta isomorphisms' that are conjectured to exist by Fukaya and Kato, and in §5 we prove an interpolation formula for the leading terms of the global Zeta isomorphisms that are associated to certain Tate motives. Finally, in §6, we prove an interpolation formula for the leading terms of the p-adic L-functions that are associated to certain critical motives. We shall use the same notation as in [39].

It is clear that the recent developments in non-commutative Iwasawa theory are due in large part to the energy, encouragement and inspiration of John Coates. It is therefore a particular pleasure for us to dedicate this paper to him on the occasion of his sixtieth birthday.

This collaboration was initiated during the conference held in Boston in June 2005 in recognition of the sixtieth birthday of Ralph Greenberg. The authors are very grateful to the organizers of this conference for the opportunity to attend such a stimulating meeting.

2. Preliminaries

2.1. Determinant functors. For any associative unital ring R we write $B(R)$ for the category of bounded (cohomological) complexes of (left) R-modules, $C(R)$ for the category of bounded (cohomological) complexes of finitely generated (left) R-modules, $P(R)$ for the category of finitely generated projective (left) R-modules and $C^p(R)$ for the category of bounded (cohomological) complexes of finitely generated projective (left) R-modules. We also write $D^p(R)$ for the category of perfect complexes as full triangulated subcategory of the bounded derived category $D^b(R)$ of (left) R-modules. We write $(P(R), \mathrm{is})$, $(C^p(R), \mathrm{quasi})$ and $(D^p(R), \mathrm{is})$ for the subcategories of isomorphisms in $P(R)$, quasi-isomorphisms in $C^p(R)$ and isomorphisms in $D^p(R)$ respectively.

For each complex $C = (C^\bullet, d_C^\bullet)$ and each integer r we define the r-fold shift $C[r]$ of C by setting $C[r]^i = C^{i+r}$ and $d^i_{C[r]} = (-1)^r d_C^{i+r}$ for each integer i.

We recall that in [16, §1.2] Fukaya and Kato construct an explicit alternative to the category of virtual objects that is used in [7]. Indeed, they construct explicitly a category $\mathcal{C}_R$ and a 'determinant functor'

$$\mathbf{d}_R : (P(R), \mathrm{is}) \to \mathcal{C}_R$$

which possess the following properties:

a) $\mathcal{C}_R$ has an associative and commutative product structure $(M,N) \mapsto M \cdot N$ (which we often write more simply as MN) with canonical unit object $\mathbf{1}_R = \mathbf{d}_R(0)$. If P is any object of $P(R)$, then in $\mathcal{C}_R$ the object $\mathbf{d}_R(P)$ has a canonical inverse $\mathbf{d}_R(P)^{-1}$. Every object of $\mathcal{C}_R$ is of the form $\mathbf{d}_R(P) \cdot \mathbf{d}_R(Q)^{-1}$ for suitable objects P and Q of $P(R)$;

b) All morphisms in $\mathcal{C}_R$ are isomorphisms and elements of the form $\mathbf{d}_R(P)$ and $\mathbf{d}_R(Q)$ are isomorphic in $\mathcal{C}_R$ if and only if P and Q correspond to the same element of the Grothendieck group $K_0(R)$. There is a natural identification $\mathrm{Aut}_{\mathcal{C}_R}(\mathbf{1}_R) \cong K_1(R)$ and if $\mathrm{Mor}_{\mathcal{C}_R}(M,N)$ is non-empty, then it is a $K_1(R)$-torsor where each element α of $K_1(R) \cong \mathrm{Aut}_{\mathcal{C}_R}(\mathbf{1}_R)$ acts on $\phi \in \mathrm{Mor}_{\mathcal{C}_R}(M,N)$ to give $\alpha\phi : M = \mathbf{1}_R \cdot M \xrightarrow{\alpha\cdot\phi} \mathbf{1}_R \cdot N = N$;

c) $\mathbf{d}_R$ preserves the product structure: specifically, for each P and Q in $P(R)$ one has $\mathbf{d}_R(P \oplus Q) = \mathbf{d}_R(P) \cdot \mathbf{d}_R(Q)$.

The functor $\mathbf{d}_R$ can be extended to give a functor

$$\mathbf{d}_R : (C^p(R), \text{quasi}) \to \mathcal{C}_R$$

in the following way: for each $C \in C^p(R)$ one sets

$$\mathbf{d}_R(C) := \mathbf{d}_R(\bigoplus_{i\in\mathbb{Z}} C^{2i})\mathbf{d}_R(\bigoplus_{i\in\mathbb{Z}} C^{2i+1})^{-1}.$$

This extended functor then has the following properties for all objects C, C' and C'' of $C^p(R)$:

d) If $0 \to C' \to C \to C'' \to 0$ is a short exact sequence in $C^p(R)$, then there exists a canonical morphism in $\mathcal{C}_R$ of the form

$$\mathbf{d}_R(C) \cong \mathbf{d}_R(C')\mathbf{d}_R(C''),$$

which we take to be an identification;

e) If C is acyclic, then the quasi-isomorphism $0 \to C$ induces a canonical morphism in $\mathcal{C}_R$ of the form

$$\mathbf{1}_R = \mathbf{d}_R(0) \to \mathbf{d}_R(C);$$

f) For any integer r there exists a canonical morphism $\mathbf{d}_R(C[r]) \cong \mathbf{d}_R(C)^{(-1)^r}$ in $\mathcal{C}_R$ which we take to be an identification;

g) The functor $\mathbf{d}_R$ factorizes through the image of $C^p(R)$ in $D^p(R)$ and extends (uniquely up to unique isomorphism) to give a functor

$$\mathbf{d}_R : (D^p(R), \text{is}) \to \mathcal{C}_R.$$

h) For each $C \in D^b(R)$ we write $H(C)$ for the complex with $H(C)^i = H^i(C)$ in each degree i and in which all differentials are 0. If $H(C)$ belongs to $D^p(R)$ (in which case we shall say that C is *cohomologically perfect*), then there are canonical morphisms in $\mathcal{C}_R$ of the form

$$\mathbf{d}_R(C) \cong \mathbf{d}_R(H(C)) \cong \prod_{i\in\mathbb{Z}} \mathbf{d}_R(H^i(C))^{(-1)^i};$$

i) If R' is any other (associative unital) ring and Y is an (R',R)-bimodule that is both finitely generated and projective as a left R'-module, then the functor $Y\otimes_R - : P(R)\to P(R')$ extends to give a diagram

$$\begin{tikzcd}
(D^p(R),\mathrm{is}) \arrow[r, "\mathbf{d}_R"] \arrow[d, "Y\otimes^{\mathbb{L}}_R -"'] & \mathcal{C}_R \arrow[d, "Y\otimes_R -"] \\
(D^p(R'),\mathrm{is}) \arrow[r, "\mathbf{d}_{R'}"] & \mathcal{C}_{R'}
\end{tikzcd}$$

which commutes (up to canonical isomorphism). In particular, if $R\to R'$ is any ring homomorphism and $C\in \mathrm{D}^p(R)$, then we often write $\mathbf{d}_R(C)_{R'}$ in place of $R'\otimes_R \mathbf{d}_R(C)$.

Remark 2.1. Unless R is a regular ring, property d) does not extend to arbitrary exact triangles in $D^p(R)$. In general therefore all constructions in the sequel which involve complexes must be made in such a way to avoid this problem (nevertheless, we suppress any explicit discussion of this issue in the present manuscript and simply refer the reader to [7] for details as to how this problem can be overcome). The second displayed morphism in h) is induced by the properties d) and f). However, whilst a precise description of the first morphism in h) is important for the purposes of explicit computations, it is actually rather difficult to find in the literature. Here we use the description given by Knudsen in [20, §3].

Remark 2.2. In the sequel we will have to distinguish between two inverses of a morphism $\phi : C\to D$ with $C,D\in\mathcal{C}_R$. The inverse with respect to composition will be denoted by $\overline{\phi} : D\to C$ while

$$\phi^{-1} := \overline{\mathrm{id}_{D^{-1}}\cdot\phi\cdot\mathrm{id}_{C^{-1}}} : C^{-1}\to D^{-1}$$

is the unique isomorphism such that $\phi\cdot\phi^{-1}=\mathrm{id}_{\mathbf{1}_R}$ under the identification $X\cdot X^{-1}=\mathbf{1}_R$ for both $X=C$ and $X=D$. If $D=C$, then $\phi : C\to C$ corresponds uniquely to an element of $K_1(R)\cong \mathrm{Aut}_{\mathcal{C}_R}(\mathbf{1}_R)$ by the rule $\phi\cdot\mathrm{id}_{C^{-1}} : \mathbf{1}_R\to\mathbf{1}_R$. Under this identification $\overline{\phi}$ and ϕ^{-1} agree in $K_1(R)$ and are inverse to ϕ. Furthermore, the following relation between $\circ$ and $\cdot$ is easily verified: if $\phi : A\to B$ and $\psi : B\to C$ are morphisms in $\mathcal{C}_R$, then one has $\psi\circ\phi=\psi\cdot\phi\cdot\mathrm{id}_{B^{-1}}$.

We shall use the following

Convention: If $\phi : \mathbf{1}\to A$ is a morphism and B an object in $\mathcal{C}_R$, then we write $B \xrightarrow{\cdot\,\phi} B\cdot A$ for the morphism $\mathrm{id}_B\cdot\phi$. In particular, any morphism $B\xrightarrow{\phi} A$ can be written as $B\xrightarrow{\cdot\,(\mathrm{id}_{B^{-1}}\cdot\,\phi)} A$.

Remark 2.3. In this remark we let C denote the complex $P_0\xrightarrow{\phi}P_1$, in which the first term is placed in degree 0 and $P_0=P_1=P$. Then, by definition, one has $\mathbf{d}_R(C)\overset{def}{=\!=}\mathbf{1}_R$. However, if ϕ is an isomorphism (so C is acyclic), then by property e) there is also a canonical morphism $\mathbf{1}_R \xrightarrow{acyc} \mathbf{d}_R(C)$. This latter morphism coincides with the composite

$$\mathbf{1}_R = \mathbf{d}_R(P_1)\mathbf{d}_R(P_1)^{-1} \xrightarrow{\mathbf{d}_R(\phi)^{-1}\cdot \mathrm{id}_{\mathbf{d}_R(P_1)^{-1}}} \mathbf{d}_R(P_0)\mathbf{d}_R(P_1)^{-1} = \mathbf{d}_R(C)$$

and thus depends on ϕ. Indeed, Remark 2.2 shows that the composite morphism

$$\mathbf{1}_R \xrightarrow{acyc} \mathbf{d}_R(C) \overset{def}{=\!=} \mathbf{1}_R$$

corresponds to the element $\mathbf{d}_R(\phi)^{-1}$ of $K_1(R)$. Thus, in order to distinguish between the above identifications of $\mathbf{1}_R$ with $\mathbf{d}_R(C)$, we shall say that C is *trivialized by the identity* when using either $\mathbf{d}_R(C) \overset{def}{=\!=} \mathbf{1}_R$ or its inverse with respect to composition.

Remark 2.4. Let $\mathcal{O} = \mathcal{O}_L$ be the valuation ring of a finite extension L of $\mathbb{Q}_p$ and A a finite $\mathcal{O}$-module. Then for any morphism in $\mathcal{C}_{\mathcal{O}}$ of the form $a : \mathbf{1}_{\mathcal{O}} \to \mathbf{d}_{\mathcal{O}}(A)$, and in particular therefore for that induced by any exact sequence of $\mathcal{O}$-modules of the form $0 \longrightarrow \mathcal{O}^n \longrightarrow \mathcal{O}^n \longrightarrow A \longrightarrow 0$, we obtain a canonical element $c = c(a) \in L^\times \cong \mathrm{Aut}_{\mathcal{C}_L}(\mathbf{1}_L)$ by means of the composite

$$\mathbf{1}_L \xrightarrow{a_L} L \otimes_{\mathcal{O}} \mathbf{d}_{\mathcal{O}}(A) = \mathbf{d}_L(L \otimes_{\mathcal{O}} A) \xrightarrow{acyc} \mathbf{1}_L$$

where the map 'acyc' is induced by property e). As an immediate consequence of the elementary divisor theorem one checks that $\mathrm{ord}_L(c) = \mathrm{length}_{\mathcal{O}}(A)$.

2.2. The localized K_1-group. In [16, §1.3] a *localized* K_1-group is defined for any full subcategory Σ of $C^p(R)$ which satisfies the following four conditions:

(i) $0 \in \Sigma$,

(ii) if C, C' are in $C^p(R)$ and C is quasi-isomorphic to C', then $C \in \Sigma \Leftrightarrow C' \in \Sigma$,

(iii) if $C \in \Sigma$, then $C[n] \in \Sigma$ for all $n \in \mathbb{Z}$,

(iv) if $0 \to C' \to C \to C'' \to 0$ is an exact sequence in $C^p(R)$ with both $C' \in \Sigma$ and $C'' \in \Sigma$, then $C \in \Sigma$.

Since we want to apply the same construction to a subcategory which is not necessarily closed under extensions, we weaken the last condition to

(iv′) if C' and C'' belong to Σ, then $C' \oplus C''$ belongs to Σ.

Definition 2.5. (Fukaya and Kato) Let Σ be any full subcategory of $C^p(R)$ which satisfies the conditions (i), (ii), (iii) and (iv′). Then the *localized* K_1-*group* $K_1(R, \Sigma)$ is defined to be the (multiplicatively written) abelian group which has as generators all symbols of the form $[C, a]$ where $C \in \Sigma$ and a is a morphism $\mathbf{1}_R \to \mathbf{d}_R(C)$ in $\mathcal{C}_R$, and as relations

(0) $[0, \mathrm{id}_{\mathbf{1}_R}] = 1$,

(1) $[C', \mathbf{d}_R(f) \circ a] = [C, a]$ if $f : C \to C'$ is a quasi-isomorphism with C (and thus also C') in Σ,

(2) if $0 \to C' \to C \to C'' \to 0$ is an exact sequence in Σ, then

$$[C, a] = [C', a'] \cdot [C'', a'']$$

where a is the composite of $a' \cdot a''$ with the isomorphism induced by property d),

(3) $[C[1], a^{-1}] = [C, a]^{-1}$.

Remark 2.6. Relation (3) is a simple consequence of the relations (0), (1) and (2). Note also that this definition of $K_1(R, \Sigma)$ makes no use of the conditions (iii) and (iv$'$) that the category Σ is assumed to satisfy. In particular, if Σ satisfies (iv) (rather than only (iv$'$)), then the above definition coincides with that given by Fukaya and Kato. We shall often refer to a morphism in $\mathcal{C}_R$ of the form $a : \mathbf{1}_R \to \mathbf{d}_R(C)$ or $a : \mathbf{d}_R(C) \to \mathbf{1}_R$ as a *trivialization* (of C).

We now assume to be given a left denominator set S of R and we let $R_S := S^{-1}R$ denote the corresponding localization and Σ_S the full subcategory of $C^p(R)$ consisting of all complexes C such that $R_S \otimes_R C$ is acyclic. For any $C \in \Sigma_S$ and any morphism $a : \mathbf{1}_R \to \mathbf{d}_R(C)$ in $\mathcal{C}_R$ we write $\theta_{C,a}$ for the element of $K_1(R_S)$ which corresponds under the canonical isomorphism $K_1(R_S) \cong \mathrm{Aut}_{\mathcal{C}_{R_S}}(\mathbf{1}_{R_S})$ to the composite

$$(1) \qquad \mathbf{1}_{R_S} \to \mathbf{d}_{R_S}(R_S \otimes_R C) \to \mathbf{1}_{R_S}$$

where the first arrow is induced by a and the second by the fact that $R_S \otimes_R C$ is acyclic. Then it can be shown that the assignment $[C, a] \mapsto \theta_{C,a}$ induces an isomorphism of groups

$$\mathrm{ch}_{R,\Sigma_S} : K_1(R, \Sigma_S) \cong K_1(R_S)$$

(cf. [16, Prop. 1.3.7]). Hence, if Σ is any subcategory of Σ_S we also obtain a composite homomorphism

$$\mathrm{ch}_{R,\Sigma} : K_1(R, \Sigma) \to K_1(R, \Sigma_S) \cong K_1(R_S).$$

In particular, we shall often use this construction in the following case: C is a fixed object of $D^p(R)$ which is such that $R_S \otimes_R C$ is acyclic and Σ denotes the smallest full subcategory Σ_C of $C^p(R)$ which contains all objects of $C^p(R)$ that are isomorphic in $D^p(R)$ to C and also satisfies the conditions (i), (ii), (iii) and (iv) that are described above. (With this definition, it is easily seen that $\Sigma_C \subset \Sigma_S$).

3. Leading terms

In this section we define a notion of the leading term at a continuous finite dimensional p-adic representation of elements of suitable localized K_1-groups. To do this we introduce an appropriate 'semisimplicity' hypothesis and use a natural construction of Bockstein homomorphisms. We also discuss several alternative characterizations of this notion. We explain how this formalism applies in the context of the canonical localizations introduced in [11] and we use it to extend several well known results concerning Generalized Euler-Poincaré characteristics.

3.1. Bockstein homomorphisms. Let G be a compact p-adic Lie group which contains a closed normal subgroup H such that the quotient group $\Gamma := G/H$ is topologically isomorphic to $\mathbb{Z}_p$. We fix a topological generator γ of Γ and denote by

$$\theta \in H^1(G, \mathbb{Z}_p) = \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Z}_p)$$

the unique homomorphism $G \twoheadrightarrow \Gamma \to \mathbb{Z}_p$ which sends γ to 1. We write $\Lambda(G)$ for the Iwasawa algebra of G. Then, since $H^1(G, \mathbb{Z}_p) \cong \mathrm{Ext}^1_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{Z}_p)$ by [25, Prop. 5.2.14], the element θ corresponds to a canonical extension of $\Lambda(G)$-modules of the form

$$0 \to \mathbb{Z}_p \to E_\theta \to \mathbb{Z}_p \to 0. \tag{2}$$

Indeed, one has $E_\theta = \mathbb{Z}_p^2$ upon which G acts via the matrix $\begin{pmatrix} 1 & \theta \\ 0 & 1 \end{pmatrix}$.
For any $A^\bullet$ in $B(\Lambda(G))$ we endow the complex $A^\bullet \otimes_{\mathbb{Z}_p} E_\theta$ with the natural diagonal G-action. Then (2) induces an exact sequence in $B(\Lambda(G))$ of the form

$$0 \to A^\bullet \to A^\bullet \otimes_{\mathbb{Z}_p} E_\theta \to A^\bullet \to 0.$$

This sequence in turn induces a 'cup-product' morphism in $D^b(\Lambda(G))$ of the form

$$A^\bullet \xrightarrow{\theta} A^\bullet[1]. \tag{3}$$

It is clear that this morphism depends upon the choice of γ, but nevertheless we continue to denote it simply by θ.
We now let $\rho : G \to \mathrm{GL}_n(\mathcal{O})$ be a (continuous) representation of G on $T_\rho := \mathcal{O}^n$, where $\mathcal{O} = \mathcal{O}_L$ denotes the valuation ring of a finite extension L of $\mathbb{Q}_p$. Then in the sequel we are mainly interested in the morphism

$$\mathcal{O}^n \otimes^{\mathbb{L}}_{\Lambda(G)} A^\bullet \xrightarrow{\theta_*} \mathcal{O}^n \otimes^{\mathbb{L}}_{\Lambda(G)} A^\bullet[1]$$

that is induced by (3), where we consider $\mathcal{O}^n$ as a right $\Lambda(G)$-module via the transpose ρ^t of ρ. In particular, in each degree i we shall refer to the induced homomorphism

$$\mathfrak{B}_i : \mathbb{T}\mathrm{or}_i^{\Lambda(G)}(T_\rho, A^\bullet) \to \mathbb{T}\mathrm{or}_{i-1}^{\Lambda(G)}(T_\rho, A^\bullet)$$

of hyper-tor groups

$$\mathbb{T}\mathrm{or}_i^{\Lambda(G)}(T_\rho, A^\bullet) := H^{-i}(\mathcal{O}^n \otimes^{\mathbb{L}}_{\Lambda(G)} A^\bullet)$$

as the *Bockstein homomorphism (in degree i) of* $(A^\bullet, T_\rho, \gamma)$.

3.2. The case $G = \Gamma$. In this section we consider the case $G = \Gamma$ and take the trivial Γ-module $\mathbb{Z}_p$ for ρ. We set $T := \gamma - 1 \in \Lambda(\Gamma)$.

3.2.1. *Bockstein homomorphisms.* For any complex $A^\bullet \in B(\Lambda(\Gamma))$ it is clear that the canonical short exact sequence

$$0 \to \Lambda(\Gamma) \xrightarrow{\times T} \Lambda(\Gamma) \to \mathbb{Z}_p \to 0$$

induces an exact triangle in $D^b(\Lambda(\Gamma))$ of the form

$$A^\bullet \xrightarrow{\times T} A^\bullet \to \mathbb{Z}_p \otimes^{\mathbb{L}}_{\Lambda(\Gamma)} A^\bullet \to A^\bullet[1]. \tag{4}$$

However, in order to be as concrete as possible, we choose to describe this result on the level of complexes. To this end we fix the following definition of the mapping cone of a morphism $f : A^\bullet \to B^\bullet$ of complexes:

$$\mathrm{cone}(f) := B^\bullet \oplus A^\bullet[1],$$

with differential in degree i equal to

$$d^i_{\mathrm{cone}(f)} := \begin{pmatrix} d^i_{B^\bullet} & f^i \\ 0 & -d^{i+1}_{A^\bullet} \end{pmatrix} : B^i \oplus A^{i+1} \to B^{i+1} \oplus A^{i+2}.$$

If $A^\bullet$ is a bounded complex of projective $\Lambda(\Gamma)$-modules, then we set

$$\mathrm{cone}(A^\bullet) := \mathrm{cone}(A^\bullet \xrightarrow{T} A^\bullet)$$

and

$$A_0^\bullet := \mathbb{Z}_p \otimes_{\Lambda(\Gamma)} A^\bullet.$$

In any such case there exists a morphism of complexes $\pi : \mathrm{cone}(A^\bullet) \to A_0^\bullet$ of the form

$$\begin{tikzcd}
{} \arrow[r] & A^{i-1} \oplus A^i \arrow[r, "d^{i-1}_{\mathrm{cone}}"] \arrow[d, "\pi^{i-1}"'] & A^i \oplus A^{i+1} \arrow[r, "d^i_{\mathrm{cone}}"] \arrow[d, "\pi^i"'] & A^{i+1} \oplus A^{i+2} \arrow[r, "d^{i+1}_{\mathrm{cone}}"] \arrow[d, "\pi^{i+1}"'] & {} \\
{} \arrow[r] & A_0^{i-1} \arrow[r, "d^{i-1}_{A_0^\bullet}"] & A_0^i \arrow[r, "d^i_{A_0^\bullet}"] & {A_0}^{i+1} \arrow[r, "d^{i+1}_{A_0^\bullet}"] & {}
\end{tikzcd}$$

where, in each degree i, π^i sends $(a, b) \in A^i \oplus A^{i+1}$ to the image of a in $\mathbb{Z}_p \otimes_{\Lambda(\Gamma)} A^i = A_0^i$. It is easy to check that π is a quasi-isomorphism.
Now from (4) we obtain short exact sequences

$$0 \to H^i(A^\bullet)_\Gamma \to \mathbb{H}_{-i}(\Gamma, A^\bullet) \to H^{i+1}(A^\bullet)^\Gamma \to 0 \tag{5}$$

where

$$\mathbb{H}_i(\Gamma, A^\bullet) := \mathbb{T}\mathrm{or}_i^{\Lambda(\Gamma)}(\mathbb{Z}_p, A^\bullet)$$

denotes the hyper-homology of $A^\bullet$ (with respect to Γ) and for any $\Lambda(\Gamma)$-module M we write $M_\Gamma = M/TM$ and $M^\Gamma = {}_TM$ (= kernel of multiplication by T) for the maximal quotient module, resp. submodule, of M upon which Γ acts trivially.

Lemma 3.1. *Let $A^\bullet$ be a bounded complex of projective $\Lambda(\Gamma)$-modules. Then in each degree i the Bockstein homomorphism of the triple $(A^\bullet, \mathbb{Z}_p, \gamma)$ coincides with the composite*

$$\mathbb{H}_i(\Gamma, A^\bullet) \to H^{-i+1}(A^\bullet)^\Gamma \xrightarrow{\kappa^{-i+1}(A^\bullet)} H^{-i+1}(A^\bullet)_\Gamma \to \mathbb{H}_{i-1}(\Gamma, A^\bullet)$$

where the first and third arrows are as in (5) and $\kappa^{-i+1}(A^\bullet)$ *denotes the tautological homomorphism*

$$H^{-i+1}(A^\bullet)^\Gamma \hookrightarrow H^{-i+1}(A^\bullet) \twoheadrightarrow H^{-i+1}(A^\bullet)_\Gamma.$$

Proof. As is shown by Rapoport and Zink in [30, Lem. 1.2], on the level of complexes the cup product morphism of the triple $(A^\bullet, \mathbb{Z}_p, \gamma)$ is described by the morphism

$$\theta : \mathrm{cone}(A^\bullet) \to \mathrm{cone}(A^\bullet)[1]$$

which sends $(a, b) \in A^i \oplus A^{i+1}$ to $(b, 0) \in A^{i+1} \oplus A^{i+2}$. Now let $\bar{a}$ be in $\ker(d^{-i}_{A_0^\bullet})$ representing a class in $\mathbb{H}_i(\Gamma, A^\bullet)$. Then there exists $(a, b) \in \ker(d^{-i}_{\mathrm{cone}})$ with $\pi^{-i}((a, b)) = \bar{a}$. Since $(a, b) \in \ker(d^{-i}_{\mathrm{cone}})$ one has $b \in \ker(d^{i+1}_{A^\bullet})$ and $Tb = -d^i_{A^\bullet}(a)$. This implies that $d^i_{A^\bullet}(a)$ is divisible by T (in A^{i+1}) and also that $b = -T^{-1}d^i_{A^\bullet}(a) \in A^{i+1}$. Thus θ maps (a, b) to $(-T^{-1}d^i_{A^\bullet}(a), 0)$ and the class in $\mathbb{H}_{i-1}(\Gamma, A^\bullet)$ is represented by $-\overline{T^{-1}d^i_{A^\bullet}(a)} \in \ker(d^{-i+1}_{A_0^\bullet})$. By using the canonical short exact sequence

$$0 \to A^\bullet \to \mathrm{cone}(A^\bullet) \to A^\bullet[1] \to 0$$

one immediately verifies that $\mathfrak{B}_i$ coincides with the composite homomorphism described in the lemma. □

From this description it is clear that for any bounded complex of projective $\Lambda(\Gamma)$-modules $A^\bullet$ the pair

$$(\mathbb{H}_i(\Gamma, A^\bullet), \mathfrak{B}_i) \tag{6}$$

forms a homological complex (which, by re-indexing, we shall consider as cohomological complex whenever convenient). It is also clear that this construction extends in a well-defined fashion to objects $A^\bullet$ of $D^p(\Lambda(\Gamma))$.

3.2.2. *Semisimplicity.*

Definition 3.2. *(Semisimplicity)* For any $A^\bullet \in D^p(\Lambda(\Gamma))$ we set

$$r_\Gamma(A^\bullet) := \sum_{i \in \mathbb{Z}} (-1)^{i+1} \dim_{\mathbb{Q}_p}(H^i(A^\bullet)^\Gamma \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \in \mathbb{Z}.$$

We say that a complex $A^\bullet \in D^p(\Lambda(\Gamma))$ is *semisimple* if the cohomology of the associated complex (6) is $\mathbb{Z}_p$-torsion (and hence finite) in all degrees. We let Σ_{ss} denote the full subcategory of $C^p(\Lambda(\Gamma))$ consisting of those complexes that are semisimple.

Remark 3.3. (i) If $A^\bullet \in D^p(\Lambda(\Gamma))$ is semisimple, then the cohomology of $A^\bullet$ is a torsion $\Lambda(\Gamma)$-module in all degrees.
(ii) In each degree i Lemma 3.1 gives rise to a canonical exact sequence

$$0 \to \mathrm{cok}(\kappa^{-i}(A^\bullet)) \to \ker(\mathfrak{B}_i)/\mathrm{im}(\mathfrak{B}_{i+1}) \to \ker(\kappa^{-i+1}(A^\bullet)) \to 0.$$

This implies that a complex $A^\bullet \in D^p(\Lambda(\Gamma))$ is semisimple if and only if the homomorphism $\kappa^i(A^\bullet)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ is bijective in each degree i, and hence also that in any such case one has

$$r_\Gamma(A^\bullet) = \sum_{i\in\mathbb{Z}}(-1)^{i+1}\dim_{\mathbb{Q}_p}(H^i(A^\bullet)_\Gamma \otimes_{\mathbb{Z}_p}\mathbb{Q}_p).$$

Definition 3.4. *(The canonical trivialization)* For each $A^\bullet \in D^b(\Lambda(\Gamma))$ we write $(\mathbb{H}_\bullet(\Gamma, A^\bullet), 0)$ for the complex with $(\mathbb{H}_\bullet(\Gamma, A^\bullet), 0)^i = \mathbb{H}_i(\Gamma, A^\bullet)$ in each degree i and in which all differentials are the zero map. In particular, if $A^\bullet \in \Sigma_{\mathrm{ss}}$, then we obtain a canonical composite morphism

$$\begin{aligned}(7)\quad t(A^\bullet) : \mathbf{d}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\Lambda(\Gamma)} A^\bullet)_{\mathbb{Q}_p} &\cong \mathbf{d}_{\mathbb{Z}_p}((\mathbb{H}_\bullet(\Gamma, A^\bullet), 0))_{\mathbb{Q}_p}\\ &= \mathbf{d}_{\mathbb{Z}_p}((\mathbb{H}_\bullet(\Gamma, A^\bullet), \mathfrak{B}_\bullet))_{\mathbb{Q}_p} \cong \mathbf{1}_{\mathbb{Q}_p}\end{aligned}$$

where the first, resp. last, morphism uses property h) (in §2.1) for the functor $\mathbf{d}_{\mathbb{Z}_p}$, resp. property i) for the natural homomorphism $\mathbb{Z}_p \to \mathbb{Q}_p$ and then property e) for the functor $\mathbf{d}_{\mathbb{Q}_p}$.

Remark 3.5. If the complex $\mathbb{Q}_p \otimes_{\Lambda(\Gamma)} A^\bullet$ is acyclic, then $t(A^\bullet)$ coincides with the trivialization obtained by directly applying property e) to $\mathbb{Q}_p \otimes_{\Lambda(\Gamma)} A^\bullet$.

The category Σ_{ss} satisfies the conditions (i), (ii), (iii) and (iv′) that are described in §2 (but does not satisfy condition (iv)). In addition, as the following result shows, the above constructions behave well on short exact sequences of semisimple complexes.

Lemma 3.6. *Let $A^\bullet, B^\bullet$ and $C^\bullet$ be objects of Σ_{ss} which together lie in a short exact sequence in $C^p(\Lambda(\Gamma))$ of the form*

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0.$$

Then one has

$$r_\Gamma(B^\bullet) = r_\Gamma(A^\bullet) + r_\Gamma(C^\bullet)$$

and, with respect to the canonical morphism

$$\mathbf{d}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\Lambda(\Gamma)} B^\bullet)_{\mathbb{Q}_p} \cong \mathbf{d}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\Lambda(\Gamma)} A^\bullet)_{\mathbb{Q}_p} \cdot \mathbf{d}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\Lambda(\Gamma)} C^\bullet)_{\mathbb{Q}_p}$$

that is induced by the given short exact sequence, one has

$$t(B^\bullet) = t(A^\bullet) \cdot t(C^\bullet).$$

Proof. We let $\mathfrak{p}$ denote the kernel of the augmentation map $\Lambda(\Gamma) \to \mathbb{Z}_p$ and R the localization $\Lambda(\Gamma)_\mathfrak{p}$ of $\Lambda(\Gamma)$ at $\mathfrak{p}$. Then R is a discrete valuation ring with uniformizer T and residue class field $R/(T)$ naturally isomorphic to $\mathbb{Q}_p$. Further, if a complex $K^\bullet \in D^p(\Lambda(\Gamma))$ is semisimple, then the structure theory of finitely generated $\Lambda(\Gamma)$-modules implies that in each degree i the R-module $H^i(K^\bullet_\mathfrak{p})$ is isomorphic to a direct sum of (finitely many) copies of $R/(T)$ and hence also to $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(K^\bullet)_\Gamma \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(K^\bullet)^\Gamma$.

To prove the claimed equality $r_\Gamma(B^\bullet) = r_\Gamma(A^\bullet) + r_\Gamma(C^\bullet)$ it is therefore enough to take dimensions over $\mathbb{Q}_p \cong R/(T)$ in the long exact cohomology sequence of the following short exact sequence in $C^p(R)$

$$0 \to A^\bullet_{\mathfrak{p}} \to B^\bullet_{\mathfrak{p}} \to C^\bullet_{\mathfrak{p}} \to 0. \tag{8}$$

To prove the second claim we note that if $K^\bullet \in C^p(\Lambda(\Gamma))$, then the complex $K^\bullet_{0,\mathfrak{p}} := \mathbb{Q}_p \otimes_{\Lambda(\Gamma)} K^\bullet$ is isomorphic in $D^p(\mathbb{Q}_p)$ to $\mathbb{Q}_p \otimes_R K^\bullet_{\mathfrak{p}}$. Hence, since each term of $C^\bullet_{\mathfrak{p}}$ is a projective R-module, the short exact sequence (8) gives rise to a short exact sequence in $C^p(\mathbb{Q}_p)$ of the form

$$0 \to A^\bullet_{0,\mathfrak{p}} \to B^\bullet_{0,\mathfrak{p}} \to C^\bullet_{0,\mathfrak{p}} \to 0. \tag{9}$$

Now one has a commutative diagram in $\mathcal{C}_{\mathbb{Q}_p}$

$$\begin{tikzcd}
\mathbf{d}_{\mathbb{Q}_p}(B^\bullet_{0,\mathfrak{p}}) \arrow[r] \arrow[d] & \mathbf{d}_{\mathbb{Q}_p}(A^\bullet_{0,\mathfrak{p}})\mathbf{d}_{\mathbb{Q}_p}(C^\bullet_{0,\mathfrak{p}}) \arrow[d] \\
\mathbf{d}_{\mathbb{Q}_p}(H(B^\bullet_{0,\mathfrak{p}})) \arrow[r] & \mathbf{d}_{\mathbb{Q}_p}(H(A^\bullet_{0,\mathfrak{p}}))\mathbf{d}_{\mathbb{Q}_p}(H(C^\bullet_{0,\mathfrak{p}}))
\end{tikzcd}$$

in which the upper, resp. lower, horizontal morphism is induced by (9), resp, by the long exact cohomology sequence of (9), and both vertical arrows are induced by applying property h) of $\mathbf{d}_{\mathbb{Q}_p}$ in §2.1. (For a proof of the commutativity of the above diagram see [2, Thm. 3.3].) Further, in this situation the exact sequences (5) induce short exact sequences $0 \to H^i(A^\bullet_{\mathfrak{p}}) \to H^i(A^\bullet_{0,\mathfrak{p}}) \to H^{i+1}(A^\bullet_{\mathfrak{p}}) \to 0$ (and similarly for $B^\bullet$ and $C^\bullet$) which together lie in a short exact sequence of long exact sequences

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
{} \arrow[r] & H^i(A^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^i(B^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^i(C^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^{i+1}(A^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & {} \\
{} \arrow[r] & H^i(A^\bullet_{0,\mathfrak{p}}) \arrow[r] \arrow[d] & H^i(B^\bullet_{0,\mathfrak{p}}) \arrow[r] \arrow[d] & H^i(C^\bullet_{0,\mathfrak{p}}) \arrow[r] \arrow[d] & H^{i+1}(A^\bullet_{0,\mathfrak{p}}) \arrow[r] \arrow[d] & {} \\
{} \arrow[r] & H^{i+1}(A^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^{i+1}(B^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^{i+1}(C^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^{i+2}(A^\bullet_{\mathfrak{p}}) \arrow[r] \arrow[d] & {} \\
 & 0 & 0 & 0 & 0 &
\end{tikzcd}$$

where the upper and lower, resp. central, row is the exact cohomology sequence of (8), resp. (9). It is now a straightforward exercise to derive the required equality $t(B^\bullet) = t(A^\bullet) \cdot t(C^\bullet)$ from the commutativity of both of the above diagrams. □

3.2.3. *Leading terms.* We write ρ_{triv} for the trivial representation of Γ.

Definition 3.7. *(The leading term)* For each $A^\bullet \in \Sigma_{\mathrm{ss}}$ and each morphism $a : \mathbf{1}_{\Lambda(\Gamma)} \to \mathbf{d}_{\Lambda(\Gamma)}(A^\bullet)$ in $\mathcal{C}_{\Lambda(\Gamma)}$ we define the *leading term* $(A^\bullet, a)^*(\rho_{\mathrm{triv}})$ *of the pair* $(A^\bullet, a)$ *at* ρ_{triv} to be equal to $(-1)^{r_\Gamma(A^\bullet)}$ times the element of $\mathbb{Q}_p \backslash \{0\}$ which corresponds via the canonical isomorphisms $\mathbb{Q}_p^\times \cong K_1(\mathbb{Q}_p) \cong \mathrm{Aut}_{\mathcal{C}_{\mathbb{Q}_p}}(\mathbf{1}_{\mathbb{Q}_p})$ to the composite morphism

$$\mathbf{1}_{\mathbb{Q}_p} \xrightarrow{\mathbb{Q}_p \otimes_{\Lambda(\Gamma)} a} \mathbf{d}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\Lambda(\Gamma)} A^\bullet)_{\mathbb{Q}_p} \xrightarrow{t(A^\bullet)} \mathbf{1}_{\mathbb{Q}_p}.$$

After taking Lemma 3.6 into account, it can be shown that this construction induces a well defined homomorphism of groups

$$\begin{aligned}(-)^*(\rho_{\mathrm{triv}}) : K_1(\Lambda(\Gamma), \Sigma_{\mathrm{ss}}) &\to \mathbb{Q}_p^\times \\ [A^\bullet, a] &\mapsto [A^\bullet, a]^*(\rho_{\mathrm{triv}}) := (A^\bullet, a)^*(\rho_{\mathrm{triv}}).\end{aligned}$$

In particular therefore, (property g) of the functor $\mathbf{d}_{\Lambda(\Gamma)}$ combines with relation (1) in the definition of $K_1(\Lambda(\Gamma), \Sigma_{\mathrm{ss}})$ to imply that) the notation $[A^\bullet, a]^*(\rho_{\mathrm{triv}})$ extends in a well-defined fashion to pairs of the form $(A^\bullet, a)$ where $A^\bullet \in D^p(\Lambda(\Gamma))$ is semisimple and a is a morphism in $\mathcal{C}_{\Lambda(\Gamma)}$ of the form $\mathbf{1}_{\Lambda(\Gamma)} \to \mathbf{d}_{\Lambda(\Gamma)}(A^\bullet)$.

The reason for the occurrence of ρ_{triv} in the above definition will become clear in the next subsection. In the remainder of the current section we justify the name 'leading term' by explaining the connection between $(A^\bullet, a)^*(\rho_{\mathrm{triv}})$ and the leading term (in the usual sense) of an appropriate characteristic power series.
To this end we note that Remark 3.3(i) implies that Σ_{ss} is a subcategory of the full subcategory of $C^p(\Lambda(\Gamma))$ consisting of those complexes C for which $Q(\Gamma) \otimes_{\Lambda(\Gamma)} C$ is acyclic, where we write $Q(\Gamma)$ for the quotient field of $\Lambda(\Gamma)$. Hence there exists a homomorphism

$$\mathrm{ch}_\Gamma := \mathrm{ch}_{\Lambda(\Gamma), \Sigma_{\mathrm{ss}}} : K_1(\Lambda(\Gamma), \Sigma_{\mathrm{ss}}) \to K_1(Q(\Gamma)) \cong Q(\Gamma)^\times.$$

Now the identification between $\Lambda(\Gamma)$ and the power series ring $\mathbb{Z}_p[[T]]$ (which, of course, depends on the choice of $T = \gamma - 1$) allows any element F of $Q(\Gamma)^\times$ to be written uniquely as

$$F(T) = T^r G(T) \tag{10}$$

with $r = r(F) \in \mathbb{Z}$ and $G(T) \in Q(\Gamma)$ such that $G(0) \in \mathbb{Q}_p^\times$. The leading coefficient of F with respect to its expansion in the Laurent series ring $\mathbb{Q}_p\{\{T\}\}$ is therefore equal to $F^*(0) := G(0)$.

Proposition 3.8. *Let $A^\bullet$ be any object of $D^p(\Lambda(\Gamma))$ which is semisimple and a any morphism in $\mathcal{C}_{\Lambda(\Gamma)}$ of the form $\mathbf{1}_{\Lambda(\Gamma)} \to \mathbf{d}_{\Lambda(\Gamma)}(A^\bullet)$.*

(i) (Order of vanishing) *For $\mathcal{L} := [A^\bullet, a]$ one has $r(\mathrm{ch}_\Gamma(\mathcal{L})) = r_\Gamma(A^\bullet)$.*

(ii) (Leading terms) *One has a commutative diagram of abelian groups*

$$\begin{tikzcd}
K_1(\Lambda(\Gamma), \Sigma_{\mathrm{ss}}) \arrow[r, "\mathrm{ch}_\Gamma"] \arrow[d, "(-)^*(\rho_{\mathrm{triv}})"'] & K_1(Q(\Gamma)) \arrow[d, "(-)^*(0)"] \\
\mathbb{Q}_p^\times \arrow[r, equal] & \mathbb{Q}_p^\times .
\end{tikzcd}$$

Proof. We use the localization R of $\Lambda(\Gamma)$ that was introduced in the proof of Lemma 3.6.

It is easy to see that both of the homomorphisms $(-)^*(\rho_{\mathrm{triv}})$ and ch_Γ factor via the flat base change $R \otimes_{\Lambda(\Gamma)} -$ through $K_1(R, \Xi)$, where Ξ denotes the full subcategory of $C^p(R)$ consisting of those complexes $K^\bullet$ with the property that in each degree i the R-module $H^i(K^\bullet)$ is isomorphic to a direct sum of (finitely many) copies of $R/(T)$. Thus it suffices to show the commutativity of the above diagram with $K_1(\Lambda(\Gamma), \Sigma_{\mathrm{ss}})$ replaced by $K_1(R, \Xi)$. Moreover, by Lemma 3.9 below this is reduced to the case where $A^\bullet$ is a complex of the form $R \xrightarrow{d} R$ where R occurs in degrees -1 and 0 and d denotes multiplication by either T or 1. Further, since the complex $R \xrightarrow{\times 1} R$ is acyclic we shall therefore assume that d denotes multiplication by T.

Now $\mathrm{Mor}_{\mathcal{C}_R}(\mathbf{1}_R, \mathbf{d}_R(A^\bullet))$ is a $K_1(R)$-torsor and so all possible trivializations arise in the following way: if ϵ is any fixed element of $R^\times$, then the R-module homomorphism $R \to A^{-1}$, resp. $R \to A^0$, that sends $1 \in R$ to $1 \in R$, resp. to $\epsilon \in R$, induces a morphism $can_1 : \mathbf{d}_R(R) \to \mathbf{d}_R(A^{-1})$, resp. $can_\epsilon : \mathbf{d}_R(R) \to \mathbf{d}_R(A^0)$, in $\mathcal{C}_R$, and hence also a morphism $a_\epsilon := (can_1)^{-1} \cdot can_\epsilon : \mathbf{1}_R \to \mathbf{d}_R(A^\bullet)$. Setting $\mathcal{L}_\epsilon := [A^\bullet, a_\epsilon] \in K_1(R, \Xi)$, one checks easily that $\mathrm{ch}_\Gamma(\mathcal{L}_\epsilon) = T^{-1}\epsilon$ and thus $\mathrm{ch}_\Gamma(\mathcal{L}_\epsilon)^*(0) = \epsilon(0)$. On the other hand, the Bockstein homomorphism $\mathfrak{B}_1$ of the triple $(A^\bullet, R/(T), \gamma)$ is equal to $\mathbb{Q}_p \xrightarrow{-1} \mathbb{Q}_p$ as one checks by using the description given in the proof of Lemma 3.1. Thus $\mathcal{L}_\epsilon^*(\rho_{\mathrm{triv}})$ is, by definition, equal to $(-1)^{r_\Gamma(A^\bullet)}$ times the determinant of

$$\mathbb{Q}_p \xrightarrow{\epsilon(0)} \mathbb{Q}_p \xrightarrow{(\mathfrak{B}_1)^{-1}=-1} \mathbb{Q}_p \xrightarrow{1} \mathbb{Q}_p.$$

Hence, observing that $r_\Gamma(A^\bullet) = -1 = r(\mathrm{ch}_\Gamma(\mathcal{L}_\epsilon))$, we have $\mathcal{L}_\epsilon^*(\rho_{\mathrm{triv}}) = \epsilon(0) = \mathrm{ch}_\Gamma(\mathcal{L}_\epsilon)^*(0)$. This proves both claims of the Proposition. □

Lemma 3.9. *Let R be a discrete valuation ring with uniformizer T and assume that $A^\bullet \in C^p(R)$ is such that in each degree i the R-module $H^i(A^\bullet)$ is annihilated by T. Then $A^\bullet$ is isomorphic in $C^p(R)$ to the direct sum of finitely many complexes of the form $R \to R$ where the differential is equal to multiplication by either* 1 *or* T.

Proof. Assume that m is the maximal degree such that $A^m \neq 0$ and fix an isomorphism $D : R^d \cong A^m$. Let $(e_1, \ldots, e_d)$ be the standard basis of R^d. Then, by assumption, for each integer i with $1 \leq i \leq d$, one has $Te_i \in \mathrm{im}(D^{-1} \circ d^{m-1})$. For each such i we set $h_i := 1$ if $e_i \in \mathrm{im}(D^{-1} \circ d^{m-1})$ and, otherwise, we set $h_i := T$. We write H for the diagonal $d \times d$-matrix with entries $h_1, \ldots, h_d$.

Then, since the image of the map $R^d \xrightarrow{H} R^d$ is equal to $\mathrm{im}(D^{-1} \circ d^{m-1})$, there exists a retraction $E : R^d \to A^{m-1}$ (i.e. with left inverse '$H^{-1} \circ D^{-1} \circ d^{m-1}$') that makes the following diagram commutative

$$\begin{tikzcd}
{} \arrow[r] & 0 \arrow[r] \arrow[d] & R^d \arrow[r, "H"] \arrow[d, "E"'] & R^d \arrow[r] \arrow[d, "D"'] & 0 \arrow[r] \arrow[d] & {} \\
{} \arrow[r] & A^{m-2} \arrow[r, "d^{m-2}"] & A^{m-1} \arrow[r, "d^{m-1}"] & A^m \arrow[r, "d^m"] & 0 \arrow[r] & {}
\end{tikzcd}.$$

Now if $B^\bullet$ denotes the upper row of this diagram and $C^\bullet := A^\bullet/B^\bullet$ the associated quotient complex (not the mapping cone!), then one checks readily that there exists a *split* exact sequence $0 \to B^\bullet \to A^\bullet \to C^\bullet \to 0$. This implies that $C^\bullet$ belongs to $C^p(R)$ and has cohomology annihilated by T (in all degrees). Thus, since the length of $C^\bullet$ is strictly shorter than the length of $A^\bullet$, the proof can be completed by induction. □

Remark 3.10. It will be clear to the reader that analogous statements hold for all results of this subsection if we replace $\mathbb{Z}_p$ by $\mathcal{O}$, $\mathbb{Q}_p$ by L, $\Lambda(\Gamma)$ by $\Lambda_{\mathcal{O}}(\Gamma) := \mathcal{O}[[\Gamma]]$ and $Q(\Gamma)$ by the quotient field $Q_{\mathcal{O}}(\Gamma)$ of $\Lambda_{\mathcal{O}}(\Gamma)$.

3.3. The general case.

We extend the constructions of §3.2 to the setting of the Bockstein homomorphisms that are discussed at the end of §3.1.

If $A^\bullet \in C^p(\Lambda(G))$, then for any continuous representation of G of the form $\rho : G \to \mathrm{GL}_n(\mathcal{O})$ we regard the complex

$$A^\bullet(\rho^*) := \mathcal{O}^n \otimes_{\mathbb{Z}_p} A^\bullet$$

as a complex of (left) $\Lambda_{\mathcal{O}}(G)$-modules by means of the following G-action: $g(x \otimes_{\mathbb{Z}_p} a) := \rho^*(g)(x) \otimes_{\mathbb{Z}_p} g(a)$ for each $g \in G$, $x \in \mathcal{O}^n$ and $a \in A^i$. With this action, there exists a natural isomorphism in $C^p(\mathbb{Z}_p)$ between $\mathbb{Z}_p \otimes_{\Lambda(G)} A^\bullet(\rho^*)$ and the complex $\mathcal{O}^n \otimes_{\Lambda(G)} A^\bullet$ that occurs in §3.1. Further, it can be shown that the Bockstein homomorphisms $\mathfrak{B}_\bullet$ of the triple $(A^\bullet, T_\rho, \gamma)$ give rise to a complex of the form $(\mathbb{H}_\bullet(G, A^\bullet(\rho^*)), \mathfrak{B}_\bullet)$ where for each integer i and each normal closed subgroup J of G we set

$$\mathbb{H}_i(J, A^\bullet(\rho^*))) := H^{-i}(\mathbb{Z}_p \otimes_{\Lambda(J)} A^\bullet(\rho^*)) \cong \mathbb{T}\mathrm{or}_i^{\Lambda(J)}(T_\rho, A^\bullet)$$

(see, for example, the proof of Lemma 3.13 below).

Definition 3.11. *(Semisimplicity at ρ)* For each $A^\bullet \in D^p(\Lambda(G))$ we set

$$r_G(A^\bullet)(\rho) := \sum_{i \in \mathbb{Z}} (-1)^{i+1} \dim_L \left(\mathbb{H}_i(H, A^\bullet(\rho^*))^\Gamma \otimes_{\mathcal{O}} L \right) \in \mathbb{Z},$$

where L is the fraction field of $\mathcal{O}$. We say that a complex $A^\bullet \in D^p(\Lambda(G))$ is *semisimple at ρ* if the cohomology of the associated complex $(\mathbb{H}_\bullet(G, A^\bullet(\rho^*)), \mathfrak{B}_\bullet)$ is $\mathbb{Z}_p$-torsion in each degree. We let $\Sigma_{\mathrm{ss}-\rho}$ denote the full subcategory of $C^p(\Lambda(G))$ consisting of those complexes that are semisimple at ρ, and we note that $\Sigma_{\mathrm{ss}-\rho}$ satisfies the conditions (i), (ii), (iii) and (iv$'$) that are described in §2.

Definition 3.12. *(Finiteness at ρ)* We say that a complex $A^\bullet \in D^p(\Lambda(G))$ is *finite at ρ* if the groups $\mathbb{H}_i(G, A^\bullet(\rho^*))$ are $\mathbb{Z}_p$-torsion in all degrees i. We let $\Sigma_{\text{fin}-\rho}$ denote the full subcategory of $C^p(\Lambda(G))$ consisting of those complexes that are finite at ρ, and we note that $\Sigma_{\text{fin}-\rho}$ satisfies the conditions (i), (ii), (iii) and (iv) that are described in §2. In particular we have $\Sigma_{\text{fin}-\rho} \subseteq \Sigma_{\text{ss}-\rho}$.

In the next result we consider the tensor product $\Lambda_{\mathcal{O}}(\Gamma) \otimes_{\mathcal{O}} \mathcal{O}^n$ as an $(\Lambda_{\mathcal{O}}(\Gamma), \Lambda(G))$-bimodule where $\Lambda_{\mathcal{O}}(\Gamma)$ acts by multiplication on the left and $\Lambda(G)$ acts on the right via the rule $(\tau \otimes_{\mathcal{O}} x)g := \tau\bar{g} \otimes_{\mathcal{O}} \rho(g)^t(x)$ for each $g \in G$ (with image $\bar{g}$ in Γ), $x \in \mathcal{O}^n$ and $\tau \in \Lambda_{\mathcal{O}}(\Gamma)$. For each complex $A^\bullet \in \Sigma_{\text{ss}-\rho}$ we then set

$$A^\bullet_\rho := (\Lambda_{\mathcal{O}}(\Gamma) \otimes_{\mathcal{O}} \mathcal{O}^n) \otimes_{\Lambda(G)} A^\bullet \in C^p(\Lambda_{\mathcal{O}}(\Gamma)).$$

Lemma 3.13. *Fix $A^\bullet \in C^p(\Lambda(G))$.*

(i) *There are natural quasi-isomorphisms in $C^p(\Lambda_{\mathcal{O}}(\Gamma))$ of the form*

$$A^\bullet_\rho \cong \Lambda_{\mathcal{O}}(\Gamma) \otimes_{\Lambda_{\mathcal{O}}(G)} A^\bullet(\rho^*) \cong \mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(H)} A^\bullet(\rho^*).$$

(ii) *One has $r_G(A^\bullet)(\rho) = r_\Gamma(A^\bullet_\rho)$.*

(iii) *The Bockstein homomorphism in any given degree of $(A^\bullet, T_\rho, \gamma)$ (as defined in §3.1) coincides with the Bockstein homomorphism in the same degree of $(A^\bullet_\rho, \mathbb{Z}_p, \gamma)$.*

(iv) *One has $A^\bullet \in \Sigma_{\text{ss}-\rho}$ if and only if $A^\bullet_\rho \in \Sigma_{\text{ss}}$ (when considered as an object of $C^p(\Lambda_{\mathcal{O}}(\Gamma))$). Further, if this is the case, then the trivialization*

$$t(A^\bullet_\rho) : \mathbf{d}_{\mathcal{O}}(\mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(\Gamma)} A^\bullet_\rho)_L \to \mathbf{1}_L$$

that is defined as in (7) *coincides with the composite morphism*

$$\begin{aligned} (11) \quad t(A^\bullet(\rho^*)) : \mathbf{d}_{\mathcal{O}}(\mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(G)} A^\bullet(\rho^*))_L &\cong \mathbf{d}_{\mathcal{O}}((\mathbb{H}_\bullet(G, A^\bullet(\rho^*)), 0))_L \\ &= \mathbf{d}_{\mathcal{O}}((\mathbb{H}_\bullet(G, A^\bullet(\rho^*)), \mathfrak{B}_\bullet))_L \cong \mathbf{1}_L \end{aligned}$$

where the first, resp. last, morphism uses property h) (in §2.1) for the functor $\mathbf{d}_{\mathcal{O}}$, resp. property i) for the homomorphism $\mathcal{O} \to L$ and then property e) for the functor $\mathbf{d}_L$.

(v) *If $A^\bullet, B^\bullet$ and $C^\bullet$ are objects of $\Sigma_{\text{ss}-\rho}$ which together lie in a short exact sequence in $C^p(\Lambda(G))$ of the form*

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0,$$

then one has

$$r_G(B^\bullet)(\rho) = r_G(A^\bullet)(\rho) + r_G(C^\bullet)(\rho)$$

and, with respect to the canonical morphism

$$\mathbf{d}_{\mathcal{O}}(\mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(G)} B^\bullet(\rho^*))_L = \mathbf{d}_{\mathcal{O}}(\mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(G)} A^\bullet(\rho^*))_L \cdot \mathbf{d}_O(\mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(G)} C^\bullet(\rho^*))_L$$

that is induced by the given short exact sequence, one has

$$t(B^\bullet(\rho^*)) = t(A^\bullet(\rho^*)) \cdot t(C^\bullet(\rho^*)).$$

Proof. Claim (i) is clear (given the specified actions). Claim (ii) then follows by using the isomorphisms of claim (i) to directly compare the definitions of $r_G(A^\bullet)(\rho)$ and $r_\Gamma(A^\bullet_\rho)$. In a similar way, claims (iii) and (iv) follow from the functorial construction of Bockstein homomorphisms and the fact that there are natural isomorphisms in $C^p(\mathcal{O})$ of the form

$$\begin{aligned} \mathcal{O}^n \otimes_{\Lambda(G)} A^\bullet &\cong \mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(G)} A^\bullet(\rho^*) \\ &\cong \mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(\Gamma)} \big(\Lambda_{\mathcal{O}}(\Gamma) \otimes_{\Lambda_{\mathcal{O}}(G)} A^\bullet(\rho^*)\big) \\ &\cong \mathbb{Z}_p \otimes_{\Lambda(\Gamma)} A^\bullet_\rho. \end{aligned}$$

Finally, to prove claim (v) we observe that, by claim (i), the given short exact sequence gives rise to a short exact sequence of semisimple complexes in $C^p(\Lambda_{\mathcal{O}}(\Gamma))$ of the form

$$0 \to A^\bullet_\rho \to B^\bullet_\rho \to C^\bullet_\rho \to 0.$$

The equalities of claim (v) thus follow from claims (ii), (iii) and (iv) and the results of Lemma 3.6 as applied to the last displayed short exact sequence. □

Definition 3.14. *(The leading term at ρ)* For each complex $A^\bullet \in \Sigma_{\mathrm{ss}-\rho}$ and each morphism $a : \mathbf{1}_{\Lambda(G)} \to \mathbf{d}_{\Lambda(G)}(A^\bullet)$ in $\mathcal{C}_{\Lambda(G)}$ we define the *leading term* $(A^\bullet, a)^*(\rho)$ *of the pair* $(A^\bullet, a)$ *at* ρ to be equal to $(-1)^{r_G(A^\bullet)(\rho)}$ times the element of $L \setminus \{0\}$ which corresponds via the canonical isomorphisms $L^\times \cong K_1(L) \cong \mathrm{Aut}_{\mathcal{C}_L}(\mathbf{1}_L)$ to the composite morphism

$$\mathbf{1}_L \xrightarrow{L^n \otimes_{\Lambda(G)} a} \mathbf{d}_L(L^n \otimes_{\Lambda(G)} A^\bullet) \xrightarrow{t(A^\bullet(\rho^*))} \mathbf{1}_L.$$

Then, since $\Sigma_{A^\bullet} \subset \Sigma_{\mathrm{ss}-\rho}$, Lemma 3.13(v) can be used to show that this construction induces a well-defined homomorphism of groups

$$\begin{aligned} (-)^*(\rho) : K_1(\Lambda(G), \Sigma_{A^\bullet}) &\to L^\times \\ [A^\bullet, a] &\mapsto [A^\bullet, a]^*(\rho) := (A^\bullet, a)^*(\rho). \end{aligned}$$

In particular, (property g) of the functor $\mathbf{d}_{\Lambda(G)}$ combines with relation (1) in the definition of $K_1(\Lambda(G), \Sigma_{A^\bullet})$ to imply that) the notation $[A^\bullet, a]^*(\rho)$ extends in a well-defined fashion to pairs of the form $(A^\bullet, a)$ where $A^\bullet \in D^p(\Lambda(G))$ is semisimple at ρ and a is a morphism in $\mathcal{C}_{\Lambda(G)}$ of the form $\mathbf{1}_{\Lambda(G)} \to \mathbf{d}_{\Lambda(G)}(A^\bullet)$.

If $A^\bullet$ is clear from the context, then we often write $a^*(\rho)$ in place of $[A^\bullet, a]^*(\rho)$. It is easily checked that (in the case $G = \Gamma$ and $\rho = \rho_{\mathrm{triv}}$) these definitions are compatible with those given in §3.2. Further, in §3.4.3 we shall reinterpret the expression $[A^\bullet, a]^*(\rho)$ defined above as the leading term at $s = 0$ of a natural p-adic meromorphic function.

Remark 3.15. If $A^\bullet \in D^p(\Lambda(G))$ is both semisimple at ρ and such that $r_G(A^\bullet)(\rho) = 0$ (which is the case, for example, if $A^\bullet$ is finite at ρ), then we set $[A^\bullet, a](\rho) := [A^\bullet, a]^*(\rho)$ and refer to this as the *value of* $[A^\bullet, a]$ *at* ρ. In particular, after taking account of Remark 3.5, it is clear that this definition coincides with that given in [16, 4.1.5].

3.4. Canonical localizations. We apply the constructions of §3.3 in the setting of the canonical localizations of $\Lambda(G)$ that were introduced in [11].

3.4.1. *The canonical Ore sets.* We recall from [11, §2-§3] that there are canonical left and right denominator sets S and S^* of $\Lambda(G)$ where

$$S := \{\lambda \in \Lambda(G) : \Lambda(G)/\Lambda(G)\lambda \text{ is a finitely generated } \Lambda(H)\text{-module}\}$$

and

$$S^* := \bigcup_{i\geq 0} p^i S.$$

We write S^*-tor for the category of finitely generated $\Lambda(G)$-modules M which satisfy $\Lambda(G)_{S^*} \otimes_{\Lambda(G)} M = 0$. We further recall from loc. cit. that a finitely generated $\Lambda(G)$-module M belongs to S^*-tor, if and only if $M/M(p)$ is finitely generated when considered as a $\Lambda(H)$-module (by restriction) where $M(p)$ denotes the submodule of M consisting of those elements that are annihilated by some power of p.

3.4.2. *Leading terms.* In this subsection we use the notation of Definition 3.14 and the isomorphism $K_1(\Lambda(G), \Sigma_{S^*}) \cong K_1(\Lambda(G)_{S^*})$ described at the end of §2.2.
If $\rho : G \to \mathrm{GL}_n(\mathcal{O})$ is any continuous representation and $A^\bullet$ any object of Σ_{S^*}, then $\Sigma_{A^\bullet} \subset \Sigma_{S^*}$ and so there exists a canonical homomorphism

$$\mathrm{ch}_{G,A^\bullet} := \mathrm{ch}_{\Lambda(G),\Sigma_{A^\bullet}} : K_1(\Lambda(G), \Sigma_{A^\bullet}) \to K_1(\Lambda(G), \Sigma_{S^*}) \cong K_1(\Lambda(G)_{S^*}).$$

In addition, the ring homomorphism $\Lambda(G)_{S^*} \to M_n(Q(\Gamma))$ which sends each element $g \in G$ to $\rho(g)\bar{g}$ where $\bar{g}$ denotes the image of g in Γ, induces a homomorphism of groups

$$\rho_* : K_1(\Lambda(G)_{S^*}) \to K_1(M_n(Q_{\mathcal{O}}(\Gamma))) \cong K_1(Q_{\mathcal{O}}(\Gamma)) \cong Q_{\mathcal{O}}(\Gamma)^\times.$$

Proposition 3.16. *Let $A^\bullet$ be a complex which belongs to both Σ_{S^*} and $\Sigma_{\mathrm{ss}-\rho}$.*

(i) (Order of vanishing) *One has $r_G(A^\bullet)(\rho) = r_\Gamma(A^\bullet_\rho) = r(\rho_* \circ \mathrm{ch}_{G,A^\bullet}(A^\bullet))$.*

(ii) (Leading terms) *The following diagram of abelian groups commutes*

$$\begin{tikzcd}
K_1(\Lambda(G), \Sigma_{A^\bullet}) \arrow[r, "\mathrm{ch}_{G,A^\bullet}"] \arrow[d, "(-)^*(\rho)"'] & K_1(\Lambda(G)_{S^*}) \arrow[d, "(\rho_*(-))^*(0)"] \\
L^\times \arrow[r, equal] & L^\times,
\end{tikzcd}$$

where $(-)^*(0)$ denotes the 'leading term' homomorphism $K_1(Q_{\mathcal{O}}(\Gamma)) \to L^\times$ which occurs in Proposition 3.8 (and Remark 3.10).

Proof. By Lemma 3.13(i) one has $\mathbb{H}_i(H, A^\bullet(\rho^*)) = H^{-i}(\mathcal{O} \otimes_{\Lambda_{\mathcal{O}}(H)} A^\bullet(\rho^*)) = H^{-i}(A^\bullet_\rho)$ in each degree i. Thus, after taking account of Proposition 3.8 (and Remark 3.10), claim (i) follows directly from Definitions 3.2 and 3.11.

Claim (ii) is proved by the same argument as used in [16, Lem. 4.3.10]. Indeed, one need only observe that the above diagram arises as the following composite commutative diagram

$$\begin{tikzcd}
K_1(\Lambda(G), \Sigma_{A^\bullet}) \arrow[r, "\mathrm{ch}_{\Lambda(G),\Sigma_{A^\bullet}}"] \arrow[d, "(\Lambda_{\mathcal{O}}(\Gamma)\otimes_{\mathcal{O}}\mathcal{O}^n)\otimes_{\Lambda(G)} -"'] & K_1(\Lambda(G)_{S^*}) \arrow[d, "\rho_*"] \\
K_1(\Lambda_{\mathcal{O}}(\Gamma), \Sigma_{\mathrm{ss}}) \arrow[r, "\mathrm{ch}_{\Lambda_{\mathcal{O}}(\Gamma),\Sigma_{\mathrm{ss}}}"] \arrow[d, "(-)^*(\rho_{\mathrm{triv}})"'] & K_1(Q_{\mathcal{O}}(\Gamma)) \arrow[d, "(-)^*(0)"] \\
L^\times \arrow[r, equal] & L^\times
\end{tikzcd}$$

where the lower square is as in Proposition 3.8. □

For any element F of $K_1(\Lambda(G)_{S^*})$ we write $F^*(\rho)$ for the *leading term* $(\rho_*(F))^*(0)$ *of* F *at* ρ. By Proposition 3.16, this notation is consistent with that of Definition 3.14 in the case that F belongs to the image of $\mathrm{ch}_{G,A^\bullet}$. In a similar way, if $r(\rho_*(F)) = 0$, then we shall use the notation $F(\rho) := F^*(\rho)$.

3.4.3. *Partial derivatives.* We now observe that the constructions of the previous section allow an interpretation of the expression $(A^\bullet, a)^*(\rho)$ defined in §3.3 as the leading term (in the usual sense) at $s = 0$ of a natural p-adic meromorphic function.

At the outset we fix a representation of G of the form $\chi : G \twoheadrightarrow \Gamma \to \mathbb{Z}_p^\times$ which has infinite order and set

$$c_{\chi,\gamma} := \log_p(\chi(\gamma)) \in \mathbb{Q}_p^\times.$$

We also fix an object $A^\bullet$ of Σ_{S^*} and a morphism $a : \mathbf{1}_{\Lambda(G)} \to \mathbf{d}_{\Lambda(G)}(A^\bullet)$ in $\mathcal{C}_{\Lambda(G)}$, we set $\mathcal{L} := [A^\bullet, a] \in K_1(\Lambda(G), \Sigma_{A^\bullet})$ and for any continuous representation $\rho : G \to \mathrm{GL}_n(\mathcal{O})$ we define

$$f_\rho(T) := \rho_*(\mathrm{ch}_{G,A^\bullet}(\mathcal{L})) \in K_1(Q_{\mathcal{O}}(\Gamma)) \cong Q_{\mathcal{O}}(\Gamma)^\times.$$

Then, since the zeros and poles of elements of $Q_{\mathcal{O}}(\Gamma)$ are discrete, the function

$$s \mapsto f_{\mathcal{L}}(\rho\chi^s) := f_\rho(\chi(\gamma)^s - 1)$$

is a p-adic meromorphic function on $\mathbb{Z}_p$.

Lemma 3.17. *Let $A^\bullet$ and a be as above and set $r := r_G(A^\bullet)(\rho)$. Then,*

(*i*) *in any sufficiently small neighbourhood U of 0 in $\mathbb{Z}_p$ one has*

$$\mathcal{L}^*(\rho\chi^s) = \mathcal{L}(\rho\chi^s) = f_{\mathcal{L}}(\rho\chi^s)$$

for all $s \in U \setminus \{0\}$,

(*ii*) *$c^r_{\chi,\gamma}\mathcal{L}^*(\rho)$ is the (usual) leading coefficient at $s = 0$ of $f_{\mathcal{L}}(\rho\chi^s)$, and*

(*iii*) *if $r \geq 0$, then one has*

$$c^r_{\chi,\gamma}\mathcal{L}^*(\rho) = \frac{1}{r!}\frac{\mathrm{d}^r}{\mathrm{d}s^r} f_{\mathcal{L}}(\rho\chi^s)\Big|_{s=0}.$$

Proof. If U is any sufficiently small neighbourhood of 0 in $\mathbb{Z}_p$, then one has $f_{\rho\chi^s}(0) \in L^\times$ for all $s \in U \setminus \{0\}$. Since $f_{\rho\chi^s}(T) = f_\rho(\chi(\gamma)^s(T+1)-1)$ we may therefore deduce from Proposition 3.16 that $\mathcal{L}^*(\rho\chi^s) = \mathcal{L}(\rho\chi^s) = f_{\rho\chi^s}(0) = f_\rho(\chi(\gamma)^s - 1) = f_{\mathcal{L}}(\rho\chi^s)$ for any $s \in U \setminus \{0\}$. This proves claim (i).

In addition, if $r \geq 0$ and we factorize $f_\rho(T)$ as $T^r G_\rho(T)$ with $G_\rho(T) \in Q_{\mathcal{O}}(\Gamma)$, then $G_\rho(0) = f_\rho^*(0)$ and

$$\begin{aligned} \frac{1}{r!}\frac{\mathrm{d}^r}{\mathrm{d}s^r} f_{\mathcal{L}}(\rho\chi^s)\big|_{s=0} &= \lim_{0\neq s\to 0} \frac{f_\rho(\chi(\gamma)^s-1)}{s^r} \\ &= \lim_{0\neq s\to 0} \big(\frac{(\chi(\gamma)^s-1)^r}{s^r}\, G_\rho(\chi(\gamma)^s-1)\big) \\ &= \big(\lim_{0\neq s\to 0} \frac{\chi(\gamma)^s-1}{s}\big)^r G_\rho(0) \\ &= (\log_p(\chi(\gamma)))^r f_\rho^*(0) \\ &= c_{\chi,\gamma}^r \mathcal{L}^*(\rho), \end{aligned}$$

where the last equality follows from Proposition 3.16. This proves claim (iii). Also, if $r < 0$, then (whilst we no longer have the interpretation of the limit as a partial derivative) the same arguments prove the statement concerning the leading coefficient at $s = 0$ that is made in claim (ii). □

Remark 3.18. Lemma 3.17 is of particular interest in the case that χ is equal to the cyclotomic character of G when the above calculus can be interpreted as partial derivation in the 'cyclotomic' direction (cf. Remark 5.6).

3.5. Generalized Euler-Poincaré characteristics. In this subsection we show that the constructions made in §3.3 give rise to a natural extension of certain results from [11, 16, 38].

To do this we fix a continuous representation $\rho : G \to \mathrm{GL}_n(\mathcal{O})$ and a complex $A^\bullet \in \Sigma_{\mathrm{ss}-\rho}$ and in each degree i we set

$$H^i_{\mathfrak{B}}(G, A^\bullet(\rho^*)) := H^i\big((\mathbb{H}_{-\bullet}(G, A^\bullet(\rho^*)), \mathfrak{B}_{-\bullet})\big).$$

We then define the (generalized) additive, respectively multiplicative, Euler-Poincaré characteristic of the complex $A^\bullet(\rho^*)$ by setting

$$\chi_{\mathrm{add}}(G, A^\bullet(\rho^*)) := \sum_{i\in\mathbb{Z}} (-1)^i \mathrm{length}_{\mathcal{O}}\big(H^i_{\mathfrak{B}}(G, A^\bullet(\rho^*))\big),$$

respectively

$$\chi_{\mathrm{mult}}(G, A^\bullet(\rho^*)) := (\#\kappa_L)^{\chi_{\mathrm{add}}(G, A^\bullet(\rho^*))}$$

where κ_L denotes the residue class field of L. We recall that for a single $\Lambda(G)$-module M, or rather its Pontryagin-dual D, similar Euler characteristics have already been studied by several other authors (cf. [12, 42, 18]). Indeed, they use the Hochschild-Serre spectral sequence to construct differentials

$$d^i : H^i(G, D) \to H^i(H, D)^\Gamma \to H^i(H, D)_\Gamma \to H^{i+1}(G, D)$$

where the second arrow is induced by the identity map on $H^i(H, D)$; then the generalized Euler characteristics studied in loc. cit. are defined just as above but by using the complex $(H^\bullet(G,D),d^\bullet)$ in place of $(\mathbb{H}_{-\bullet}(G,-),\mathfrak{B}_{-\bullet})$. However, Lemma 3.13(i) implies that the Pontryagin dual of d^i is equal to the Bockstein homomorphism $\mathfrak{B}_{i+1}:\mathbb{H}_{i+1}(G,P^\bullet)\to\mathbb{H}_i(G,P^\bullet)$ where $P^\bullet$ is a projective resolution of M.

Proposition 3.19. *Let* ord_L *denote the valuation of* L *which takes the value* 1 *on any uniformizing parameter and* $|-|_p$ *the* p*-adic absolute value, normalized so that* $|p|_p=p^{-1}$.
If $A^\bullet\in\Sigma_{\mathrm{ss}-\rho}$ *and* $a:\mathbf{1}_{\Lambda(G)}\to\mathbf{d}_{\Lambda(G)}(A^\bullet)$ *is any morphism in* $\mathcal{C}_{\Lambda(G)}$*, then for* $\mathcal{L}:=[A^\bullet,a]$ *one has*

$$\chi_{\mathrm{add}}(G,A^\bullet(\rho^*))=\mathrm{ord}_L(\mathcal{L}^*(\rho))$$

and

$$\chi_{\mathrm{mult}}(G,A^\bullet(\rho^*))=|\mathcal{L}^*(\rho)|_p^{-[L:\mathbb{Q}_p]}.$$

Proof. We observe first that by combining Lemma 3.13 with property h) in §2.1 (with $R=\mathcal{O}$) we obtain canonical morphisms

$$\begin{aligned}\mathbf{1}_{\mathcal{O}}\xrightarrow{\mathcal{O}^n\otimes_{\Lambda(G)}a}\mathbf{d}_{\mathcal{O}}(\mathcal{O}^n\otimes_{\Lambda(G)}A^\bullet)\;&\cong\;\mathbf{d}_{\mathcal{O}}(\mathcal{O}\otimes_{\Lambda_{\mathcal{O}}(G)}A^\bullet(\rho^*)))\\ &\cong\;\mathbf{d}_{\mathcal{O}}((\mathbb{H}_{-\bullet}(G,A^\bullet(\rho^*)),\mathfrak{B}_{-\bullet}))\\ &\cong\;\prod_{i\in\mathbb{Z}}\mathbf{d}_{\mathcal{O}}\big(H^i_{\mathfrak{B}}(G,A^\bullet(\rho^*))\big)^{(-1)^i}.\end{aligned}$$

After applying $L\otimes_{\mathcal{O}}-$ to this composite morphism and then identifying all factors in the product expression with $\mathbf{1}_L$ by acyclicity we recover the definition of the leading term $\mathcal{L}^*(\rho):=(A^\bullet,a)^*(\rho)$. On the other hand, if we take the product over all i of any arbitrarily chosen maps $f_i:\mathbf{1}_{\mathcal{O}}\to\mathbf{d}_{\mathcal{O}}\big(H^i_{\mathfrak{B}}(G,A^\bullet(\rho^*))\big)^{(-1)^i}$, this will coincide with the above map modulo $\mathcal{O}^\times$. Thus the product over all i of the maps

$$(\mathbf{1}_{\mathcal{O}})_L\xrightarrow{(f_i)_L}\mathbf{d}_{\mathcal{O}}\big(H^i_{\mathfrak{B}}(G,A^\bullet(\rho^*))\big)_L^{(-1)^i}\xrightarrow{acyc}\mathbf{1}_L\ ,$$

which calculate the length of $H^i_{\mathfrak{B}}(G,A^\bullet(\rho^*))$ by Remark 2.4, differs from $\mathcal{L}^*(\rho)$ only by a unit in $\mathcal{O}$ and hence the claimed result follows. □

Remark 3.20. If the complex $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}A^\bullet(\rho^*)$ is acyclic, then the leading term $\mathcal{L}^*(\rho)$ is equal to the value of $\mathcal{L}$ at ρ (in the sense of Remark 3.15). This implies that Proposition 3.19 recovers the results of [11, Thm. 3.6], [38, Prop. 6.3] and [16, Rem. 4.1.13].

4. Global Zeta isomorphisms

In this section we recall the non-commutative Tamagawa Number Conjecture that has been formulated by Fukaya and Kato.

4.1. Galois cohomology. The main reference for this section is [16, §1.6], but see also [7]; here we use the same notation as in the survey article [39]. For simplicity we assume throughout this section that p is odd.

We fix a finite set S of places of $\mathbb{Q}$ which contains both $S_p := \{p\}$ and $S_\infty := \{\infty\}$ and let U denote the corresponding dense open subset $\mathrm{Spec}(\mathbb{Z}[\frac{1}{S}])$ of $\mathrm{Spec}(\mathbb{Z})$. We fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and, for each place v of $\mathbb{Q}$, an algebraic closure $\bar{\mathbb{Q}}_v$ of $\mathbb{Q}_v$. We then set $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $G_{\mathbb{Q}_v} := \mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v)$ and write G_S for the Galois group of the maximal extension of $\mathbb{Q}$ inside $\bar{\mathbb{Q}}$ which is unramified outside S. If X is any topological abelian group which is endowed with a continuous action of G_S, then we write $\mathrm{R}\Gamma(U, X)$ $(\mathrm{R}\Gamma_c(U, X))$ for global Galois cohomology with restricted ramification (and compact support) and for any place v of $\mathbb{Q}$ we denote by $\mathrm{R}\Gamma(\mathbb{Q}_v, X)$ the corresponding local Galois cohomology complex.

We let L denote a finite extension of $\mathbb{Q}_p$, we write $\mathcal{O}$ for the valuation ring of L and we let V denote a finite dimensional L-vector space which is endowed with a continuous action of $G_{\mathbb{Q}}$. Then the 'finite parts' of global and local Galois cohomology are written as $\mathrm{R}\Gamma_f(\mathbb{Q}, V)$ and $\mathrm{R}\Gamma_f(\mathbb{Q}_v, V)$ respectively, and there exists a canonical exact triangle of the form

(12)
$$\mathrm{R}\Gamma_c(U, V) \longrightarrow \mathrm{R}\Gamma_f(\mathbb{Q}, V) \longrightarrow \bigoplus_{v\in S} \mathrm{R}\Gamma_f(\mathbb{Q}_v, V) \longrightarrow \mathrm{R}\Gamma_c(U, V)[1].$$

We set $t_p(V) := D_{dR}(V)/D^0_{dR}(V)$ and also $t_\ell(V) := 0$ for each prime number $\ell \neq p$. Then, for each prime ℓ, Fukaya and Kato define a canonical morphism in $\mathcal{C}_L$ of the form

$$\eta_\ell(V) : \quad \mathbf{1}_L \quad \to \mathbf{d}_L(\mathrm{R}\Gamma_f(\mathbb{Q}_\ell, V))\mathbf{d}_L(t_\ell(V)). \tag{13}$$

For the explicit definition of this morphism we refer the reader either to the original reference [16, §2.4.4] or to the survey article [39, Appendix].

4.2. K-Motives over $\mathbb{Q}$. For further background on this (standard) material we refer the reader to either [16, §2.2, 2.4], [7, §3] or [39, §2].

We fix a finite extension K of $\mathbb{Q}$ and a motive M that is defined over $\mathbb{Q}$ and has coefficients K. As usual we write M_B, M_{dR}, M_ℓ and M_λ for the Betti, de Rham, ℓ-adic and λ-adic realizations of M, where ℓ ranges over rational primes and λ over non-archimedean places of K. We also let t_M denote the tangent space M_{dR}/M^0_{dR} of M. For any ring R and $R[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-module X we denote by X^+ and X^- the R-submodule of X upon which complex conjugation acts as multiplication by $+1$ and -1 respectively.

In our later calculations we will use each of the following isomorphisms:

- The comparison isomorphisms between the Betti and λ-adic realizations of M induce canonical isomorphisms of K_λ-modules, respectively K_ℓ-modules, of the form

$$g^+_\lambda : K_\lambda \otimes_K M^+_B \cong M^+_\lambda, \text{ respectively } g^+_\ell : K_\ell \otimes_K M^+_B \cong M^+_\ell. \tag{14}$$

- We set $K_{\mathbb{R}} := \mathbb{R} \otimes_{\mathbb{Q}} K$. Then the comparison isomorphism between the de Rham and Betti realizations of M induces a canonical $K_{\mathbb{R}}$-equivariant period map

$$\mathbb{R} \otimes_{\mathbb{Q}} M_B^+ \xrightarrow{\alpha_M} \mathbb{R} \otimes_{\mathbb{Q}} t_M. \tag{15}$$

- For each p-adic place λ of K, the comparison isomorphism between the p-adic and de Rham realizations of M induces a canonical isomorphism of K_λ-modules of the form

$$t_p(M_\lambda) = D_{dR}(M_\lambda)/D^0_{dR}(M_\lambda) \xrightarrow[\cong]{g^t_{dR}} K_\lambda \otimes_K t_M. \tag{16}$$

We further recall that the 'motivic cohomology groups' $H^0_f(M) := H^0(M)$ and $H^1_f(M)$ of M are K-modules that can be defined either in terms of algebraic K-theory or motivic cohomology in the sense of Voevodsky (cf. [7]). They are both conjectured to be finite dimensional.

4.3. The Tamagawa Number Conjecture. For each embedding $K \to \mathbb{C}$ the complex L-function that is associated to a K-motive M is defined (for the real part of s large enough) as an Euler product

$$L_K(M,s) = \prod_\ell P_\ell(M, p^{-s})^{-1}$$

over all rational primes ℓ. We assume meromorphic continuation of this function and write $L^*_K(M) \in \mathbb{C}^\times$ and $r(M) \in \mathbb{Z}$ for its leading coefficient and order of vanishing at $s = 0$ respectively.
To establish a link between $L^*_K(M)$ and Galois cohomology one uses the 'fundamental line'

$$\begin{aligned} \Delta_K(M) : \quad = \quad & \mathbf{d}_K(H^0_f(M))^{-1}\mathbf{d}_K(H^1_f(M))\mathbf{d}_K(H^0_f(M^*(1))^*)\mathbf{d}_K(H^1_f(M^*(1))^*)^{-1} \\ & \mathbf{d}_K(M_B^+)\mathbf{d}_K(t_M)^{-1}. \end{aligned}$$

Indeed, as described in [16, §2.2.7], it is conjectured that archimedean regulators and height pairings combine with the period map α_M to induce a canonical morphism in $\mathcal{C}_{K_{\mathbb{R}}}$ (the 'period-regulator isomorphism') of the form

$$\vartheta_\infty(N) : K_{\mathbb{R}} \otimes_K \Delta_K(M) \cong \mathbf{1}_{K_{\mathbb{R}}}. \tag{17}$$

In addition, a standard conjecture on cycle class maps and Chern class maps induces, for each non-archimedean place λ of K, a canonical 'λ-adic period-regulator isomorphism' in C_{K_λ} (which involves the morphism in (13))

$$\vartheta_\lambda(N) : \Delta_K(M)_{K_\lambda} \cong \mathbf{d}_{K_\lambda}(\mathrm{R}\Gamma_c(U, M_\lambda))^{-1}. \tag{18}$$

We now fix a compact p-adic Lie extension F_∞ of $\mathbb{Q}$ which is unramified outside S. We set $G := \mathrm{Gal}(F_\infty/\mathbb{Q})$ and write $\Lambda(G)$ for the associated Iwasawa algebra. For any motive M over $\mathbb{Q}$ we fix a $G_{\mathbb{Q}}$-stable full $\mathbb{Z}_p$-sublattice T_p of M_p and define a (left) Λ-module by setting

$$\mathbb{T} := \Lambda(G) \otimes_{\mathbb{Z}_p} T_p$$

on which $\Lambda(G)$ acts via left multiplication (on the left hand factor) and each element g of $G_{\mathbb{Q}}$ acts diagonally via $g(x\otimes_{\mathbb{Z}_p}y) = x\bar{g}^{-1}\otimes_{\mathbb{Z}_p}g(y)$, where $\bar{g}$ denotes the image of g in $G\subset\Lambda(G)$.
For any non-archimedean place λ of K we write $\mathcal{O}_\lambda$ for the valuation ring of K_λ. We consider a continuous representation $\rho : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ of G which, with respect to a suitable choice of basis, is the λ-adic realization N_λ of a K-motive N. We continue to denote by ρ the induced ring homomorphism $\Lambda(G) \to \mathrm{M}_n(\mathcal{O}_\lambda)$ and we consider $\mathcal{O}_\lambda^n$ as a right $\Lambda(G)$-module via action by the transpose ρ^t on the left, viewing $\mathcal{O}_\lambda^n$ as set of column vectors (contained in K_λ^n). Note that, setting $M(\rho^*) := N^*\otimes M$, we obtain an isomorphism of Galois representations

$$\mathcal{O}_\lambda^n\otimes_{\Lambda(G)}\mathbb{T}\cong T_\lambda(M(\rho^*)),$$

where $T_\lambda(M(\rho^*))$ is the $\mathcal{O}_\lambda$-lattice $\mathcal{O}_\lambda^n\otimes T_p$ of $M(\rho^*)_\lambda$, on which $g\in G_{\mathbb{Q}}$ acts diagonally: $g(x\otimes t) = \rho^*(g)x\otimes g\cdot t$ denoting by ρ^* the contragredient representation of ρ.

Conjecture 4.1 (Fukaya and Kato, [16, Conj. 2.3.2]). *Set $\Lambda := \Lambda(G)$. Then there exists a canonical morphism in $\mathcal{C}_\Lambda$*

$$\zeta_\Lambda(M) := \zeta_\Lambda(\mathbb{T}) : \mathbf{1}_\Lambda \to \mathbf{d}_\Lambda(\mathrm{R}\Gamma_c(U,\mathbb{T}))^{-1}$$

with the following property: for all K,λ and ρ as above the (generalized) base change $K_\lambda^n\otimes_\Lambda -$ sends $\zeta_\Lambda(M)$ to the composite morphism

$$\mathbf{1}_{K_\lambda}\xrightarrow{\zeta_K(M(\rho^*))_{K_\lambda}}\Delta_K(M(\rho^*))_{K_\lambda}\xrightarrow{\vartheta_\lambda(N)}\mathbf{d}_{K_\lambda}(\mathrm{R}\Gamma_c(U,M(\rho^*)_\lambda))^{-1},$$

where

$$\zeta_K(M(\rho^*)) : \mathbf{1}_K \to \Delta_K(M(\rho^*))$$

denotes the unique morphism which is such that, for every embedding $K\to\mathbb{C}$, the leading coefficient $L_K^*(M(\rho^*))$ is equal to the composite

$$\mathbf{1}_{\mathbb{C}}\xrightarrow{\zeta_K(M(\rho^*))_{\mathbb{C}}}\Delta_K(M(\rho^*))_{\mathbb{C}}\xrightarrow{(\vartheta_\infty(N))_{\mathbb{C}}}\mathbf{1}_{\mathbb{C}}.$$

Fukaya and Kato refer to the (conjectural) morphism '$\zeta_\Lambda(M)$' in Conjecture 4.1 as a *global Zeta isomorphism.* We note also that it is straightforward to show that Conjecture 4.1 implies the 'p-primary component' of the Equivariant Tamagawa Number Conjecture that is formulated by Flach and the first named author in [7, Conj. 4(iv)] and hence also implies the 'main conjecture of non-abelian Iwasawa theory' that is discussed by Huber and Kings in [19]. For a further discussion of Conjecture 4.1 see [39, §4].

5. The interpolation formula for Tate motives

In this section we give a first explicit application of the formalism developed in §3. More precisely, we show that the 'p-adic Stark conjecture at $s = 1$', as formulated by Serre in [35] and discussed by Tate in [37, Chap. VI, §5], can be naturally interpreted as an interpolation formula for the leading term (in the sense of Definition 3.14) of certain global Zeta isomorphisms that are predicted to exist by Conjecture 4.1 in terms of the leading terms (in the classical sense) of suitable p-adic Artin L-functions. Interested readers can find further explicit results concerning Conjecture 4.1 in the special case that we consider here in, for example, both [3] and [8].

Throughout this section we set $\mathrm{G}(F/E) := \mathrm{Gal}(F/E)$ for any Galois extension of fields F/E. We also fix an odd prime p and a totally real Galois extension F_∞ of $\mathbb{Q}$ which contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{\mathrm{cyc}}$ of $\mathbb{Q}$ and is such that $G := \mathrm{G}(F_\infty/\mathbb{Q})$ is a compact p-adic Lie group. We assume further that $F_\infty/\mathbb{Q}$ is unramified outside a finite set of prime numbers S (which therefore contains p). We set $H := \mathrm{G}(F_\infty/\mathbb{Q}_{\mathrm{cyc}})$ and $\Gamma := \mathrm{G}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}) \cong G/H$. We fix a subfield E of F_∞ which is both Galois and of finite degree over $\mathbb{Q}$, we set $\bar{G} := \mathrm{G}(E/\mathbb{Q})$ and we write $S_p(E)$ for the set of p-adic places of E and E_{cyc}, $E_{w,\mathrm{cyc}}$ for each $w \in S_p(E)$ and $\mathbb{Q}_{p,\mathrm{cyc}}$ for the cyclotomic $\mathbb{Z}_p$-extensions of E, E_w and $\mathbb{Q}_p$ respectively. For simplicity, we always assume that the following condition is satisfied

$$E \cap \mathbb{Q}_{\mathrm{cyc}} = \mathbb{Q} \text{ and } E_w \cap \mathbb{Q}_{p,\mathrm{cyc}} = \mathbb{Q}_p \text{ for all } w \in S_p(E). \tag{19}$$

We note that this condition implies that there is a direct product decomposition $\mathrm{G}(E_{\mathrm{cyc}}/\mathbb{Q}) \cong \Gamma \times \bar{G}$ and hence allows us to regard γ as a topological generator of each of the groups Γ, $\mathrm{G}(E_{\mathrm{cyc}}/E)$, $\mathrm{G}(E_{w,\mathrm{cyc}}/E_w)$ for $w \in S_p(E)$ and $\mathrm{G}(\mathbb{Q}_{p,\mathrm{cyc}}/\mathbb{Q}_p)$.

We let $\mathbb{T}$ denote the (left) $\Lambda(G)$-module $\Lambda(G)$ endowed with the following (left) action of $G_{\mathbb{Q}}$: each $\sigma \in G_{\mathbb{Q}}$ acts on $\mathbb{T}$ as right multiplication by the element $\chi_{\mathrm{cyc}}(\bar{\sigma})\bar{\sigma}^{-1}$ where $\bar{\sigma}$ denotes the image of σ in G and χ_{cyc} is the cyclotomic character $G \to \Gamma \to \mathbb{Z}_p^\times$. For each subfield F of F_∞ which is Galois over $\mathbb{Q}$ we let $\mathbb{T}_F$ denote the (left) $\Lambda(\mathrm{G}(F/\mathbb{Q}))$-module $\Lambda(\mathrm{G}(F/\mathbb{Q})) \otimes_{\Lambda(G)} \mathbb{T}$. We also set $U := \mathrm{Spec}(\mathbb{Z}[\frac{1}{S}])$ and note that for each such field F there is a natural isomorphism in $D^p(\Lambda(\mathrm{G}(F/\mathbb{Q})))$ of the form

$$\Lambda(\mathrm{G}(F/\mathbb{Q})) \otimes^{\mathbb{L}}_{\Lambda(G)} \mathrm{R}\Gamma_c(U, \mathbb{T}) \cong \mathrm{R}\Gamma_c(U, \mathbb{T}_F). \tag{20}$$

We regard each character of $\bar{G}$ as a character of G via the natural projection $G \twoheadrightarrow \bar{G}$. For any field C we write $R_C^+(\overline{G})$ and $R_C(\overline{G})$ for the set of finite dimensional C-valued characters of $\overline{G}$ and for the ring of finite dimensional C-valued virtual characters of $\overline{G}$, respectively. For each $\rho \in R_C^+(\overline{G})$ we fix a representation space V_ρ of character ρ and for any $\mathbb{Q}_p[\overline{G}]$-module N, respectively endomorphism α of a $\mathbb{Q}_p[\bar{G}]$-module N, we write N^ρ for the $\mathbb{C}_p$-module

$$\mathrm{Hom}_{\bar{G}}(V_\rho, \mathbb{C}_p \otimes_{\mathbb{Q}_p} N) \cong ((V_{\rho^*})_{\mathbb{C}_p} \otimes_{\mathbb{Q}_p} N)_{\bar{G}},$$

respectively α^ρ for the induced endomorphism of N^ρ. We use similar notation for complex characters ρ and $\mathbb{Q}[\bar{G}]$-modules N.

For any abelian group A we write $A\hat{\otimes}\mathbb{Z}_p$ for its p-adic completion $\varprojlim_n A/p^nA$.

5.1. LEOPOLDT'S CONJECTURE. We recall that Leopoldt's Conjecture (for the field E at the prime p) is equivalent to the injectivity of the natural localisation map

$$\lambda_p : \mathcal{O}_E\left[\frac{1}{p}\right]^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \prod_{w\in S_p(E)} E_w^\times \hat{\otimes}\mathbb{Z}_p.$$

If $\rho \in R^+_{\mathbb{C}_p}(\bar{G})$, then in the sequel we say that Leopoldt's Conjecture 'is valid at ρ' if one has $(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \ker(\lambda_p))^\rho = 0$.

We set $c_\gamma := c_{\chi_{\rm cyc},\gamma} \in \mathbb{Q}_p^\times$ (see §3.4.3) and for each $\rho \in R^+_{\mathbb{C}_p}(\bar{G})$ we define

$$\langle\rho, 1\rangle := \dim_{\mathbb{C}_p}(H^0(\bar{G}, V_\rho)) = \dim_{\mathbb{C}_p}((\mathbb{Q}_p)^\rho).$$

Lemma 5.1. *We fix $\rho \in R^+_{\mathbb{C}_p}(\bar{G})$ and assume that Leopoldt's Conjecture is valid at ρ.*

(i) *There are canonical isomorphisms*

$$(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i_c(U, \mathbb{T}_E))^\rho \cong \begin{cases} (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \operatorname{cok}(\lambda_p))^\rho, & \text{if } i = 2\\ (\mathbb{Q}_p)^\rho, & \text{if } i = 3\\ 0, & \text{otherwise.}\end{cases}$$

(ii) $\mathrm{R\Gamma}_c(U, \mathbb{T})$ *is semisimple at ρ and one has $r_G(\mathrm{R\Gamma}_c(U, \mathbb{T}))(\rho) = \langle\rho, 1\rangle$.*

(iii) *For each $w \in S_p(E)$ we write $\mathrm{N}_{E_w/\mathbb{Q}_p}$ for the homomorphism $E_w^\times\hat{\otimes}\mathbb{Z}_p \to \mathbb{Q}_p^\times\hat{\otimes}\mathbb{Z}_p$ that is induced by the field theoretic norm map. Then, with respect to the identifications given in claim (i), the Bockstein homomorphism in degree -2 of $(\mathrm{R\Gamma}_c(U, \mathbb{T}), T_\rho, \gamma)$ is equal to $-c_\gamma^{-1}$ times the homomorphism*

$$(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2_c(U, \mathbb{T}_E))^\rho \to (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^3_c(U, \mathbb{T}_E))^\rho$$

that is induced by the homomorphism

$$\log_{p,E} : \prod_{w\in S_p(E)} E_w^\times\hat{\otimes}\mathbb{Z}_p \to \mathbb{Z}_p$$

which sends each element $(e_w)_w$ to $\sum_w \log_p(\mathrm{N}_{E_w/\mathbb{Q}_p}(e_w))$.

Proof. Claim (i) can be verified by combining the exact cohomology sequence of the tautological exact triangle

$$\mathrm{R\Gamma}_c(U, \mathbb{T}_E) \to \mathrm{R\Gamma}(U, \mathbb{T}_E) \to \bigoplus_{\ell\in S}\mathrm{R\Gamma}(\mathbb{Q}_\ell, \mathbb{T}_E) \to \mathrm{R\Gamma}_c(U, \mathbb{T}_E)[1] \tag{21}$$

together with the canonical identifications $H^i(U, \mathbb{T}_E) \cong H^i(\mathcal{O}_E[\frac{1}{S}], \mathbb{Z}_p(1))$ and $H^i(\mathbb{Q}_\ell, \mathbb{T}_E) \cong \bigoplus_{w\in S_\ell(E)} H^i(E_w, \mathbb{Z}_p(1))$ and an explicit computation of each of the groups $H^i(\mathcal{O}_E[\frac{1}{S}], \mathbb{Z}_p(1))$ and $H^i(E_w, \mathbb{Z}_p(1))$. As this is routine we leave explicit details to the reader except to note that $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}H^2_c(U, \mathbb{T}_E)$ is canonically isomorphic to $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \operatorname{cok}(\lambda_p)$ (independently of Leopoldt's Conjecture), whilst the fact that E is totally real implies that the vanishing of $(\mathbb{Q}_p\otimes_{\mathbb{Z}_p} H^1_c(U, \mathbb{T}_E))^\rho$ is equivalent to that of $(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \ker(\lambda_p))^\rho$.

To prove claims (ii) and (iii) we note first that, in terms of the notation used in §3.3, the isomorphism (20) (with $F = E_{\rm cyc}$) induces a canonical isomorphism in $D^p(\Lambda_{\mathcal{O}}(\Gamma))$ of the form

$$\mathrm{R}\Gamma_c(U, \mathbb{T})_\rho \cong \mathcal{O}^n \otimes_{\mathbb{Z}_p[\bar{G}]} \mathrm{R}\Gamma_c(U, \mathbb{T}_{E_{\rm cyc}}), \tag{22}$$

where Γ acts naturally on the right hand factor in the tensor product.

From Lemma 3.13(iv) we may therefore deduce that $\mathrm{R}\Gamma_c(U,\mathbb{T})$ is semisimple at ρ if and only if the complex $\mathcal{O}^n \otimes_{\mathbb{Z}_p[\bar{G}]} \mathrm{R}\Gamma_c(U, \mathbb{T}_{E_{\rm cyc}}) \in D^p(\Lambda_{\mathcal{O}}(\Gamma))$ is semisimple. But the latter condition is easy to check by using the criterion of Remark 3.3(ii): indeed, one need only note that $H^i_c(U, \mathbb{T}_{E_{\rm cyc}})$ is finite if $i \notin \{2,3\}$, that $H^3_c(U, \mathbb{T}_{E_{\rm cyc}})$ identifies with $\mathbb{Z}_p$ (as a Γ-module) and that the exact sequences of (5) combine with the descriptions of claim (i) to imply that $((\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_c(U, \mathbb{T}_{E_{\rm cyc}}))^\rho)^\Gamma$ and $(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_c(U, \mathbb{T}_{E_{\rm cyc}}))^\rho_\Gamma$ both vanish. In addition, the same observations combine with Lemma 3.13(ii) to imply that $r_G(\mathrm{R}\Gamma_c(U,\mathbb{T}))(\rho) = \dim_{\mathbb{C}_p}((\mathbb{Q}_p)^\rho)$.

Regarding claim (iii), the isomorphism (22) combines with Lemma 3.13(iii) to imply that $(\mathfrak{B}_{-2})^\rho = (\hat{\mathfrak{B}}_{-2})^\rho$ where $\hat{\mathfrak{B}}_{-2}$ is the Bockstein homomorphism in degree -2 of $(\mathrm{R}\Gamma_c(U, \mathbb{T}_{E_{\rm cyc}}), \mathbb{Z}_p, \gamma)$, with γ regarded as a topological generator of $\mathrm{G}(E_{\rm cyc}/E)$. Also, by comparing (21) to the corresponding exact triangle with $E_{\rm cyc}$ in place of E, we obtain a morphism of exact triangles of the form

$$\begin{tikzcd}
\mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{T}_{E_{\rm cyc}}) \arrow[r, "\gamma-1"] \arrow[d] & \mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{T}_{E_{\rm cyc}}) \arrow[r] \arrow[d] & \mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{T}_E) \arrow[r] \arrow[d] & {} \\
\mathrm{R}\Gamma_c(U, \mathbb{T}_{E_{\rm cyc}})[1] \arrow[r, "\gamma-1"] & \mathrm{R}\Gamma_c(U, \mathbb{T}_{E_{\rm cyc}})[1] \arrow[r] & \mathrm{R}\Gamma_c(U, \mathbb{T}_E)[1] \arrow[r] & {} .
\end{tikzcd}$$

Thus, by combining the description of Lemma 3.1 with consideration of the long exact cohomology sequences of this diagram we obtain a commutative diagram

$$\begin{tikzcd}
\bigoplus_{w\in S_p(E)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(E_w, \mathbb{Z}_p(1)) \arrow[r] \arrow[d, "(\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathfrak{B}_{-1,w})_w"'] & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2_c(U, \mathbb{T}_E) \arrow[d, "(-1)\times(\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\hat{\mathfrak{B}}_{-2})"] \\
\bigoplus_{w\in S_p(E)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(E_w, \mathbb{Z}_p(1)) \arrow[r] & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^3_c(U, \mathbb{T}_E).
\end{tikzcd}$$

Here the upper row is the (tautological) surjection that is induced by the canonical identifications $H^1(E_w, \mathbb{Z}_p(1)) \cong E_w^\times \hat{\otimes} \mathbb{Z}_p$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2_c(U, \mathbb{T}_E) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{cok}(\lambda_p)$, the lower row is the surjection induced by the canonical identifications $H^2(E_w, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ and $H^3_c(U, \mathbb{T}_E) \cong \mathbb{Z}_p$ together with the identity map on $\mathbb{Z}_p$, $\mathfrak{B}_{-1,w}$ is the Bockstein homomorphism in degree -1 of $(\mathrm{R}\Gamma(E_{w,\rm cyc}, \mathbb{Z}_p(1)), \mathbb{Z}_p, \gamma)$ where γ is considered as a topological generator of $\mathrm{G}(E_{w,\rm cyc}/E_w)$, and the factor -1 occurs on the right hand vertical arrow because of the 1-shift in the lower row of the previous diagram.

Further, for each $w \in S_p(E)$ the natural isomorphism (in $D^p(\mathbb{Z}_p)$)

$$\mathbb{Z}_p \otimes^{\mathbb{L}}_{\mathbb{Z}_p[\mathrm{G}(E_w/\mathbb{Q}_p)]} \mathrm{R}\Gamma(E_w, \mathbb{Z}_p(1)) \cong \mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{Z}_p(1))$$

induces a commutative diagram

$$\begin{tikzcd}
H^1(E_w, \mathbb{Z}_p(1)) \arrow[r] \arrow[d, "\mathfrak{B}_{-1,w}"'] & H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)) \arrow[d, "\mathfrak{B}_{-1,p}"] \\
H^2(E_w, \mathbb{Z}_p(1)) \arrow[r] & H^2(\mathbb{Q}_p, \mathbb{Z}_p(1))
\end{tikzcd}$$

where the upper horizontal arrow is induced by the canonical identifications $H^1(E_w, \mathbb{Z}_p(1)) \cong E_w^\times \hat{\otimes} \mathbb{Z}_p$ and $H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{Q}_p^\times \hat{\otimes} \mathbb{Z}_p$ together with the map $\mathrm{N}_{E_w/\mathbb{Q}_p}$, the lower horizontal arrow is induced by the canonical identifications $H^2(E_w, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ and $H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ together with the identity map on $\mathbb{Z}_p$, and $\mathfrak{B}_{-1,p}$ is the Bockstein homomorphism in degree -1 of $(\mathrm{R}\Gamma(\mathbb{Q}_{p,\mathrm{cyc}}, \mathbb{Z}_p(1)), \mathbb{Z}_p, \gamma)$. To prove claim (iii) it thus suffices to recall that, with respect to the natural identifications $H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{Q}_p^\times \hat{\otimes} \mathbb{Z}_p$ and $H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$, the map $\mathfrak{B}_{-1,p}$ is equal to $c_\gamma^{-1} \cdot \log_p$ (see, for example, [9, p. 352]). □

5.2. The p-adic Stark conjecture at $s = 1$. For each character $\chi \in R_{\mathbb{C}}(\bar{G})$ we write $L_S(s, \chi)$ for the Artin L-function of χ that is truncated by removing the Euler factors attached to primes in S (cf. [37, Chap. 0, §4]). Then, for each character $\rho \in R_{\mathbb{C}_p}(G)$ there exists a unique p-adic meromorphic function $L_{p,S}(\cdot, \rho) : \mathbb{Z}_p \to \mathbb{C}_p$ such that for each strictly negative integer n and each isomorphism $\iota : \mathbb{C}_p \cong \mathbb{C}$ one has

$$L_{p,S}(n, \rho)^\iota = L_S(n, (\rho \cdot \omega^{n-1})^\iota)$$

where $\omega : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ is the Teichmüller character (cf. [37, Chap. V., Thm. 2.2]). Indeed, this function is the 'S-truncated p-adic Artin L-function' of ρ that is constructed by Greenberg in [17] by combining techniques of Brauer induction with the fundamental results of Deligne and Ribet [15] and Cassou-Noguès [10]. For typographical simplicity in the sequel, we fix an isomorphism $\iota : \mathbb{C}_p \cong \mathbb{C}$ as above and hence often omit it from the notation.

In this section we recall a conjecture of Serre regarding the 'leading term at $s = 1$' of $L_{p,S}(s, \rho)$. To this end we set $E_\infty := \mathbb{R} \otimes_{\mathbb{Q}} E \cong \prod_{\mathrm{Hom}(E,\mathbb{C})} \mathbb{R}$ and write $\log_\infty(\mathcal{O}_E^\times)$ for the inverse image of $\mathcal{O}_E^\times \hookrightarrow E_\infty^\times$ under the (componentwise) exponential map $\exp_\infty : E_\infty \to E_\infty^\times$. We set $E_0 := \{x \in E : \mathrm{Tr}_{E/\mathbb{Q}}(x) = 0\}$. Then $\log_\infty(\mathcal{O}_E^\times)$ is a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} E_0$ and so there is a canonical isomorphism of $\mathbb{C}[\bar{G}]$-modules

$$\mu_\infty : \mathbb{C} \otimes_{\mathbb{Z}} \log_\infty(\mathcal{O}_E^\times) \cong \mathbb{C} \otimes_{\mathbb{Q}} E_0.$$

By a standard argument (cf. [14, §6, Exer. 6]) this implies that the $\mathbb{Q}[\bar{G}]$-modules E_0 and $\mathbb{Q} \otimes_{\mathbb{Z}} \log_\infty(\mathcal{O}_E^\times)$ are (non-canonically) isomorphic. We also note that the composite homomorphism

$$\text{(23)}\quad \log_\infty(\mathcal{O}_E^\times) \xrightarrow{\exp_\infty} \mathcal{O}_E^\times \xrightarrow{\lambda_p} \prod_{w\in S_p(E)} U^1_{E_w} \xrightarrow{(u_w)_w\mapsto(\log_p(u_w))_w} \prod_{w\in S_p(E)} E_w \cong \mathbb{Q}_p\otimes_{\mathbb{Q}} E,$$

factors through the inclusion $\mathbb{Q}_p\otimes_{\mathbb{Q}} E_0 \subset \mathbb{Q}_p\otimes_{\mathbb{Q}} E$ and hence induces an isomorphism of $\mathbb{Q}_p[\bar{G}]$-modules

$$\mu_p : \mathbb{Q}_p\otimes_{\mathbb{Z}} \log_\infty(\mathcal{O}_E^\times) \cong \mathbb{Q}_p\otimes_{\mathbb{Q}} E_0.$$

Conjecture 5.2 (Serre). *For each $\rho\in R^+_{\mathbb{C}_p}(\bar{G})$ we set*

$$L^*_{p,S}(1,\rho) := \lim_{s\to 1}(s-1)^{\langle\rho,1\rangle}\cdot L_{p,S}(s,\rho).$$

Then $L^*_{p,S}(1,\rho)$ is equal to the leading term of $L_{p,S}(s,\rho)$ at $s=1$, and for each choice of isomorphism of $\mathbb{Q}[\bar{G}]$-modules $g: E_0\to\mathbb{Q}\otimes_{\mathbb{Z}}\log_\infty(\mathcal{O}_E^\times)$ one has

$$\frac{L^*_{p,S}(1,\rho)}{\det_{\mathbb{C}_p}((\mathbb{C}_p\otimes_{\mathbb{Q}_p}\mu_p)\circ(\mathbb{C}_p\otimes_{\mathbb{Q}} g))^\rho} = \frac{L^*_S(1,\rho)}{\det_{\mathbb{C}}(\mu_\infty\circ(\mathbb{C}\otimes_{\mathbb{Q}} g))^\rho}.$$

Remark 5.3. This conjecture is the 'p-adic Stark conjecture at $s=1$' as discussed by Tate in [37, Chap. VI, §5], where it is attributed to Serre [35]. More precisely, there are some slight imprecisions in the discussion of [37, Chap. VI, §5] (for example, and as already noted by Solomon in [36, §3.3], the intended meaning of the symbols '$\log U$' and 'μ_p' in [37, p. 137] is unclear) and Conjecture 5.2 represents a natural clarification of the presentation given in loc. cit..

Remark 5.4. We fix a subgroup J of $\bar{G}$ and write 1_J for the trivial character of J. If $\rho = \mathrm{Ind}_J^{\bar{G}} 1_J$, then the inductive behaviour of L-functions combines with the analytic class number formula for E^J to show that Conjecture 5.2 is valid for ρ if and only if the p-adic zeta function of the field E^J has a simple pole at $s=1$ with residue equal to $2^{[E^J:\mathbb{Q}]-1}hR_pe_p/\sqrt{|d|}$ where h, R_p and d are the class number, p-adic regulator and absolute discriminant of E^J respectively and $e_p := \prod_{v\in S_p(E^J)}(1-\mathrm{N}v^{-1})$ (cf. [37, Rem., p. 138]). From the main result (§5, Thm.) of Colmez in [13] one may thus deduce that Conjecture 5.2 is valid for $\rho = \mathrm{Ind}_J^{\bar{G}} 1_J$ if and only if Leopoldt's Conjecture is valid for E^J. We note also that if Leopoldt's Conjecture is valid for E, then it is valid for all such intermediate fields E^J.

5.3. The interpolation formula. We now reinterpret the equality of Conjecture 5.2 as an interpolation formula for the Zeta isomorphism $\zeta_{\Lambda(G)}(\mathbb{T})$ that is predicted to exist by Conjecture 4.1.

Theorem 5.5. *If Conjecture 5.2 is valid, then for each $\rho\in R^+_{\mathbb{C}_p}(\bar{G})$ the complex $\mathrm{R}\Gamma_c(U,\mathbb{T})$ is semisimple at ρ and one has both $r_G(\mathrm{R}\Gamma_c(U,\mathbb{T}))(\rho) = \langle\rho,1\rangle$ and*

$$\text{(24)}\qquad c_\gamma^{\langle\rho,1\rangle}\cdot\zeta_{\Lambda(G)}(\mathbb{T})^*(\rho) = L^*_{p,S}(1,\rho).$$

Remark 5.6. One can naturally interpret (24) as an equality of leading terms of p-adic meromorphic functions. Indeed, whilst Conjecture 5.2 predicts that $L^*_{p,S}(1,\rho)$ is the leading term at $s=1$ of $L_{p,S}(s,\rho)$, Lemma 3.17 interprets the left hand side of (24) as the leading term at $s=0$ of the function $f_{\mathcal{L}}(\rho\chi^s_{\mathrm{cyc}})$ with $\mathcal{L} := [\mathrm{R}\Gamma_c(U,\mathbb{T}), \zeta_{\Lambda(G)}(\mathbb{T})] \in K_1(\Lambda(G), \Sigma_{\mathrm{ss}-\rho})$.

Proof. We note first that if Conjecture 5.2 is valid, then Remark 5.4 implies that Leopoldt's Conjecture is valid for E and so Lemma 5.1(ii) implies that $r_G(\mathrm{R}\Gamma_c(U,\mathbb{T}))(\rho) = \langle \rho, 1\rangle$ for each $\rho \in R^+_{\mathbb{C}_p}(\bar{G})$ and also that $\mathrm{R}\Gamma_c(U,\mathbb{T})$ is semisimple at each such ρ.

We now fix $\rho \in R^+_{\mathbb{C}_p}(\bar{G})$ and a number field K over which the character ρ can be realised. We fix an embedding $K \hookrightarrow \mathbb{C}$ and write λ for the place of K which is induced by the fixed isomorphism $\iota : \mathbb{C}_p \cong \mathbb{C}$. We set $M := h^0(\operatorname{Spec} E)(1)$ and note that $M([\rho]^*) := M \otimes [\rho]^*$ is a K-motive, where $[\rho]^*$ denotes the dual of the Artin motive corresponding to ρ.

To evaluate $\zeta_{\Lambda(G)}(\mathbb{T})^*(\rho)$ we need to make Definition 3.14 explicit. To do this we use the observations of [6, §1.1, §1.3] to explicate the isomorphism $\zeta_K(M([\rho]^*))_{K_\lambda}$ which occurs in Conjecture 4.1. Indeed one has $H^1_f(M) = \mathcal{O}_E^\times \otimes_{\mathbb{Z}} \mathbb{Q}$, $H^0_f(M^*(1)) = \mathbb{Q}$, $t_M = E$ and $H^0_f(M) = H^1_f(M^*(1)) = M^+_B = 0$ (the latter since E is totally real). This implies that

$$\mathbb{C} \otimes_K \Delta_K(M([\rho]^*)) = \mathbf{d}_{\mathbb{C}}((\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_E^\times)_\rho)\mathbf{d}_{\mathbb{C}}((\mathbb{Q})_\rho)\mathbf{d}_{\mathbb{C}}((E)_\rho)^{-1}$$

and that $\zeta_K(M([\rho]^*))_{K_\lambda}$ is equal to the composite morphism

$$\begin{aligned} \text{(25)} \quad \mathbf{1}_{\mathbb{C}_p} \to & \mathbf{1}_{\mathbb{C}_p} \\ \to & \mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_E^\times)^\rho)\mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p)^\rho)\mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Q}} E)^\rho)^{-1} \\ \to & \mathbf{d}_{\mathbb{C}_p}(\mathbb{C}_p \otimes_{K_\lambda} H^2_c(U, M([\rho]^*)_\lambda))^{-1}\mathbf{d}_{\mathbb{C}_p}(\mathbb{C}_p \otimes_{K_\lambda} H^3_c(U, M([\rho]^*)_\lambda) \\ \to & \mathbf{d}_{\mathbb{C}_p}(\mathbb{C}_p \otimes_{K_\lambda} \mathrm{R}\Gamma_c(U, M([\rho]^*)_\lambda))^{-1}. \end{aligned}$$

In this displayed formula we have used the following notation: the first map corresponds to multiplication by $L^*_S(1,\rho)$; the second map is induced by applying $(\mathbb{C}_p \otimes_{\mathbb{R},\iota^{-1}} -)^\rho$ to both the natural isomorphism $\mathbb{R} \otimes_{\mathbb{Q}} E \cong \prod_{\mathrm{Hom}(E,\mathbb{C})} \mathbb{R}$ and also the exact sequence

$$\text{(26)} \qquad 0 \to \mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_E^\times \xrightarrow{(\log \circ \sigma)_\sigma} \prod_{\sigma \in \mathrm{Hom}(E,\mathbb{C})} \mathbb{R} \xrightarrow{(x_\sigma)_\sigma \mapsto \sum_\sigma x_\sigma} \mathbb{R} \to 0;$$

the third map is induced by Lemma 5.1(i) and the inverse of the isomorphism

$$\text{(27)} \qquad \prod_{w \in S_p(E)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{E_w} \xrightarrow{(u_w)_w \mapsto (\log_p(u_w))_w} \prod_{w \in S_p(E)} E_w \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} E;$$

the last map is induced by property h) as described in §2.1 (with $R = \mathbb{C}_p$).

Also, from Lemma 5.1(iii) we know that $\mathbb{C}_p \otimes_{K_\lambda} t(\mathrm{R}\Gamma_c(U, \mathbb{T})(\rho^*))$ is equal to the composite

$$\begin{aligned} \text{(28)} \qquad & \mathbf{d}_{\mathbb{C}_p}(\mathbb{C}_p \otimes_{K_\lambda} \mathrm{R}\Gamma_c(U, M([\rho]^*)_\lambda)^{-1} \\ & \to \mathbf{d}_{\mathbb{C}_p}(H^2_c(U, M([\rho]^*)_\lambda)^{-1}\mathbf{d}_{\mathbb{C}_p}(H^3_c(U, M([\rho]^*)_\lambda) \\ & \to \mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p)^\rho)^{-1}\mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p)^\rho) = \mathbf{1}_{\mathbb{C}_p} \end{aligned}$$

where the first arrow is induced by property h) in §2.1 (with $R = \mathbb{C}_p$) and the second by Lemma 5.1(i) and the homomorphism $-c_\gamma^{-1}\log_{p,E}$ described in Lemma 5.1(iii).

Now, after taking account of Lemma 5.1(ii), the leading term $\zeta_{\Lambda(G)}(\mathbb{T})^*(\rho)$ is defined (in Definition 3.14) to be equal to $(-1)^{\langle\rho,1\rangle}$ times the element of $\mathbb{C}_p^\times$ which corresponds to the composite of (25) and (28). Thus, after noting that there is a commutative diagram of the form

$$\begin{tikzcd} \prod_{w\in S_p(E)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{E_w} \arrow[r] \arrow[d, "(27)"'] & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{cok}(\lambda_p) \arrow[d, "\log_{p,E}"] \\ \mathbb{Q}_p \otimes_{\mathbb{Q}} E \arrow[r, "\mathrm{Tr}_{E/\mathbb{Q}}"] & \mathbb{Q}_p \end{tikzcd}$$

where the upper horizontal arrow is the tautological projection, the observations made above imply that

$$\text{(29)} \qquad c_\gamma^{\langle\rho,1\rangle} \cdot \zeta_{\Lambda(G)}(\mathbb{T})^*(\rho) = L_S^*(1,\rho)\cdot\xi$$

where ξ is the element of $\mathbb{C}_p^\times$ that corresponds to the composite morphism

$$\begin{aligned} \text{(30)} \qquad \mathbf{1}_{\mathbb{C}_p} &= \mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_E^\times)^\rho)\mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_E^\times)^\rho)^{-1} \\ & \to \mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Q}} E_0)^\rho)\mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_E^\times)^\rho)^{-1} \\ & \to \mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Q}} E_0)^\rho)\mathbf{d}_{\mathbb{C}_p}((\mathbb{Q}_p \otimes_{\mathbb{Q}} E_0)^\rho)^{-1} = \mathbf{1}_{\mathbb{C}_p}. \end{aligned}$$

Here the first arrow is induced by applying $\mathbb{C}_p \otimes_{\mathbb{R},\iota^{-1}} -$ to the isomorphism $\mathbb{R}\otimes_{\mathbb{Z}}\mathcal{O}_E^\times \cong \mathbb{R}\otimes_{\mathbb{Q}}E_0$ coming from the map $(\log\circ\sigma)_\sigma$ in (26) and the second by the isomorphism $\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_E^\times \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} E_0$ coming from the second and third arrows in (23). (Note also that the factor $(-1)^{\langle\rho,1\rangle}$ in the definition of $\zeta_{\Lambda(G)}(\mathbb{T})^*(\rho)$ cancels against the factor -1 in the term $-c_\gamma^{-1}$ which occurs in the morphism (28) and hence does not occur in the formula (29)).

But, upon comparing the definitions of μ_∞ and μ_p in §5.2 with the maps involved in (30), one finds that ξ is equal to

$$\det_{\mathbb{C}_p}((\mathbb{C}_p \otimes_{\mathbb{Q}_p} \mu_p)\circ(\mathbb{C}_p \otimes_{\mathbb{C},\iota^{-1}} \mu_\infty)^{-1})^\rho = \frac{\det_{\mathbb{C}_p}((\mathbb{C}_p \otimes_{\mathbb{Q}_p} \mu_p)\circ(\mathbb{C}_p \otimes_{\mathbb{Q}} g))^\rho}{\det_{\mathbb{C}}(\mu_\infty \circ (\mathbb{C}\otimes_{\mathbb{Q}} g))^\rho}$$

and hence (29) implies that

$$\frac{c_\gamma^{\langle\rho,1\rangle}\cdot\zeta_{\Lambda(G)}(\mathbb{T})^*(\rho)}{\det_{\mathbb{C}_p}((\mathbb{C}_p \otimes_{\mathbb{Q}_p} \mu_p)\circ(\mathbb{C}_p \otimes_{\mathbb{Q}} g))^\rho} = \frac{L_S^*(1,\rho)}{\det_{\mathbb{C}}(\mu_\infty \circ (\mathbb{C}\otimes_{\mathbb{Q}} g))^\rho}.$$

The claimed equality (24) now follows immediately upon comparing this equality to that of Conjecture 5.2. □

Corollary 5.7. *If Leopoldt's Conjecture is valid for E at p, then for every finite dimensional $\mathbb{Q}$-rational character ρ of $\bar{G}$ there exists a natural number n_ρ such that*

$$(c_\gamma^{\langle\rho,1\rangle}\cdot\zeta_{\Lambda(G)}(\mathbb{T})^*(\rho))^{n_\rho}=L^*_{p,S}(1,\rho)^{n_\rho}.$$

Further, if ρ is a permutation character, then one can take $n_\rho=1$.

Proof. If ρ is $\mathbb{Q}$-rational, then Artin's Induction Theorem implies the existence of a natural number n_ρ such that in $R_{\mathbb{C}_p}(G)$ one has $n_\rho\cdot\rho=\sum_H n_H\cdot\mathrm{Ind}_H^G 1_H$ where H runs over the set of subgroups of $\bar{G}$ and each n_H is an integer (cf. [37, Chap. II, Thm. 1.2]). Further, ρ is said to be a permutation character if and only if there exists such a formula with $n_\rho=1$. The stated result thus follows by combining Theorem 5.5 with Remark 5.4 and the fact that each side of (24) is both additive and inductive in ρ. □

6. The interpolation formula for critical motives

As a second application of the formalism introduced in §3, in this section we prove an interpolation formula for the leading terms (in the sense of Definition 3.14) of the p-adic L-functions that Fukaya and Kato conjecture to exist for any critical motive which has good ordinary reduction at all places above p. (We recall that a motive M is said to be 'critical' if the map (15) is bijective). To study these p-adic L-functions we must combine Conjecture 4.1 together with a local analogue of this conjecture (which is also due to Fukaya and Kato, and is recalled as Conjecture 6.1 below) and aspects of Nekovář's theory of Selmer complexes and of the theory of p-adic height pairings.

6.1. Local epsilon isomorphisms. At the outset we fix a 'p-adic period' t (that is, a topological generator of $\mathbb{Z}_p(1)$). Let L be any finite extension of $\mathbb{Q}_p$ and V any finite-dimensional L-vector space with continuous $G_{\mathbb{Q}_p}$-action. Then we write $\epsilon_p(V):=\epsilon(D_{pst}(V))$ for Deligne's epsilon-factor at p, where $D_{pst}(V)$ is endowed with the linearized action of the Weil group and thereby considered as a representation of the Weil-Deligne group, see [16, §3.2] or [29, App. C]. (Note that this notation hides dependence on the choice of a Haar measure and p-adic period. Note also that the choice of $t=(t_n)\in\mathbb{Z}_p(1)$ determines a homomorphism $\psi_p:\mathbb{Q}_p\to\overline{\mathbb{Q}_p}^\times$ with $\ker(\psi_p)=\mathbb{Z}_p$ by sending $\frac{1}{p^n}$ to $t_n\in\mu_{p^n}$). The subfield of inertial invariants $(B_{dR})^{I_p}$ of B_{dR} identifies with the completion $\widehat{\mathbb{Q}_p^{nr}}$ of the maximal unramified extension $\mathbb{Q}_p^{nr}$ of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}_p}$. For L and V as above we set $\widetilde{L}:=\widehat{\mathbb{Q}_p^{nr}}\otimes_{\mathbb{Q}_p}L$ and

$$\Gamma^*(-j):=\begin{cases}\Gamma(j)=(j-1)!, & \text{if } j>0,\\ \lim_{s\to j}(s-j)\Gamma(s)=(-1)^j((-j)!)^{-1}, & \text{if } j\le 0,\end{cases}$$

and

$$\Gamma_L(V) := \prod_{j\in\mathbb{Z}} \Gamma^*(j)^{-h(-j)},$$

where $h(j) := \dim_L gr^j D_{dR}(V)$.
We let

$$\epsilon_{p,L}(V) : \mathbf{1}_{\widetilde{L}} \to \big(\mathbf{d}_L(\mathrm{R}\Gamma(\mathbb{Q}_p, V))\mathbf{d}_L(V)\big)_{\widetilde{L}}$$

denote the morphism that is obtained by taking the product of $\Gamma_L(V)$ with the morphisms $\eta_\ell(V)$ and $\overline{(\eta_\ell(V^*(1))^*)}$ from (13) and the morphism

$$\epsilon_{dR}(V) : \mathbf{1}_{\widetilde{L}} \to \mathbf{d}_{\widetilde{L}}(V)\mathbf{d}_{\widetilde{L}}(D_{dR}(V))^{-1}$$

that is constructed by Fukaya and Kato in [16, Prop. 3.3.5].
We set $\Lambda := \Lambda(G)$ and define

$$\widetilde{\Lambda} := W(\overline{\mathbb{F}_p})[\![G]\!] = \varprojlim_U \big(W(\overline{\mathbb{F}_p}) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G/U]\big),$$

where U runs over all open normal subgroups of G and $W(\overline{\mathbb{F}_p})$ denotes the Witt ring of $\overline{\mathbb{F}_p}$. Now we fix a finite-dimensional $\mathbb{Q}_p$-linear representation V of $G_{\mathbb{Q}_p}$, a full Galois stable $\mathbb{Z}_p$-sublattice T of V, set $\mathbb{T} := \Lambda \otimes_{\mathbb{Z}_p} T$ and we write $\mathcal{O}$ for the valuation ring of L. For any continuous representations $\rho : G \to \mathrm{GL}_n(\mathcal{O})$ we denote by $V(\rho^*)$ the Galois representation $\rho^* \otimes V := \mathcal{O}^n \otimes_{\mathbb{Z}_p} V$, on which $G_{\mathbb{Q}_p}$ acts diagonally, via ρ^* on the first factor.
The following conjecture will play a key role in the sequel (for further discussion of this conjecture see [39, Conj. 5.9]).

Conjecture 6.1 (Fukaya and Kato, [16, Conj. 3.4.3]). *There exists a canonical morphism in $\mathcal{C}_{\widetilde{\Lambda}}$ of the form*

$$\epsilon_{p,\Lambda}(\mathbb{T}) : \mathbf{1}_{\widetilde{\Lambda}} \to \big(\mathbf{d}_\Lambda(\mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{T})) \cdot \mathbf{d}_\Lambda(\mathbb{T})\big)_{\widetilde{\Lambda}}$$

which is such that for all finite degree extensions L of $\mathbb{Q}_p$, with valuation ring $\mathcal{O}$, and all continuous representations $\rho : G \to \mathrm{GL}_n(\mathcal{O}) \subseteq \mathrm{GL}_n(L)$ such that $V(\rho^*)$ is de Rham one has

$$L^n \otimes_\Lambda \epsilon_{p,\Lambda}(\mathbb{T}) = \epsilon_{p,L}(V(\rho^*)).$$

6.2. Selmer complexes. We fix a continuous finite-dimensional L-linear representation W of $G_{\mathbb{Q}}$ which satisfies the following 'condition of Dąbrowski-Panchishkin':

(DP) W is de Rham and there exists a $G_{\mathbb{Q}_p}$-subrepresentation $\hat{W}$ of W (restricted to $G_{\mathbb{Q}_p}$) such that $D^0_{dR}(\hat{W}) = t_p(W) := D_{dR}(W)/D^0_{dR}(W)$.

Thus we have an exact sequence of $G_{\mathbb{Q}_p}$-representations

$$0 \to \hat{W} \to W \to \tilde{W} \to 0$$

such that $D^0_{dR}(\hat{W}) = t_p(\tilde{W}) = 0$ (cf. [23, Prop. 1.28]). Setting $Z := W^*(1)$, $\hat{Z} := \tilde{W}^*(1)$ and $\tilde{Z} := \hat{W}^*(1)$ we obtain by Kummer duality the analogous exact sequence

$$0 \to \hat{Z} \to Z \to \tilde{Z} \to 0$$

and we note that Z also satisfies the condition (DP).
We now fix a finite set S of places of $\mathbb{Q}$ which contains both $S_\infty := \{\infty\}$ and $S_p := \{p\}$ and is such that W (and hence also Z) is a representation of G_S, and we set $U := \operatorname{Spec}(\mathbb{Z}[\frac{1}{S}])$.
Then the *Selmer complex* $SC_U(\hat{W}, W)$ is defined to be the natural mapping fibre
(31)

$$SC_U(\hat{W}, W) \to \mathrm{R}\Gamma(U, W) \to \mathrm{R}\Gamma(\mathbb{Q}_p, W/\hat{W}) \oplus \bigoplus_{\ell \neq p} \mathrm{R}\Gamma(\mathbb{Q}_\ell, W) \to$$

while the *modified Selmer complex* $SC(\hat{W}, W)$ is defined to be the natural mapping fibre
(32)

$$SC(\hat{W}, W) \to \mathrm{R}\Gamma(U, W) \to \mathrm{R}\Gamma(\mathbb{Q}_p, W/\hat{W}) \oplus \bigoplus_{\ell \neq p} \mathrm{R}\Gamma_{/f}(\mathbb{Q}_\ell, W) \to$$

where in both cases ℓ runs over all prime numbers that are distinct from p. Also, for each such ℓ, the complex $\mathrm{R}\Gamma_{/f}(\mathbb{Q}_\ell, W)$ is defined as the natural mapping cone

$$\mathrm{R}\Gamma_f(\mathbb{Q}_\ell, W) \longrightarrow \mathrm{R}\Gamma(\mathbb{Q}_\ell, W) \longrightarrow \mathrm{R}\Gamma_{/f}(\mathbb{Q}_\ell, W) \longrightarrow \tag{33}$$

For any $G_{\mathbb{Q}_p}$-representation V and prime number ℓ we define an element of the polynomial ring $L[u]$ by setting

$$P_\ell(V, u) := P_{L,\ell}(V, u) := \begin{cases} \det_L(1 - \varphi_\ell u | V^{I_\ell}), & \text{if } \ell \neq p, \\ \det_L(1 - \varphi_p u | D_{cris}(V)), & \text{if } \ell = p, \end{cases}$$

where φ_ℓ denotes the geometric Frobenius automorphism of ℓ.
Then the following three conditions are easily seen to be equivalent:

(A$_1$) $P_\ell(W, 1)P_\ell(Z, 1) \neq 0$ for all primes $\ell \neq p$,
(A$_2$) $H^0(\mathbb{Q}_\ell, W) = H^0(\mathbb{Q}_\ell, Z) = 0$ for all primes $\ell \neq p$,
(A$_3$) $\mathrm{R}\Gamma_f(\mathbb{Q}_\ell, W)$ is quasi-null for all primes $\ell \neq p$.

We also consider the following conditions:

(B$_1$) $P_p(W, 1)P_p(Z, 1) \neq 0$,
(B$_2$) $D_{cris}(W)^{\varphi_p - 1} = D_{cris}(Z)^{\varphi_p - 1} = 0$,
(B$_3$) $H^0(\mathbb{Q}_p, W) = H^0(\mathbb{Q}_p, Z) = 0$.

We note that (B_1) is equivalent to (B_2) and that [23, Thm. 1.15] shows that (B_3) implies (B_2).
Finally we consider the following mutually equivalent conditions (to see that (C_2) is equivalent to (C_3) one uses loc. cit. and the fact that $t_p(\tilde{W}) = t_p(\tilde{Z}) = 0$) :

(C$_1$) $P_p(\tilde{W}, 1)P_p(\tilde{Z}, 1) \neq 0$,
(C$_2$) $D_{cris}(\tilde{W})^{\varphi_p - 1} = D_{cris}(\tilde{Z})^{\varphi_p - 1} = 0$,
(C$_3$) $H^0(\mathbb{Q}_p, \tilde{W}) = H^0(\mathbb{Q}_p, \tilde{Z}) = 0$.

Lemma 6.2. *Let X denote either W or Z.*

(i) *If condition (A_1) is satisfied, then for every prime $\ell \neq p$ all of the following complexes are quasi-null*

$$\mathrm{R}\Gamma(\mathbb{Q}_\ell, X) \cong \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, X) \cong \mathrm{R}\Gamma_{/f}(\mathbb{Q}_\ell, X) \cong 0.$$

(ii) *If condition (C_1) is satisfied, then there are isomorphisms in $D^p(L)$ of the form*

$$\mathrm{R}\Gamma_{/f}(\mathbb{Q}_p, X) \cong \mathrm{R}\Gamma(\mathbb{Q}_p, \tilde{X})$$

and

$$\mathrm{R}\Gamma_f(\mathbb{Q}_p, X) \cong \mathrm{R}\Gamma(\mathbb{Q}_p, \hat{X}) \cong \mathrm{R}\Gamma_f(\mathbb{Q}_p, \hat{X}).$$

(iii) *If conditions (A_1) and (C_1) are both satisfied, then there exists an isomorphism in $D^p(L)$ of the form*

$$SC_U(\hat{W}, W) \cong \mathrm{R}\Gamma_f(\mathbb{Q}, W).$$

Proof. We assume (A_1). Then by local duality and the local Euler characteristic formula it follows immediately that $\mathrm{R}\Gamma(\mathbb{Q}_\ell, X)$ is quasi-null. The other statements in claim (i) are then obvious. To prove claim (ii) we assume (C_1). Then, since every bounded complex of finitely generated L-modules is canonically isomorphic in $D^b(L)$ to its cohomology, considered as a complex with zero differentials, we have $\mathrm{R}\Gamma(\mathbb{Q}_p, \hat{X}) \cong \mathrm{R}\Gamma_f(\mathbb{Q}_p, \hat{X}) \cong \mathrm{R}\Gamma_f(\mathbb{Q}_p, X)$ by [16, Lem. 4.1.7]. Thus the exact triangles

$$\mathrm{R}\Gamma(\mathbb{Q}_p, \hat{X}) \to \mathrm{R}\Gamma(\mathbb{Q}_p, X) \to \mathrm{R}\Gamma(\mathbb{Q}_p, \tilde{X}) \to$$

and

$$\mathrm{R}\Gamma_f(\mathbb{Q}_p, X) \to \mathrm{R}\Gamma(\mathbb{Q}_p, X) \to \mathrm{R}\Gamma_{/f}(\mathbb{Q}_p, X) \to$$

are naturally isomorphic in $D^p(L)$. Finally, we note that claim (iii) follows immediately from claims (i) and (ii) and the respective definitions of $SC_U(\hat{W}, W)$ and $\mathrm{R}\Gamma_f(\mathbb{Q}, W)$. □

6.3. p-adic height pairings. To prepare for our derivation of the interpolation formula in §6.4 we now discuss certain preliminaries regarding p-adic height pairings.

We let M be any motive over $\mathbb{Q}$, $V = M_p$ its p-adic realization, ρ an Artin representation defined over the number field K and $[\rho]$ the corresponding Artin motive. We fix a p-adic place λ of K, set $L := K_\lambda$ and write $\mathcal{O}$ for the valuation ring of L. Then the λ-adic realisation

$$W := N_\lambda = V \otimes_{\mathbb{Q}_p} [\rho]^*_\lambda \tag{34}$$

of the motive $N := M(\rho^*) := M \otimes [\rho]^*$ is an L-adic representation. We assume that V (and hence, since $[\rho]^*$ is pure of weight zero, also W) satisfies the condition (DP). We fix a full Galois stable $\mathbb{Z}_p$-sublattice T of V and set $T_\rho := T \otimes_{\mathbb{Z}_p} \mathcal{O}^n$, a Galois stable lattice in W (where we assume that without loss of generality $[\rho]^*_\lambda$ is given as $\rho^* : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathcal{O})$). Similarly we fix a full $G_{\mathbb{Q}_p}$-stable $\mathbb{Z}_p$-sublattice $\hat{T}$ of $\hat{V}$ and we define $\tilde{T}$ to be the lattice in $\tilde{V}$ that is induced from T. Finally we set $\hat{T}_\rho := \hat{T} \otimes_{\mathbb{Z}_p} \mathcal{O}^n$ and $\tilde{T}_\rho := \tilde{T} \otimes_{\mathbb{Z}_p} \mathcal{O}^n$ (which are Galois stable $\mathcal{O}$-sublattices of $\hat{W}$ and $\tilde{W}$ respectively).

Example 6.3. Let A be an abelian variety that is defined over $\mathbb{Q}$ and set $M := h^1(A)(1)$. If A has good ordinary reduction at p, then $W := N_\lambda$ satisfies the conditions (DP), (A_1), (B_1) and (C_1). Indeed, the last three conditions are valid for weight reasons, and more generally, condition (DP) is known to be valid for any motive which has good ordinary reduction at p (see [28]). More precisely, for A (still in the good ordinary case) we have $\hat{W} = \hat{V} \otimes [\rho]^*_\lambda$ where $\hat{V} = V_p(\widehat{A^\vee})$ denotes the p-adic Tate-module of the formal group of the dual abelian variety $A^\vee$ of A. However, if, for example, A is an elliptic curve with (split) multiplicative reduction at p, then M does not satisfy the condition (B_1).

Now we define a $G_{\mathbb{Q}_p}$-stable $\mathbb{Z}_p$-sublattice of $\hat{V}$ by setting

$$\hat{T} := T \cap \hat{V}.$$

As before we let $\mathbb{T}$ denote the Galois representation $\Lambda \otimes_{\mathbb{Z}_p} T$ and set $\hat{\mathbb{T}} := \Lambda \otimes_{\mathbb{Z}_p} \hat{T}$ similarly. Then $\hat{\mathbb{T}}$ is a $G_{\mathbb{Q}_p}$-stable Λ-submodule of $\mathbb{T}$. It is in fact a direct summand of $\mathbb{T}$ and there exists a morphism in $\mathcal{C}_{\tilde{\Lambda}}$ of the form

$$\beta : \mathbf{d}_\Lambda(\mathbb{T}^+)_{\tilde{\Lambda}} \cong \mathbf{d}_\Lambda(\hat{\mathbb{T}})_{\tilde{\Lambda}}. \tag{35}$$

Now the Selmer complexes $SC_U(\hat{\mathbb{T}}, \mathbb{T})$ and $SC(\hat{\mathbb{T}}, \mathbb{T})$ are defined analogously as for W above.

Then $SC_U(\hat{X}, X)$ coincides with the Selmer complex $\widetilde{\mathrm{R}\Gamma_f}(X)$ that occurs in [24, (11.3.1.5)] for $X \in \{W, Z\}$. More generally, we set $\Gamma := \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$ and define

$$\mathbb{T}_{\mathrm{cyc},\rho} := \Lambda(\Gamma) \otimes_{\mathbb{Z}_p} T_\rho$$

and similarly also $\hat{\mathbb{T}}_{\mathrm{cyc},\rho}$ and $\tilde{\mathbb{T}}_{\mathrm{cyc},\rho}$. Then $SC_U(\hat{\mathbb{T}}_{\mathrm{cyc},\rho}, \mathbb{T}_{\mathrm{cyc},\rho})$ identifies with the Selmer complex $\widetilde{\mathrm{R}\Gamma_{f,\mathrm{Iw}}}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, T_\rho)$ that is defined in [24, (8.8.5)] (with Nekovář's local conditions induced by setting $T^+_\ell := \hat{\mathbb{T}}_{\mathrm{cyc}}(\rho)$ if $\ell = p$ and $T^+_\ell := 0$ otherwise, and with Nekovář's set Σ taken to be the set of all rational primes). Thus we obtain a pairing

$$h_p(W) : H^1_f(\mathbb{Q}, W) \times H^1_f(\mathbb{Q}, Z) \to L$$

from [24, §11] where $h_p(W)$ is denoted $\tilde{h}_{\pi,1,1}$. Now, by [24, Thm. 11.3.9], the pairing $h_p(W)$ coincides up to sign with the height pairings constructed by Schneider [32] (in the case of abelian varieties) and Perrin-Riou [26] (for semistable representations) and also those constructed earlier by Nekovář [23]: see also [loc. cit., §8.1] and the papers of Mazur and Tate [22] and Zarhin [41] for alternative definitions of related height pairings.

It follows from the construction of Nekovář's height pairing (cf. [24, the sentence after (11.1.3.2)]) that the induced map

$$\mathrm{ad}(h_p(W)) : H^1_f(\mathbb{Q}, W) \to H^1_f(\mathbb{Q}, Z)^* \tag{36}$$

is equal to the composite

$$(37)\quad H^1_f(\mathbb{Q},W)\cong H^1(SC_U(\hat{W},W))\xrightarrow{\mathfrak{B}} H^2(SC_U(\hat{W},W))\\ \cong H^2_f(\mathbb{Q},W)\cong H^1_f(\mathbb{Q},Z)^*$$

where the first and third maps are by Lemma 6.2(iii), $\mathfrak{B}$ denotes the Bockstein homomorphism for $SC_U(\hat{\mathbb{T}}_{\mathrm{cyc},\rho},\mathbb{T}_{\mathrm{cyc},\rho})$ and the last map comes from global duality.

6.4. The interpolation formula. In this section we assume that the motive $N := M(\rho^*)$ is critical. Then, assuming the conjecture [39, Conj. 3.3] of Fontaine and Perrin-Riou to be valid, the motivic cohomology groups

(D_1) $H^0_f(N) = H^0_f(N^*(1)) = 0$

both vanish. In fact, if we also assume the validity of a well-known conjecture [39, Conj. 3.6] on p-adic regulator maps, this last condition is equivalent to the condition

(D_2) $H^0_f(\mathbb{Q},W) = H^0_f(\mathbb{Q},Z) = 0$

where W is defined in (34) and $Z := W^*(1)$.
We also consider the condition

(F) The pairing $h_p(W)$ is non-degenerate.

Example 6.4. If A is an abelian variety over $\mathbb{Q}$, then the motive $M = h^1(A)(1)$ satisfies the conditions (D_1) and (D_2). However, very little is known about the non-degeneracy of the p-adic height pairing in the ordinary case. Indeed, as far as we are aware, the only theoretical evidence for non-degeneracy is a result of Bertrand [1] that for an elliptic curve with complex multiplication, the height of a point of infinite order is non-zero (but even this is unknown in the non CM case). Computationally, however, there has been a lot of work done recently by Stein and Wuthrich [40]. We are grateful to J. Coates, P. Schneider and C. Wuthrich for providing us with these examples.

We now fix a compact p-adic Lie extension F_∞ of $\mathbb{Q}$ which contains $\mathbb{Q}_{\mathrm{cyc}}$ and is unramified outside S. We let G denote the group $\mathrm{Gal}(F_\infty/\mathbb{Q})$, with quotient $\Gamma := \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$, and we set $\Lambda := \Lambda(G)$.
In [16] Fukaya and Kato use the morphisms $\zeta_\Lambda(M)$ and $\epsilon_{p,\Lambda}(\hat{\mathbb{T}})$ that are predicted to exist by Conjecture 4.1 and Conjecture 6.1 to construct canonical 'p-adic L-function' morphisms in $\mathcal{C}_\Lambda$ of the form

$$(38)\qquad \mathcal{L}_{U,\beta} := \mathcal{L}_{U,\beta}(M) : \mathbf{1}_\Lambda \to \mathbf{d}_\Lambda(SC_U(\hat{\mathbb{T}},\mathbb{T}))$$

and

$$(39)\qquad \mathcal{L}_{\beta} := \mathcal{L}_{\beta}(M) : \mathbf{1}_\Lambda \to \mathbf{d}_\Lambda(SC(\hat{\mathbb{T}},\mathbb{T}))$$

both depending on the isomorphism β in (35). We set $SC_U := SC_U(\hat{\mathbb{T}},\mathbb{T})$ and $SC := SC(\hat{\mathbb{T}},\mathbb{T})$. Then the morphisms $\mathcal{L}_{U,\beta}$ and $\mathcal{L}_\beta$ give rise to elements $[SC_U,\mathcal{L}_{U,\beta}]$ and $[SC,\mathcal{L}_\beta]$ of $K_1(\Lambda(G),\Sigma_{SC_U})$ and $K_1(\Lambda(G),\Sigma_{SC})$ respectively

(where we use the notation Σ_C introduced at the end of §2.2), and for simplicity we continue to denote these elements by $\mathcal{L}_{U,\beta}$ and $\mathcal{L}_\beta$ respectively.
We write Υ for the set of all primes $\ell \neq p$ with the property that the ramification index of ℓ in $F_\infty/\mathbb{Q}$ is infinite. We note that Υ is empty if G has a commutative open subgroup.

Theorem 6.5. *We assume that the motive $M(\rho^*)$ is critical, that the representation W defined in (34) satisfies the conditions (DP), (A_1), (B_1), (C_1), (D_2) and (F) and that the morphisms $\zeta_\Lambda(M)$ and $\epsilon_{p,\Lambda}(\hat{\mathbb{T}})$ that are described in Conjecture 4.1 and Conjecture 6.1 exist.*
Then both $SC_U(\hat{\mathbb{T}},\mathbb{T})$ and $SC(\hat{\mathbb{T}},\mathbb{T})$ are semisimple at ρ, one has $r := r_G(SC_U(\hat{\mathbb{T}},\mathbb{T}))(\rho) = r_G(SC(\hat{\mathbb{T}},\mathbb{T}))(\rho) = \dim_L H^1_f(\mathbb{Q},W)$ and the leading term $\mathcal{L}^*_\beta(\rho)$ (respectively $\mathcal{L}^*_{U,\beta}(\rho)$) is equal to the product

$$(40)\qquad (-1)^r \frac{L^*_{K,B}(M(\rho^*))}{\Omega_\infty(M(\rho^*))R_\infty(M(\rho^*))}\cdot \Omega_{p,\beta}(M(\rho^*))R_p(M(\rho^*)) \cdot \Gamma_{\mathbb{Q}_p}(\hat{V})^{-1}\cdot \frac{P_{L,p}(\hat{W}^*(1),1)}{P_{L,p}(\hat{W},1)},$$

where $L^*_{K,B}(M(\rho^*))$ denotes the leading term at $s=0$ of the B-truncated complex L-function of $M(\rho^*)$ with $B := \Upsilon \cup S_p$ (respectively $B := S\setminus S_\infty$). Further, the regulator terms $R_\infty(M(\rho^*))$ and $R_p(M(\rho^*))$ and period terms $\Omega_\infty(M(\rho^*))$ and $\Omega_{p,\beta}(M(\rho^*))$ that occur in the above formula are as defined in the course of the proof given below.

Remark 6.6. The formulas of Theorem 6.5 represent a natural generalization of the formulas obtained by Perrin-Riou in [29, 4.2.2 and 4.3.6]. Further, by slightly altering the definition of the complex L-function an analogous formula can be proved even in the case that the condition (B_1) is not satisfied. Indeed, if condition (B_1) fails, then one can have $P_{L,p}(W,0)=0$ and so the order of vanishing at $s=0$ of the functions $L_{K,B}(M(\rho^*),s)$ and $L_K(M(\rho^*),s)$ may differ. However, to avoid this problem, in formula (40) one need only replace $P_{L,p}(\hat{W},1)$ by the leading coefficient of $P_{L,p}(\hat{W},p^s)$ at $s=0$, or equivalently one can replace the term $\frac{L^*_{K,B}(M(\rho^*))}{P_{L,p}(\hat{W},1)}$ by $\frac{L^*_{K,B\setminus\{p\}}(M(\rho^*))}{\{P_{L,p}(W,u)^{-1}P_{L,p}(\hat{W},u)\}_{u=1}}$.

Proof. We first prove all of the assertions concerning $SC_U(\hat{\mathbb{T}},\mathbb{T})$.
By [16, 4.1.4(2)] there exists a canonical isomorphism

$$(41)\qquad (\Lambda_{\mathcal{O}}(\Gamma)\otimes_{\mathcal{O}}\mathcal{O}^n)\otimes^{\mathbb{L}}_{\Lambda(G)} SC_U(\hat{\mathbb{T}},\mathbb{T}) \cong SC_U(\hat{\mathbb{T}}_{\mathrm{cyc},\rho},\mathbb{T}_{\mathrm{cyc},\rho}).$$

Lemma 3.13 therefore combines with the following result to imply that, under the stated conditions, $SC_U(\hat{\mathbb{T}},\mathbb{T})$ is semisimple at ρ and one has $r_G(SC_U(\hat{\mathbb{T}},\mathbb{T}))(\rho) = \dim_L H^1_f(\mathbb{Q},W)$.

Lemma 6.7. *We assume that the conditions (A_1), (C_1) and (D_2) are satisfied.*

(i) *Then $SC_U(\hat{\mathbb{T}}_{\mathrm{cyc},\rho},\mathbb{T}_{\mathrm{cyc},\rho})$ is semisimple if and only if the condition (F) holds.*

(ii) *Further, if condition (F) is satisfied, then* $r_\Gamma(SC_U(\hat{\mathbb{T}}_{\mathrm{cyc},\rho}, \mathbb{T}_{\mathrm{cyc},\rho})) = \dim_L H^1_f(\mathbb{Q}, W)$.

Proof. By assumption, the condition (D_2) can be combined with the isomorphism of Lemma 6.2 (iii) and the global duality isomorphism $H^3_f(\mathbb{Q}, W) \cong H^0_f(\mathbb{Q}, Z)^*$ to imply that $SC_U(\hat{W}, W)$ is acyclic outside degrees 1 and 2. Both claims therefore follow from the fact that the homomorphisms (36) and (37) are known to coincide and that there are canonical isomorphisms $L \otimes_{\Lambda(\Gamma)} \mathbb{T}_{\mathrm{cyc},\rho} \cong W$, $L \otimes_{\Lambda(\Gamma)} \hat{\mathbb{T}}_{\mathrm{cyc},\rho} \cong \hat{W}$ and thus $L \otimes_{\Lambda(\Gamma)} SC_U(\hat{\mathbb{T}}_{\mathrm{cyc},\rho}, \mathbb{T}_{\mathrm{cyc},\rho}) \cong SC_U(\hat{W}, W)$. □

We next prove the explicit formula (40) for the leading term $\mathcal{L}^*_{U,\beta}(\rho)$. Our proof of this result is closely modeled on that of [16, Thm. 4.2.26] (as amplified in [39, proof of Thm. 6.4]).

At the outset we set $N := M(\rho^*)$, let $\gamma = (\gamma_i)_i$ and $\delta = (\delta_i)_i$ denote a choice of 'good bases' (in the sense of [16, 4.2.24(3)]) of M_B^+ and t_M for $\hat{\mathbb{T}}$ and write γ' and δ' for the induced K-bases of N_B^+ and t_N respectively. Then these choices induce a morphism

$$can_{\gamma',\delta'} : \mathbf{1}_K \to \mathbf{d}_K(N_B^+)\mathbf{d}_K(t_N)^{-1}. \tag{42}$$

Furthermore, we let $P^\vee = (P_1^\vee, \ldots, P_{d(N)}^\vee)$ and $P = (P_1, \ldots, P_{d(N)})$ be K-bases of $H^1_f(N)$ and $H^1_f(N^*(1))$ respectively. Then, letting $P^d := (P_1^d, \ldots, P_{d(N)}^d)$ denote the dual basis of P, we obtain a similar morphism

$$can_{P^\vee,P^d} : \mathbf{1}_K \to \mathbf{d}_K(H^1_f(N))\mathbf{d}_K(H^1_f(N^*(1))^*)^{-1}. \tag{43}$$

Then $can := can_{\gamma',\delta'} \cdot can_{P^\vee,P^d}$ is a morphism

(44)

$$can : \mathbf{1}_K \to \Delta_K(N) = \mathbf{d}_K(N_B^+)\mathbf{d}_K(t_N)^{-1}\mathbf{d}_K(H^1_f(N))\mathbf{d}_K(H^1_f(N^*(1))^*)^{-1}.$$

We fix an embedding of K into $\mathbb{C}$. We let $\Omega_\infty(N)$ denote the determinant of the canonical isomorphism

$$\alpha_N : (N_B^+)_\mathbb{C} \to (t_N)_\mathbb{C} \tag{45}$$

with respect to the bases γ' and δ', and $R_\infty(N)$ the determinant of the inverse of the canonical isomorphism

$$h_\infty(N) : \left(H^1_f(N^*(1))^*\right)_\mathbb{C} \to H^1_f(N)_\mathbb{C} \tag{46}$$

with respect to the bases P^d and $P^\vee$ respectively. Thus we have morphisms

$$\Omega_\infty(N): \ \mathbf{1}_\mathbb{C} \xrightarrow{(can_{\gamma',\delta'})_\mathbb{C}} \mathbf{d}_K(N_B^+)_\mathbb{C}\mathbf{d}_K(t_N)_\mathbb{C}^{-1} \xrightarrow{\mathbf{d}(\alpha_N)\cdot \mathrm{id}} \mathbf{1}_\mathbb{C}$$

and

$$R_\infty(N): \ \mathbf{1}_\mathbb{C} \xrightarrow{(can_{P^\vee,P^d})_\mathbb{C}} \mathbf{d}_K(H^1_f(N))_\mathbb{C}\mathbf{d}_K(H^1_f(N^*(1))^*)_\mathbb{C}^{-1} \xrightarrow{\mathrm{id}\cdot\mathbf{d}(h_\infty(N))^{-1}} \mathbf{1}_\mathbb{C}$$

whose product gives

$$\Omega_\infty(N)R_\infty(N): \ \mathbf{1}_\mathbb{C} \xrightarrow{can} \Delta_K(N)_\mathbb{C} \xrightarrow{(\vartheta_\infty(N))_\mathbb{C}} \mathbf{1}_\mathbb{C}.$$

Upon comparing this with the leading term

$$L_K^*(M): \quad \mathbf{1}_{\mathbb{C}} \xrightarrow{\zeta_K(N)_{\mathbb{C}}} \Delta_K(N)_{\mathbb{C}} \xrightarrow{(\vartheta_\infty(N))_{\mathbb{C}}} \mathbf{1}_{\mathbb{C}}$$

we deduce that $\zeta_K(N) : \mathbf{1}_K \to \Delta_K(N)$ is equal to the morphism

$$\frac{L_K^*(M)}{\Omega_\infty(N)R_\infty(N)} \cdot can : \mathbf{1}_K \to \Delta_K(N).$$

Before proceeding we recall the relevant descent properties of Selmer complexes.

Lemma 6.8. *We use the notation of §6.3.*

(i) *There exist canonical isomorphisms of the form*

$$L^n \otimes^{\mathbb{L}}_{\Lambda,\rho} \mathrm{R}\Gamma_c(U,\mathbb{T}) \cong \mathrm{R}\Gamma_c(U,W), \quad L^n \otimes^{\mathbb{L}}_{\Lambda,\rho} SC_U(\hat{\mathbb{T}},\mathbb{T}) \cong SC_U(\hat{W},W).$$

(ii) *There exists an exact triangle of the form*

$$L^n \otimes^{\mathbb{L}}_{\Lambda,\rho} SC(\hat{\mathbb{T}},\mathbb{T}) \longrightarrow SC(\hat{W},W) \longrightarrow \textstyle\bigoplus_{\ell\in\Upsilon} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell,W) \longrightarrow \ .$$

Proof. See [16, Prop. 1.6.5 and Prop. 4.2.17]. □

Now, after taking account of Lemma 6.8(i), the leading term $\mathcal{L}^*_{U,\beta}(\rho)$ is defined (in Definition 3.14) to be equal to $(-1)^r$ times the morphism

$$\mathbf{1}_{\tilde{L}} \xrightarrow{\zeta_\Lambda(M)(\rho)_{\tilde{L}}} \mathbf{d}_L(\mathrm{R}\Gamma_c(U,W))^{-1}_{\tilde{L}} \xrightarrow{\beta(\rho)\epsilon(\hat{\mathbb{T}})^{-1}(\rho)}$$

$$\mathbf{d}_L(SC_U(\hat{W},W))^{-1}_{\tilde{L}} \xrightarrow{t(SC_U(\rho^*))_{\tilde{L}}} \mathbf{1}_{\tilde{L}}$$

where $\zeta_\Lambda(M)(\rho) := L^n \otimes_\Lambda \zeta_\Lambda(N)$, $\beta(\rho) := L^n \otimes_\Lambda \beta$ and $\epsilon(\hat{\mathbb{T}})(\rho) := L^n \otimes_\Lambda \epsilon_{p,\Lambda}(\hat{\mathbb{T}})$. But Conjecture 4.1 implies that $\zeta_\Lambda(M)(\rho)$ is equal to

$$\mathbf{1}_{\tilde{L}} \xrightarrow{\zeta_K(N)_{\tilde{L}}} \Delta_K(N)_{\tilde{L}} \xrightarrow{\vartheta_\lambda(N)} \mathbf{d}_L(\mathrm{R}\Gamma_c(U,W))^{-1}_{\tilde{L}},$$

while Conjecture 6.1 implies that

$$\epsilon(\hat{\mathbb{T}})(\rho) = \epsilon_{p,L}(\hat{W}),$$

and hence it follows that $\mathcal{L}^*_{U,\beta}(\rho)$ is equal to the product of the following seven terms (47)-(53):

(47) $$(-1)^r \frac{L_K^*(N)}{\Omega_\infty(M(\rho^*))R_\infty(N)};$$

(48) $$\Gamma_L(\hat{W})^{-1} = \Gamma_{\mathbb{Q}_p}(\hat{V})^{-1};$$

(49)

$$\Omega_{p,\beta}(M(\rho^*)) : \ \mathbf{d}_L(\hat{W})_{\tilde{L}} \xrightarrow{\cdot\,\epsilon_{dR}(\hat{W})^{-1}} \mathbf{d}_L(D_{dR}(\hat{W}))_{\tilde{L}} \xrightarrow{\mathbf{d}(g^t_{dR})} \mathbf{d}_K(t_{M(\rho^*)})_{\tilde{L}} \xrightarrow{\cdot\, can_{\gamma,\delta}}$$

$$\mathbf{d}_K\big(M(\rho^*)^+_B\big)_{\tilde{L}} \xrightarrow{\mathbf{d}(g^+_\lambda)} \mathbf{d}_L(W^+)_{\tilde{L}} \xrightarrow{\beta(\rho)} \mathbf{d}_L(\hat{W})_{\tilde{L}},$$

where we use $D^0_{dR}(\hat{W}) = 0$ for the second isomorphism and where we apply Remark 2.2 to regard this as an automorphism of $\mathbf{1}_{\tilde{L}}$;

$$(50)\qquad \prod_{\ell\in S\setminus\{p,\infty\}} P_{L,\ell}(W,1):$$

$$\mathbf{1}_L \xrightarrow{\prod \eta_\ell(W)} \textstyle\prod_{\ell\in S\setminus\{p,\infty\}} \mathbf{d}_L(\mathrm{R}\Gamma_f(\mathbb{Q}_\ell,W)) \xrightarrow{acyc} \mathbf{1}_L,$$

where the first map comes from the trivialization by the identity and the second from the acyclicity;

$$(51)\quad \{P_{L,p}(W,u)P_{L,p}(\hat{W},u)^{-1}\}_{u=1}:$$

$$\mathbf{1}_L \xrightarrow{\eta_p(W)\cdot\eta_p(\hat{W})^{-1}} \mathbf{d}_L(\mathrm{R}\Gamma_f(\mathbb{Q}_p,W))\mathbf{d}_L(\mathrm{R}\Gamma_f(\mathbb{Q}_p,\hat{W}))^{-1} \xrightarrow{\quad quasi \quad} \mathbf{1}_L,$$

where we use that $t_p(W) = D_{dR}(\hat{W}) = t_p(\hat{W})$ and the quasi-isomorphism described in Lemma 6.2(ii);

$$(52)\qquad P_{L,p}(\hat{W}^*(1),1):\ \mathbf{1}_L \xrightarrow{\overline{(\eta_p(\hat{W}^*(1)))^*}} \mathbf{d}_L(\mathrm{R}\Gamma_f(\mathbb{Q}_p,\hat{W}^*(1))) \xrightarrow{acyc} \mathbf{1}_L,$$

where we use the fact that $t_p(\hat{W}^*(1)) = D^0_{dR}(\hat{W}) = 0$;

$$(53)\quad R_p(N):\ \ \mathbf{1}_L \xrightarrow{(can_{P^\vee,P^d})_L} \mathbf{d}_K(H^1_f(N))_L\mathbf{d}_K(H^1_f(N^*(1))^*)_L^{-1} \xrightarrow{\cong}$$

$$\mathbf{d}_K(H^1_f(\mathbb{Q},W))_L\mathbf{d}_K(H^1_f(\mathbb{Q},Z)^*)_L^{-1} \xrightarrow{h_p(W)} \mathbf{1}_L$$

which is equal to the determinant over L of the isomorphism $\mathrm{ad}(h_p(W))$ with respect to the chosen bases $P^\vee$ and P.

Indeed, in order to compare $\mathcal{L}^*_{U,\beta}(\rho)$ with the product of the above terms (47)-(53) one just has to verify that after revealing all definitions and identifications, in particular all comparison isomorphisms, the same constituents show up in both expressions (here we rely on Remark 2.2 which implies that all compositions of maps in $\mathcal{C}_{\tilde{L}}$ can be interpreted as products and hence are independent of any ordering). Thus we shortly indicate how the constituents of $\mathcal{L}^*_{U,\beta}(\rho)$ give rise to precisely those in the product: As we remarked earlier, $\zeta_\Lambda(M)(\rho)$ decomposes up to the comparison isomorphism $\mathbf{d}(g^+_\lambda)$, which contributes to factor (49), into $\zeta_K(N)_L$ and $\vartheta_\lambda(N)$. While $\zeta_K(N)_L$ gives the full factor (47) and contributes with $can_{\gamma,\delta}$ and $can_{P^\vee,P^d}$ to the factors (49) and (53), respectively, the second part $\vartheta_\lambda(N)$ gives the full factor (50), the half factor (51) in the form of $\eta_p(W)$ and contributes $\mathbf{d}(g^+_{dR})$ to factor (49). Further, $\beta(\rho)$ contributes to factor (49), while according to [16, §3.3] $\epsilon(\hat{\mathbb{T}})^{-1}(\rho) = \epsilon_{p,L}(\hat{W})^{-1}$ gives the full factors (48) and (52), the other half of (51) in the form of $\eta_p(\hat{W})^{-1}$ and adds $\epsilon_{dR}(\hat{W})$ to factor (49). Finally, we had observed at the end of §6.3 that $t(SC_U(\rho^*))$ is equal to $h_p(W)$.

Since $\mathcal{L}^*_{U,\beta}(\rho)$ is equal to the product of the terms (47)-(53), it is therefore enough to show that the product of these terms is also equal to the explicit product expression in (40). But this follows immediately by a direct comparison of the maps involved and then using the fact that

$$L^*_{K,B}(N) = L^*_K(N)\cdot \prod_{\ell\in S\setminus S_\infty} P_{L,\ell}(W,1)\cdot P_{L,p}(\hat{W},1)^{-1}\cdot P_{L,p}(\hat{W}^*(1),1).$$

At this stage we have proved all of the claims in Theorem 6.5 concerning $SC_U(\hat{\mathbb{T}},\mathbb{T})$ and so it only remains to prove the analogous claims for the complex $SC(\hat{\mathbb{T}},\mathbb{T})$. But these claims can be proved easily by combining the above argument with consideration of the exact triangle

$$SC_U(\hat{W},W)\to L^n\otimes^{\mathbb{L}}_\Lambda SC(\hat{\mathbb{T}},\mathbb{T})\to \bigoplus_{\ell\notin(S_p\cup\Upsilon)} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell,W)\to$$

(which itself results from comparing the defining exact triangles (31) and (32) firstly with each other and then with the exact triangle in Lemma 6.8(ii)) and the equality

$$L^*_{K,\Upsilon'}(N) = L^*_{K,B'}(N)\prod_{\ell\in B\setminus\Upsilon} P_{L,\ell}(W,1)^{-1}$$

with $\Upsilon'=\Upsilon\cup\{p\}$ and $B'=S\setminus S_\infty$. □

Example 6.9. Let E be an elliptic curve defined over $\mathbb{Q}$. Set $M := h^1(E)(1)$ and $F_\infty := \mathbb{Q}(E(p))$ where $E(p)$ denotes the p-power torsion subgroup of $E(\overline{\mathbb{Q}})$. Then it is conjectured that $SC_U(\hat{\mathbb{T}},\mathbb{T})$ always belongs to Σ_{S^*} (cf. [11, Conj. 5.1] and [16, 4.3.5 and Prop. 4.3.7]). Further, as was shown in [16], the existence of a morphism $\mathcal{L}_\beta(M)$ as in (39) implies the existence of the element $\mathcal{L}_E$ of $K_1(\Lambda(G)_{S^*})$ that [11, Conj. 5.7] predicts to exist with a precise interpolation property for all Artin representations ρ such that $r_G(SC(\hat{\mathbb{T}},\mathbb{T}))(\rho)=0$. More generally, the formula (40) now gives a precise interpolation property for (the leading term of) the element $\mathcal{L}_E$ at all Artin representations at which the underlying archimedean and p-adic height pairings are non-degenerate.

References

[1] D. Bertrand, Valuers de fonctions theta et hauteur p-adiques, in *Séminaire de Théorie des Nombres, Paris, 1980–81*, Progress in Math. 22, Birkhäuser, 1982. 6.4

[2] M. Breuning and D. Burns, Additivity of Euler characteristics in relative algebraic K-theory, Homology, Homotopy and Applications 7 (3), (2005) 11-36. 3.2.2

[3] M. Breuning and D. Burns, On the leading terms of Artin L-functions at $s=0$ and $s=1$, to appear in Compositio Math. 5

[4] D. Burns, On the values of equivariant Zeta functions of curves over finite fields, Documenta Math. 9 (2004) 357-399. 1

[5] D. Burns, Algebraic p-adic L-functions in non-commutative Iwasawa theory, preprint, 2006. 1

[6] D. Burns and M. Flach, Motivic L-functions and Galois module structures, Math. Ann. 305 (1996) 65-102. 5.3

[7] D. Burns and M. Flach, Equivariant Tamagawa numbers for motives with (non-commutative) coefficients, Documenta Math. 6 (2001) 501-570. 1, 2.1, 2.1, 4.1, 4.2, 4.2, 4.3

[8] D. Burns and M. Flach, On the equivariant Tamagawa number conjecture for Tate motives, Part II, to appear in this volume. 5

[9] D. Burns and C. Greither, On the equivariant Tamagawa number conjecture for Tate motives, Invent. Math. 153 (2003), no. 2, 303–359. 1, 5.1

[10] P. Cassou-Noguès, Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques, Invent. Math. 51 (1979) 29-59. 5.2

[11] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication, Publ. I.H.E.S. 101 (2005) 163-208. 1, 3, 3.4, 3.4.1, 3.5, 3.20, 6.9

[12] J. Coates, P. Schneider, and R. Sujatha, Links between cyclotomic and GL_2 Iwasawa theory, Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday, (2003), 187-215. 3.5

[13] P. Colmez, Résidu en $s = 1$ des fonctions zêta p-adiques, Invent. Math. 91 (1988) 371-389. 5.4

[14] C. W. Curtis and I. Reiner, Methods of Representation Theory, Vol. I, John Wiley and Sons, New York, 1990. 5.2

[15] P. Deligne and K. Ribet, Values of Abelian L-functions at negative integers over totally real fields, Invent. Math. 59 (1980) 227-286. 5.2

[16] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory, Proc. St . Petersburg Math. Soc. 11 (2005). 1, 2.1, 2.2, 2.2, 3.15, 3.4.2, 3.5, 3.20, 4.1, 4.1, 4.2, 4.3, 4.1, 6.1, 6.1, 6.2, 6.4, 6.4, 6.4, 6.4, 6.4, 6.9

[17] R. Greenberg, On p-adic Artin L-functions, Nagoya Math. J. 89 (1983) 77-87. 5.2

[18] Y. Hachimori and O. Venjakob, Completely faithful Selmer groups over Kummer extensions, Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday, (2003), 443–478. 3.5

[19] A. Huber and G. Kings, Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture, *in* Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), 149–162, Higher Ed. Press, Beijing, 2002. 1, 4.3

[20] F. Knudsen, Determinant functors on exact categories and their extensions to categories of bounded complexes, Michigan Math. J. 50 (2002), 407-444. 2.1

[21] B. Mazur and K. Rubin, Finding large Selmer groups, J. Differential Geometry 70 (2005), 1-22. 1

[22] B. Mazur and J. Tate, Canonical height pairings via biextensions, in *Arithmetic and geometry*, Vol. I, 195–237, Progress in Math. 35, Birkhäuser, 1983. 6.3

[23] J. Nekovář, On p-adic height pairings, in *Séminaire de Théorie des Nombres, Paris, 1990–91*, 127–202, Progress in Math. 108, Birkhäuser, 1993. 6.2, 6.2, 6.3

[24] J. Nekovář, Selmer complexes, to appear in Astérisque. 1, 6.3

[25] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of number fields, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, 2000. 3.1

[26] B. Perrin-Riou, Théorie d'Iwasawa et hauteurs p-adiques, Invent. Math. 109 (1992), no. 1, 137–185. 6.3

[27] B. Perrin-Riou, Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes), Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 203–220. 1

[28] B. Perrin-Riou, Representations p-adiques ordinaires, Astérisque 223 (1994), 185–220. 6.3

[29] B. Perrin-Riou, p-adic L-functions and p-adic representations, SMF/AMS Texts and Monographs, vol. 3, Amer. Math. Soc., Providence, RI, 2000. 1, 6.1, 6.6

[30] M. Rapoport and T. Zink, Über die lokale Zetafunktion von Shimuravarietäten. Monodromiefiltration und verschwindende Zyklen in ungleicher Charakteristik, Invent. Math. 68 (1982) 21-101. 3.2.1

[31] P. Schneider, Height pairings in the Iwasawa theory of abelian varieties, in *Séminaire de Théorie des Nombres, Paris, 1980–81*, 309–316, Progress in Math. 22, Birkhäuser, 1982. 1

[32] P. Schneider, p-adic height pairings. I., Invent. Math. 69 (1982), 401–409. 1, 6.3

[33] P. Schneider, Iwasawa L-functions of varieties over algebraic number fields. A first approach, Invent. Math. 71 (1983), no. 2, 251–293. 1

[34] P. Schneider, p-adic height pairings. II., Invent. Math. 79 (1985), 329–374. 1

[35] J-P. Serre, Sur le résidue de la fonction zêta p-adique d'un corps de nombres, C.R. Acad. Sci. Paris 278 (1978) 183-188. 1, 5, 5.3

[36] D. Solomon, p-adic abelian Stark conjecture at $s = 1$, Ann. Inst. Fourier 52 (2002) 379-417. 5.3

[37] J. Tate, Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$ (notes par D. Bernardi et N. Schappacher), Progress in Math., 47, Birkhäuser, Boston, 1984. 1, 5, 5.2, 5.3, 5.4, 5.3

[38] O. Venjakob, Characteristic Elements in Noncommutative Iwasawa Theory, J. reine angew. Math., 583, 2005. 3.5, 3.20

[39] O. Venjakob, From the Birch and Swinnerton-Dyer Conjecture to noncommutative Iwasawa theory via the Equivariant Tamagawa Number Conjecture - a survey, to appear in 'L-functions and Galois representations',

Proceedings of the 2004 Durham Symposium, C.U.P. 1, 4.1, 4.1, 4.2, 4.3, 6.1, 6.4, 6.4

[40] C. Wuthrich, On p-adic heights in families of elliptic curves, J. London Math. Soc. (2) 70 (2004), no. 1 , 23–40. 6.4

[41] Y. Zarhin, Neron coupling and quasicharacters, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 497–509. 6.3

[42] S. Zerbes, Selmer groups over p-adic Lie extensions. I, J. London Math. Soc. (2) 70 (2004), no. 3, 586–608. 3.5

David Burns
King's College London
Dept. of Mathematics
London WC2R 2LS
United Kingdom

Otmar Venjakob
Universität Bonn
Mathematisches Institut
Beringstraße 1
D-53115 Bonn
Germany

The 2-adic Eigencurve is Proper.

Kevin Buzzard[1] and Frank Calegari[2]

Received: August 25, 2005
Revised: February 27, 2006

Abstract. Coleman and Mazur ask whether the Eigencurve has any "holes". We answer their question in the negative for the 2-adic Eigencurve of tame level one.

2000 Mathematics Subject Classification: 11F11, 14G35
Keywords and Phrases: Modular Forms, Modular Curves

Dedicated to John Coates on his 60th birthday.

1 Introduction

In [7], Coleman and Mazur construct a rigid analytic space $\mathcal{E}$ (the "Eigencurve") that parameterizes overconvergent and therefore classical modular eigenforms of finite slope. The geometry of $\mathcal{E}$ is at present poorly understood, and seems quite complicated, especially over the centre of weight space. Recently, some progress has been made in understanding the geometry of $\mathcal{E}$ in certain examples (see for example [3],[4]). Many questions remain. In this paper, we address the following question raised on p5 of [7]:

> Do there exist p-adic analytic families of overconvergent eigenforms of finite slope parameterized by a punctured disc, and converging, at the puncture, to an overconvergent eigenform of infinite slope?

We answer this question in the negative for the 2-adic eigencurve of tame level 1. Another way of phrasing our result is that the map from the eigencurve to weight space satisfies the *valuative criterion of properness*, and it is in this sense that the phrase "proper" is used in the title, since the projection to weight space has infinite degree and so is not technically proper in the sense of rigid analytic geometry. One might perhaps say that this map is "functorially proper". Our approach is based on the following simple idea. One knows (for instance, from [1]) that finite slope eigenforms of integer weight may be

[1] Supported in part by an EPSRC Advanced Research Fellowship
[2] Supported in part by the American Institute of Mathematics

analytically continued far into the supersingular regions of the moduli space. On the other hand, it turns out that eigenforms in the kernel of U do not extend as far. Now one can check that a limit of highly overconvergent eigenforms is also highly overconvergent, and this shows that given a punctured disc as above, the limiting eigenform cannot lie in the kernel of U.

The problem with this approach is that perhaps the most natural definition of "highly overconvergent" is not so easy to work with at non-integral weight. The problem stems from the fact that such forms of non-integral weight are not defined as sections of a line bundle. In fact Coleman's definition of an overconvergent form of weight κ is a formal q-expansion F for which F/E_κ is overconvergent of weight 0, where E_κ is the p-deprived weight κ Eisenstein series. One might then hope that the overconvergence of F/E_κ would be a good measure of the overconvergence of F. One difficulty is that if F is an eigenform for the Hecke operators, the form F/E_κ is unlikely to be an eigenform. This does not cause too much trouble when proving that finite slope eigenforms overconverge a long way, as one can twist the U-operator as explained in [5] and apply the usual techniques. We outline the argument in sections 2 and 3 of this paper. On the other hand we do not know how to prove general results about (the lack of) overconvergence of forms in the kernel of U in this generality. Things would be easier if we used $V(E_\kappa)$ to twist from weight κ to weight 0, but unfortunately the results we achieve using this twist are not strong enough for us to get the strict inequalities that we need.

The approach that we take in our "test case" of $N = 1$ and $p = 2$ is to control the kernel of U in weight κ by explicitly writing down the matrix of U (and of $2VU - \mathrm{Id}$) with respect to a carefully-chosen basis. To enable us to push the argument through, however, we were forced to diverge from Coleman's choice of twist. We define the overconvergence of F, not in terms of F/E_κ, but rather in terms of F/h^s for some explicit modular form h. The benefit of our choice of h is that it is nicely compatible with the explicit formulae developed in [3], and hence we may prove all our convergence results by hand in this case. Our proof that eigenforms of finite slope overconverge "as far as possible" is essentially standard. The main contribution of this paper is to analyze the overconvergence (or lack thereof) of eigenforms in the kernel of the U operator in this case.

One disadvantage of our approach is that the power series defining h^s only converges for s sufficiently small and hence our arguments only deal with forms whose weights lie in a certain disc at the centre of weight space. However, recently in [4], the 2-adic level 1 eigencurve was shown to be a disjoint union of copies of weight space near the boundary of weight space, and hence is automatically proper there.

2 Definitions

Let $\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$ denote the classical level 1 weight 12 modular form (where $q = e^{2\pi i\tau}$). Set

$$f = \Delta(2\tau)/\Delta(\tau) = q + 24q^2 + 300q^3 + 2624q^4 + \cdots,$$

a uniformizer for $X_0(2)$, and

$$h = \Delta(\tau)^2/\Delta(2\tau) = \prod_{n\geq 1}\left(\frac{1-q^n}{1+q^n}\right)^{24} = 1 - 48q + 1104q^2 - 16192q^3 + \ldots$$

a modular form of level 2 and weight 12. Note that the divisor of h is $3(0)$, where (0) denotes the zero cusp on $X_0(2)$, and hence that

$$h^{1/3} = \prod_{n\geq 1}\left(\frac{1-q^n}{1+q^n}\right)^{8}$$

is a classical modular form of weight 4 and level 2.

We briefly review the theory of overconvergent p-adic modular forms, and make it completely explicit in the setting we are interested in, namely $p = 2$ and tame level 1. Let $\mathbb{C}_2$ denote the completion of an algebraic closure of $\mathbb{Q}_2$. Normalize the norm on $\mathbb{C}_2$ such that $|2| = 1/2$, and normalize the valuation $v : \mathbb{C}_2^\times \to \mathbb{Q}$ so that $v(2) = 1$. Choose a group-theoretic splitting of v sending 1 to 2, and let the resulting homomorphism $\mathbb{Q} \to \mathbb{C}_2^\times$ be denoted $t \mapsto 2^t$. Define $v(0) = +\infty$. Let $\mathcal{O}_2$ denote the elements of $\mathbb{C}_2$ with non-negative valuation.

If $r \in \mathbb{Q}$ with $0 < r < 2/3$ (note that $2/3 = p/(p+1)$ if $p = 2$) then there is a rigid space $X_0(1)_{\geq 2^{-r}}$ over $\mathbb{C}_2$ such that functions on this space are r-overconvergent 2-adic modular functions. Let $X[r]$ denote the rigid space $X_0(1)_{\geq 2^{-r}}$. By Proposition 1 of the appendix to [3], we see that $X[r]$ is simply the closed subdisc of the j-line defined by $|j| \geq 2^{-12r}$. We will also need to use (in Lemma 6.13) the rigid space $X[2/3]$, which we define as the closed subdisc of the j-line defined by $|j| \geq 2^{-8}$. The parameter q can be viewed as a rigid function defined in a neighbourhood of ∞ on $X[r]$, and hence any rigid function on $X[r]$ can be written as a power series in q; this is the q-expansion of the form in this rigid analytic setting. Moreover, it is well-known that the classical level 2 form f descends to a function on $X[r]$ (for any $r < 2/3$), with the same q-expansion as that given above.

For $0 < r < 2/3$, define $M_0[r]$ to be the space of rigid functions on $X[r]$, equipped with its supremum norm. Then $M_0[r]$ is a Banach space over $\mathbb{C}_2$ — it is the space of r-overconvergent modular forms of weight 0. An easy calculation using the remarks after Proposition 1 of the appendix to [3] shows that the set $\{1, 2^{12r}f, 2^{24r}f^2, \ldots, (2^{12r}f)^n, \ldots\}$ is an orthonormal Banach basis for $M_0[r]$, and we endow $M_0[r]$ once and for all with this basis.

We define $\mathcal{W}$ to be the open disc of centre 1 and radius 1 in the rigid affine line over $\mathbb{C}_2$. If $w \in \mathcal{W}(\mathbb{C}_2)$ then there is a unique continuous group homomorphism $\kappa : \mathbb{Z}_2^\times \to \mathbb{C}_2^\times$ such that $\kappa(-1) = 1$ and $\kappa(5) = w$; moreover this establishes a bijection between $\mathcal{W}(\mathbb{C}_2)$ and the set of even 2-adic weights, that is, continuous group homomorphisms $\kappa : \mathbb{Z}_2^\times \to \mathbb{C}_2^\times$ such that $\kappa(-1) = 1$. Note that if k is an even integer then the map $x \mapsto x^k$ is such a homomorphism, and we refer to this weight as weight k. Let $\tau : \mathbb{Z}_2^\times \to \mathbb{C}_2^\times$ denote the character with kernel equal to $1 + 4\mathbb{Z}_2$, and let $\langle\cdot\rangle$ denote the character $x \mapsto x/\tau(x)$; this character corresponds to $w = 5 \in \mathcal{W}(\mathbb{C}_2)$. If $t \in \mathbb{C}_2$ with $|t| < 2$ then we may define $5^t := \exp\big(t\log(5)\big) \in \mathcal{W}(\mathbb{C}_2)$ and we let $\langle\cdot\rangle^t$ denote the homomorphism $\mathbb{Z}_2^\times \to \mathbb{C}_2^\times$ corresponding to this point of weight space. One checks easily that the points of weight space corresponding to characters of this form are $\{w \in \mathcal{W}(\mathbb{C}_2) : |w-1| < 1/2\}$.

We now explain the definitions of overconvergent modular forms of general weight that we shall use in this paper. Recall $h = \prod_{n\geq 1}(1-q^n)^{24}/(1+q^n)^{24}$. Define $h^{1/8}$ to be the formal q-expansion $\prod_{n\geq 1}((1-q^n)^3/(1+q^n)^3$. Now

$$(1-q^n)/(1+q^n) = 1 - 2q^n + 2q^{2n} - \cdots \in 1 + 2q\mathbb{Z}[[q]]$$

and hence $h^{1/8} \in 1 + 2q\mathbb{Z}[[q]]$. Write $h^{1/8} = 1 + 2qg$ with $g \in \mathbb{Z}[[q]]$. If S is a formal variable then we define $h^S \in 1 + 16qS\mathbb{Z}_2[[8S, q]]$ to be the formal binomial expansion of $(1+2qg)^{8S}$. If $s \in \mathbb{C}_2$ with $|s| < 8$ then we define h^s to be the specialization in $1 + 2q\mathcal{O}_2[[q]]$ of h^S at $S = s$. In fact for the main part of this paper we shall only be concerned with h^s when $|s| < 4$.

If $s \in \mathbb{C}_2$ with $|s| < 8$, then define $\mu(s) := \min\{v(s), 0\}$, so $-3 < \mu(s) \leq 0$. Define $\mathcal{X}$ to be the pairs (κ, r) (where $\kappa : \mathbb{Z}_2^\times \to \mathbb{C}_2^\times$ and $r \in \mathbb{Q}$) such that there exists $s \in \mathbb{C}_2$ with $|s| < 8$ satisfying

- $\kappa = \langle\cdot\rangle^{-12s}$, and
- $0 < r < 1/2 + \mu(s)/6$.

Note that the second inequality implies $r < 1/2$, and conversely if $|s| \leq 1$ and $0 < r < 1/2$ then $(\langle\cdot\rangle^{-12s}, r) \in \mathcal{X}$.

For $(\kappa, r) \in \mathcal{X}$, and only for these (κ, r), we define the space $M_\kappa[r]$ of r-overconvergent forms of weight κ thus. Write $\kappa = \langle\cdot\rangle^{-12s}$ and define $M_\kappa[r]$ to be the vector space of formal q-expansions $F \in \mathbb{C}_2[[q]]$ such that Fh^s is the q-expansion of an element of $M_0[r]$. We give $M_\kappa[r]$ the Banach space structure such that multiplication by h^s induces an isomorphism of Banach spaces $M_\kappa[r] \to M_0[r]$, and we endow $M_\kappa[r]$ once and for all with the orthonormal basis $\{h^{-s}, h^{-s}(2^{12r}f), h^{-s}(2^{12r}f)^2, \ldots\}$.

Remark 2.1. *We do not consider the question here as to whether, for all $(\kappa, r) \in \mathcal{X}$, the space $M_\kappa[r]$ is equal to the space of r-overconvergent modular forms of weight κ as defined by Coleman (who uses the weight κ Eisenstein series E_κ to pass from weight κ to weight 0). One could use the methods* *of proof of §5 of [4] to verify this; the issue is verifying whether $E_\kappa h^s$ is r-overconvergent and has no zeroes on $X[r]$. However, we do not need this result — we shall prove all the compactness results for the U operator that we need by explicit matrix computations, rather than invoking Coleman's results. Note however that our spaces clearly coincide with Coleman's if $\kappa = 0$, as the two definitions coincide in this case. Note also that for $r > 0$ sufficiently small (depending on $\kappa = \langle\cdot\rangle^{-12s}$ with $|s| < 8$), the definitions do coincide, because if $E_1 := 1 + 4q + 4q^2 + \cdots$ denotes the weight 1 level 4 Eisenstein series, then $h/E_1^{12} = 1 - 96q + \cdots$ is overconvergent of weight 0, has no zeroes on $X[r]$ for $r < 1/3$, and has q-expansion congruent to 1 mod 32. Hence for $r > 0$ sufficiently small, the supremum norm of $(h/E_1^{12}) - 1$ on $X[r]$ is t with $t < 1/2$ and $|s|t < 1/2$, and this is enough to ensure that the power series $(h/E_1^{12})^s$ is the q-expansion of a function on $X[r]$ with supremum norm at most 1. Hence instead of using powers of h to pass between weight κ and weight 0, we could use powers of E_1. Finally, Corollary B4.5.2 of [5] shows that if $\kappa = \langle\cdot\rangle^{-12s}$ then there exists $r > 0$ such that E_1^{-12s}/E_κ is r-overconvergent, which suffices.*

Recall that if X and Y are Banach spaces over a complete field K with orthonormal bases $\{e_0, e_1, e_2, \ldots\}$ and $\{f_0, f_1, f_2, \ldots\}$, then by the *matrix* of a continuous linear map $\alpha : X \to Y$ we mean the collection $(a_{ij})_{i,j\geq 0}$ of elements of K such that $\alpha(e_j) = \sum_{i\geq 0} a_{ij} f_i$. One checks that

- $\sup_{i,j} |a_{ij}| < \infty$, and
- for all j we have $\lim_{i\to\infty} |a_{ij}| = 0$,

and conversely that given any collection $(a_{ij})_{i,j\geq 0}$ of elements of K having these two properties, there is a unique continuous linear map $\alpha : X \to Y$ having matrix $(a_{ij})_{i,j\geq 0}$ (see Proposition 3 of [10] and the remarks following it for a proof). When we speak of "the matrix" associated to a continuous linear map between two spaces of overconvergent modular forms, we will mean the matrix associated to the map using the bases that we fixed earlier.

If R is a ring then we may define maps U, V and W on the ring $R[[q]]$ by

$$U\left(\sum a_n q^n\right) = \sum a_{2n} q^n,$$
$$V\left(\sum a_n q^n\right) = \sum a_n q^{2n},$$

and

$$W\left(\sum a_n q^n\right) = \sum (-1)^n a_n q^n.$$

Recall that $U(V(G)F) = GU(F)$ for F, G formal power series in q, and that $V : R[[q]] \to R[[q]]$ is a ring homomorphism. The operator W is not standard (or at least, our notation for it is not standard), but is also a ring homomorphism (it sends $f(q)$ to $f(-q)$) and one also checks easily that $W = 2VU - \mathrm{Id}$. We shall show later on that there are continuous linear maps between various spaces of overconvergent modular forms which correspond to U and W, and will write down explicit formulae for the matrices associated to these linear maps.

3 The U operator on overconvergent modular forms

Our goal in this section is to make precise the statement in the introduction that finite slope U-eigenforms overconverge a long way. Fix $r \in \mathbb{Q}$ with $0 < r < 1/2$. We will show that if $(\kappa, r) \in \mathcal{X}$ then the U-operator (defined on q-expansions) induces a continuous linear map $M_\kappa[r] \to M_\kappa[r]$, and we will compute the matrix of this linear map (with respect to our chosen basis of $M_\kappa[r]$). We will deduce that if $0 < \rho < r$ and F is ρ-overconvergent with $UF = \lambda F \neq 0$ then F is r-overconvergent. These results are essentially standard but we shall re-prove them, for two reasons: firstly to show that the arguments still go through with our choice of twist, and secondly to introduce a technique for computing matrices of Hecke operators in arbitrary weight that we shall use when analyzing the W operator later.
It is well-known that the U-operator induces a continuous linear map $U : M_0[r] \to M_0[r]$, and its associated matrix was computed in [3]. Now choose $m \in \mathbb{Z}_{\geq 0}$, and set $k = -12m$. One checks that $(k, r) \in \mathcal{X}$. If $\phi \in M_0[r]$ then

$$h^m U\left(h^{-m}\phi\right) = h^m U\left(\Delta(2\tau)^{-m} f^{2m}\phi\right)$$
$$= h^m \Delta(\tau)^{-m} U\left(f^{2m}\phi\right) = f^{-m} U\left(f^{2m}\phi\right).$$

A simple analysis of the q-expansion of $f^{-m}U(f^{2m}\phi)$ shows that it has no pole at the cusp of $X[r]$ and hence $f^{-m}U(f^{2m}\phi) \in M_0[r]$. We deduce that U induces a continuous map $M_k[r] \to M_k[r]$, and moreover that the matrix of this map (with respect to the basis fixed earlier) equals the matrix of the operator $U_k := f^{-m}Uf^{2m}$ acting on $M_0[r]$. We now compute this matrix.

Lemma 3.1. *For $m \in \mathbb{Z}_{\geq 0}$ and $k = -12m$ as above, and $j \in \mathbb{Z}_{\geq 0}$, we have*

$$U_k\left((2^{12r}f)^j\right) = \sum_{i=0}^{\infty} u_{ij}(m)(2^{12r}f)^i,$$

where $u_{ij}(m)$ is defined as follows: we have $u_{00}(0) = 1$, $u_{ij}(m) = 0$ if $2i - j < 0$ or $2j - i + 3m < 0$, and

$$u_{ij}(m) = \frac{3(i+j+3m-1)!(j+2m)2^{8i-4j+12r(j-i)}}{2(2i-j)!(2j-i+3m)!}$$

if $2i - j \geq 0$, $2j - i + 3m \geq 0$, and i, j, m are not all zero.

Proof. The case $m = 0$ of the lemma is Lemma 2 of [3], and the general case follows easily from the fact that $U_k = f^{-m}Uf^{2m}$. Note that in fact all the sums in question are finite, as $u_{ij}(m) = 0$ for $i > 2j + 3m$. □

Now for $i, j \in \mathbb{Z}_{\geq 0}$ define a polynomial $u_{ij}(S) \in \mathbb{C}_2[S]$ by $u_{ij}(S) = 0$ if $2i < j$, $u_{ij}(S) = 2^{12ir}$ if $2i = j$, and

$$u_{ij}(S) = \frac{3 \cdot 2^{12r(j-i)}(j+2S)2^{8i-4j}}{2(2i-j)!} \prod_{\lambda=1}^{2i-j-1} (2j - i + \lambda + 3S)$$

if $2i > j$. One checks easily that evaluating $u_{ij}(S)$ at $S = m$ for $m \in \mathbb{Z}_{\geq 0}$ gives $u_{ij}(m)$, so there is no ambiguity in notation. Our goal now is to prove that for all $s \in \mathbb{C}_2$ such that $|s| < 8$ and $(\langle\cdot\rangle^{-12s}, r) \in \mathcal{X}$, the matrix $(u_{ij}(s))_{i,j\geq 0}$ is the matrix of the U-operator acting on $M_\kappa[r]$ for $\kappa = \langle\cdot\rangle^{-12s}$ (with respect to the basis of $M_\kappa[r]$ that we fixed earlier).

Say $s \in \mathbb{C}_2$ with $|s| < 8$, define $\kappa = \langle\cdot\rangle^{-12s}$, set $\mu = \min\{v(s), 0\}$, and say $0 < r < 1/2 + \mu/6$. Then $(\kappa, r) \in \mathcal{X}$. Note that $v(as + b) \geq \mu$ for any $a, b \in \mathbb{Z}$, and $3 + \mu - 6r > 0$.

Lemma 3.2. *(a) One has* $v(u_{ij}(s)) \geq (3 + \mu - 6r)(2i - j) + 6rj$.
(b) There is a continuous linear map $U(s) : M_0[r] \to M_0[r]$ *with matrix* $u_{ij}(s)$. *Equivalently, there is a continuous linear map* $U(s) : M_0[r] \to M_0[r]$ *such that*

$$U(s)\left((2^{12r}f)^j\right) = \sum_{i=0}^{\infty} u_{ij}(s)(2^{12r}f)^i.$$

Proof. (a) This is a trivial consequence of our explicit formula for $u_{ij}(s)$, the remark about $v(as + b)$ above, and the fact that $v(m!) \leq m - 1$ if $m \geq 1$ (see Lemma 6.2).

(b) Recall that $u_{ij}(s) = 0$ if $2i < j$. Hence by (a) we see that $|u_{ij}(s)| \leq 1$ for all i, j. It remains to check that for all j we have $\lim_{i\to\infty} v(u_{ij}(s)) = +\infty$ which is also clear from (a). □

Note that $U(s) = U_{-12s}$ if $s = m \in \mathbb{Z}_{\geq 0}$.

In fact the same argument gives slightly more. Choose $\epsilon \in \mathbb{Q}$ with $0 < \epsilon < \min\{r, 1/2 + \mu/6 - r\}$. Then $(\kappa, r + \epsilon) \in \mathcal{X}$.

Theorem 3.3. *The endomorphism* $U(s)$ *of* $M_0[r]$ *is the composite of a continuous map* $M_0[r] \to M_0[r + \epsilon]$ *and the restriction* $M_0[r + \epsilon] \to M_0[r]$.

Proof. Define $w_{ij}(s) = u_{ij}(s)/2^{12\epsilon i}$. By the previous lemma we have

$$v(w_{ij}(s)) \geq (2i - j)(3 + \mu - 6r - 6\epsilon) + 6j(r - \epsilon)$$

and $w_{ij}(s) = 0$ if $j > 2i$. In particular $v(w_{ij}(s)) \geq 0$ for all i, j, and moreover for all j we have $\lim_{i\to\infty} w_{ij}(s) = 0$. The continuous linear map $M_0[r] \to M_0[r+\epsilon]$ with matrix $(w_{ij}(s))_{i,j\geq 0}$ will hence do the job. □

As usual say $|s| < 8$, $\kappa = \langle\cdot\rangle^{-12s}$ and $(\kappa, r) \in \mathcal{X}$.

Corollary 3.4. *The map* $U(s) : M_0[r] \to M_0[r]$ *is compact and its characteristic power series is independent of* r *with* $0 < r < 1/2 + \mu/6$. *Furthermore if* $0 < \rho < r$ *then any non-zero* $U(s)$*-eigenform with non-zero eigenvalue on* $M_0[\rho]$ *extends to an element of* $M_0[r]$.

Proof. This follows via standard arguments from the theorem; see for example Proposition 4.3.2 of [7], although the argument dates back much further. □

Keep the notation: $|s| < 8$, $\kappa = \langle\cdot\rangle^{-12s}$, $\mu = \min\{v(s), 0\}$ and $0 < r < 1/2 + \mu/6$, so $(\kappa, r) \in \mathcal{X}$. We now twist $U(s)$ back to weight κ and show that the resulting compact operator is the U-operator (defined in the usual way on power series).

Proposition 3.5. *The compact endomorphism of $M_\kappa[r]$ defined by $\phi \mapsto h^{-s}U(s)(h^s\phi)$ is the U-operator, i.e., sends $\sum a_n q^n$ to $\sum a_{2n} q^n$.*

Proof. It suffices to check the proposition for $\phi = h^{-s}(2^{12r}f)^j$ for all $j \in \mathbb{Z}_{\geq 0}$, as the result then follows by linearity. If S is a formal variable then recall that we may think of h^S as an element of $1 + 16qS\mathcal{O}_2[[8S, q]])$ and in particular as an invertible element of $\mathcal{O}_2[[8S, q]]$. Write h^{-S} for its inverse. We may think of $(h^S)U(h^{-S}(2^{12r}f)^j)$ as an element of $\mathcal{O}_2[[8S, q]]$ (though not yet as an element of $M_0[r]$). Write

$$(h^S)U(h^{-S}(2^{12r}f)^j) = \sum_{i\geq 0} \tilde{u}_{ij}(S)(2^{12r}f)^i$$

with $\tilde{u}_{ij}(S) \in \mathcal{O}_2[[8S]] \otimes \mathbb{C}_2$ (this is clearly possible as $f = q + \ldots$). The proposition is just the statement that the power series $\tilde{u}_{ij}(S)$ equals the polynomial $u_{ij}(S)$. Now there exists some integer $N \gg 0$ such that both $2^N u_{ij}(S)$ and $2^N \tilde{u}_{ij}(S)$ lie in $\mathcal{O}_2[[8S]]$ (as $u_{ij}(S)$ is a polynomial). Furthermore, Lemma 3.1 shows that $u_{ij}(m) = \tilde{u}_{ij}(m)$ for all $m \in \mathbb{Z}_{\geq 0}$ and hence $2^N(u_{ij}(S) - \tilde{u}_{ij}(S))$ is an element of $\mathcal{O}_2[[8S]]$ with infinitely many zeroes in the disc $|8s| < 1$, so it is identically zero by the Weierstrass approximation theorem. □

Corollary 3.6. *If $(\kappa, r) \in \mathcal{X}$ and $\kappa = \langle\cdot\rangle^{-12s}$ then U is a compact operator on $M_\kappa[r]$ and its characteristic power series coincides with the characteristic power series of $U(s)$ on $M_0[r]$. Furthermore $F \in M_\kappa[r]$ is an eigenvector for U iff $Fh^s \in M_0[r]$ is an eigenvector for $U(s)$.*

Proof. Clear. □

The utility of these results is that they allow us to measure the overconvergence of a finite slope form F of transcendental weight by instead considering the associated form Fh^s in weight 0. This will be particularly useful to us later on in the case when F is in the kernel of U. We record explicitly what we have proved. By an overconvergent modular form of weight κ we mean an element of $\bigcup_r M_\kappa[r]$, where r runs through the $r \in \mathbb{Q}$ for which $(\kappa, r) \in \mathcal{X}$.

Corollary 3.7. *If $(\kappa, r) \in \mathcal{X}$ and f is an overconvergent modular form of weight κ which is an eigenform for U with non-zero eigenvalue, then f extends to an element of $M_\kappa[r]$.*

Proof. This follows from 3.4 and 3.5. □

In fact we will need a similar result for families of modular forms, but our methods generalize to this case. We explicitly state what we need.

Corollary 3.8. *Let $A \subseteq \mathcal{W}$ be an affinoid subdomain, say $0 < \rho < r < 1/2$, and assume that for all $\kappa \in A(\mathbb{C}_2)$ we have $(\kappa, r) \in \mathcal{X}$. Let $F \in \mathcal{O}(A)[[q]]$ be an analytic family of ρ-overconvergent modular forms, such that $UF = \lambda F$ for some $\lambda \in \mathcal{O}(A)^\times$. Then F is r-overconvergent.*

□

4 The W operator on overconvergent modular forms

We need to perform a similar analysis to the previous section with the operator W. Because $W = 2VU - \mathrm{Id}$ we know that W induces a continuous linear map $V : M_0[r] \to M_0[r]$ for $r < 1/3$ (for r in this range, U doubles and then V halves the radius of convergence). Our goal in this section is to show that, at least for $\kappa = \langle\cdot\rangle^{-12s}$ with $|s| < 8$, there is an operator on weight κ overconvergent modular forms which also acts on q-expansions in this manner, and to compute its matrix.

We proceed as in the previous section by firstly introducing a twist of W. If $m \in \mathbb{Z}_{\geq 0}$, if $k = -12m$ and if $\phi \in M_0[r]$ then the fact that $h(q)/h(-q) = (f(-q)/f(q))^2$ implies

$$h^m W(h^{-m}\phi) = f^{-2m} W(f^{2m}\phi)$$

and so we define the operator W_k on $M_0[r]$, $r < 1/3$, by $W_k := f^{-2m} W f^{2m} : M_0[r] \to M_0[r]$.

Set $g = Wf$, so $g(q) = f(-q) = -q + 24q^2 - 300q^3 + \ldots$. Because $g = 2VUf - f = 48Vf + 4096(Vf)^2 - f$, we see that the g can be regarded as a meromorphic function on $X_0(4)$ of degree at most 4. Similarly f may be regarded as a function on $X_0(4)$ of degree 2. Now the meromorphic function

$$(1 + 48f - 8192f^2g)^2 - (1 + 16f)^2(1 + 64f)$$

on $X_0(4)$ has degree at most 16 but the first 1000 terms of its q-expansion can be checked to be zero on a computer, and hence this function is identically zero. We deduce the identity

$$g = \frac{1 + 48f - (1 + 16f)\sqrt{1 + 64f}}{8192f^2},$$

where the square root is the one of the form $1 + 32f + \ldots$, and one verifies using the binomial theorem that $g = \sum_{i \geq 1} c_i f^i$ with

$$\begin{aligned} c_i &:= (-1)^i 2^{4i-4} \left(\frac{(2i+2)!}{(i+1)!(i+2)!} - \frac{(2i)!}{i!(i+1)!} \right) \\ &= (-1)^i 2^{4(i-1)} \frac{3(2i)!}{(i-1)!(i+2)!} \end{aligned}$$

The other ingredient we need to compute the matrix of W_k is a combinatorial lemma.

Lemma 4.1. *If $j \geq 1$ and $i \geq j+1$ are integers then*

$$\sum_{a=j}^{i-1} \frac{3(2a+j-1)!j(2i-2a)!}{(a-j)!(a+2j)!(i-a-1)!(i-a+2)!} = \frac{(2i+j)!(j+1)}{(i-j-1)!(i+2j+2)!}.$$

Proof. Set $k = i-1-a$ and $n = i-1-j$ and then eliminate the variables i and a; the lemma then takes the form

$$\sum_{k=0}^{n} F(j,n,k) = G(j,n)$$

and, for fixed n and k, both $F(j,n,k)$ and $G(j,n)$ are rational functions of j. The lemma is now easily proved using Zeilberger's algorithm (regarding j as a free variable), which proves that the left hand side of the equation satisfies an explicit (rather cumbersome) recurrence relation of degree 1; however it is easily checked that the right hand side is a solution to this recurrence relation, and this argument reduces the proof of the lemma to the case $n = 0$, where it is easily checked by hand. □

We now compute the matrix of W_k on $M_0[r]$ for $r < 1/3$ and $k = -12m$, $m \in \mathbb{Z}_{\geq 0}$.

Lemma 4.2. *For $j \geq 0$ we have*

$$W_k\big((2^{12r}f)^j\big) = \sum_{i=0}^{\infty} \eta_{ij}(m)(2^{12r}f)^i,$$

where $\eta_{ij}(m)$ is defined as follows: we have $\eta_{ij}(m) = 0$ if $i < j$, $\eta_{ii}(m) = (-1)^i$, and for $i > j$ we define

$$\eta_{ij}(m) = \frac{(2i+j-1+6m)!3(j+2m)\cdot 2^{(4-12r)(i-j)}(-1)^i}{(i-j)!(i+2j+6m)!}.$$

Proof. We firstly deal with the case $m = 0$, by induction on j. The case $j = 0$ is easily checked as $\eta_{i0}(0) = 0$ for $i > 0$, and the case $j = 1$ follows from the fact that $c_i 2^{12r(1-i)} = \eta_{i1}(0)$ for $i \geq 1$, as is easily verified. For $j \geq 1$ we have $W(f^{j+1}) = f(-q)^{j+1} = g \cdot W(f^j) = (\sum_{t\geq 1} c_t f^t)W(f^j)$, and so to finish the $m = 0$ case it suffices to verify that for $j \geq 1$ and $i \geq j+1$ we have $\eta_{i\,j+1}(0) = 2^{12r}\sum_{a=0}^{i-1} c_{i-a}2^{-12r(i-a)}\eta_{aj}(0)$, which quickly reduces to the combinatorial lemma above.
Finally we note that because $\eta_{i+2m\,j+2m}(0) = \eta_{ij}(m)$, the general case follows easily from the case $m = 0$ and the fact that $W_k = f^{-2m}Wf^{2m}$. □

As before, we now define polynomials $\eta_{ij}(S)$ by $\eta_{ij}(S) = 0$ if $i < j$, $\eta_{ii}(S) = (-1)^i$, and

$$\eta_{ij}(S) = \frac{3(j+2S)2^{(4-12r)(i-j)}(-1)^i}{(i-j)!}\prod_{\lambda=1}^{i-j-1}(i+2j+\lambda+6S)$$

for $i > j$. We observe that $\eta_{ij}(S)$ specializes to $\eta_{ij}(m)$ when $S = m \in \mathbb{Z}_{\geq 0}$. Now if $|s| < 8$ and $\kappa = \langle\cdot\rangle^{-12s}$, and we set $\lambda = \min\{v(2s), 0\} > -2$, then we check easily that $v(\eta_{ij}(s)) \geq (3 - 12r + \lambda)(i - j) + 1$, so for $12r < 3 + \lambda$ we see that $(\eta_{ij}(s))_{i,j\geq 0}$ is the matrix of a continuous endomorphism $W(s)$ of $M_0[r]$. Moreover, arguments analogous to those of the previous section show that if furthermore $(\kappa, r) \in \mathcal{X}$ (so $M_\kappa[r]$ is defined), then the endomorphism of $M_\kappa[r]$ defined by sending ϕ to $h^{-s}W(s)(h^s\phi)$ equals the W operator as defined on q-expansions. Note that if $|s| \leq 4$ then $12r < 3 + \lambda$ implies $(\kappa, r) \in \mathcal{X}$.

5 Strategy of the proof.

We have proved in Corollary 3.7 that overconvergent modular forms f such that $Uf = \lambda f$ with $\lambda \neq 0$ overconverge "a long way". Using the W-operator introduced in the previous section we will now prove that overconvergent modular forms $f = q + \cdots$ such that $Uf = 0$ cannot overconverge as far. We introduce a definition and then record the precise statement.

Definition 5.1. *If $x \in \mathbb{C}_2$ then set $\beta = \beta(x) = \sup\{v(x - n) : n \in \mathbb{Z}_2\}$, allowing $\beta = +\infty$ if $x \in \mathbb{Z}_2$, and define $\nu = \nu(x)$ as follows: $\nu = \beta$ if $\beta \leq 0$, $\nu = \beta/2$ if $0 \leq \beta \leq 1$, and in general*

$$\nu = \sum_{k=1}^{n} 1/2^k + (\beta - n)/2^{n+1}$$

if $n \leq \beta \leq n + 1$. Finally define $\nu = 1$ if $\beta = +\infty$.

The meaning of the following purely elementary lemma will become apparent after the statement of Theorem 5.3.

Lemma 5.2. *Say $s \in \mathbb{C}_2$ with $|s| < 4$ and furthermore assume $2s \notin \mathbb{Z}_2^\times$. Then for all $s' \in \mathbb{C}_2$ with $|s - s'| \leq 1$, we have $0 < \frac{3+\nu(2s)}{12} < \frac{1}{2} + \frac{\mu(s')}{6}$.*

Proof. We have $\nu(2s) > -1$ and so certainly $\frac{3+\nu(s)}{12} > 0$. The other inequality can be verified on a case-by-case basis. We sketch the argument.

If $|s| > 2$ then $|s'| = |s| > 2$ and $\nu(2s) - 1 = v(s) = v(s') = \mu(s')$; the inequality now follows easily from the fact that $\mu(s') > -2$.

If $|s| \leq 2$ but $2s \notin \mathbb{Z}_2$ then $0 < \beta(2s) < \infty$ and $\nu(2s) < 1$; now $|s'| \leq 2$ and hence $\mu(s') \geq -1$, thus $\frac{3+\nu(2s)}{12} < \frac{1}{3} \leq \frac{1}{2} + \frac{\mu(s')}{6}$.

Finally if $2s \in \mathbb{Z}_2$ then we are assuming $2s \notin \mathbb{Z}_2^\times$ and hence $s \in \mathbb{Z}_2$ so $|s| \leq 1$ and hence $|s'| \leq 1$. Hence $\mu(s') = 0$ and we have $\frac{3+\nu(2s)}{12} = \frac{1}{3} < \frac{1}{2} + \frac{\mu(s')}{6}$. □

Again say $|s| < 4$ and $2s \notin \mathbb{Z}_2^\times$. Write $\kappa = \langle\cdot\rangle^{-12s}$, and $\nu = \nu(2s)$. Let $G = q + \cdots$ be an overconvergent form of weight κ (by which we mean an element of $M_\kappa[\rho]$ for some $\rho \in \mathbb{Q}_{>0}$ sufficiently small). The theorem we prove in the next section (which is really the main contribution of this paper) is

Theorem 5.3. *If $G = q + \cdots$ satisfies $UG = 0$, then $F := h^sG \in M_0[\rho]$ does not extend to an element of $M_0[r]$ for $r = \frac{3+\nu}{12}$. Equivalently, $G \notin M_\kappa[r]$.*

Note that by Lemma 5.2 we have $(\kappa, r) \in \mathcal{X}$ so the theorem makes sense. Furthermore, by Corollary 3.7, overconvergent eigenforms of the form $q + \cdots$ in the kernel of U overconverge less than finite slope overconvergent eigenforms. Note also that if $2s \in \mathbb{Z}_2^\times$ then $\nu(2s) = 1$ and for κ, r as above we have $(\kappa, r) \notin \mathcal{X}$. We deal with this minor annoyance in the last section of this paper.

6 The Kernel of U

In this section we prove Theorem 5.3. We divide the argument up into several cases depending on the value of s. We suppose that $|s| < 4$ and $2s \notin \mathbb{Z}_2^\times$, and we set $\kappa = \langle\cdot\rangle^{-12s}$. Define $\nu = \nu(2s)$ as in the previous section, and set $r = \frac{3+\nu}{12}$. For simplicity we drop the s notation from $\eta_{ij}(s)$ and write

$$\begin{aligned}\eta_{ij} &= \frac{3(j+2s)2^{(4-12r)(i-j)}(-1)^i}{(i-j)!}\prod_{t=1}^{i-j-1}(i+2j+t+6s)\\ &= \frac{3(j+2s)2^{(1-\nu)(i-j)}(-1)^i}{(i-j)!}\prod_{t=1}^{i-j-1}(i+2j+t+6s).\end{aligned}$$

Say $G = q + \cdots$ as in Theorem 5.3 is ρ-overconvergent for some $0 < \rho < r$, so $F = h^sG \in M_0[\rho]$. If we expand F as

$$F = \sum_{j\geq 1} \tilde{a}_j (2^{12\rho} f)^j$$

then it follows that $\tilde{a}_1 \neq 0$. Recall also that $\tilde{a}_j \to 0$ as $j \to \infty$. On the other hand, $F = -W(s)F$, and so

$$\tilde{a}_i = -\sum_{j=1}^{\infty} \tilde{a}_j \tilde{\eta}_{i,j},$$

where $\tilde{\eta}_{ij}$ denotes the matrix of $W(s)$ on $M_0[\rho]$ (so $\eta_{ij} = \tilde{\eta}_{ij}2^{12(r-\rho)(j-i)}$). We deduce from this that if we define $a_i = \tilde{a}_i 2^{12(\rho-r)i}$ then $F = \sum_{j\geq 1} a_j (2^{12r}f)^j$ and

$$a_i = -\sum_{j\geq 1} a_j \eta_{ij}.$$

Note in particular that the sum converges even if $W(s)$ does not extend to a continuous endomorphism of $M_0[r]$ or if F does not extend to an element of $M_0[r]$. In fact our goal is to show that the a_i do not tend to zero, and in particular that F does not extend to an element of $M_0[r]$.

Lemma 6.1. *Suppose F is as above. Suppose also that there exist constants c_1 and $c_3 \in \mathbb{R}$, an infinite set I of positive integers, and for each $i \in I$ constants $N(i)$ and $c_2(i)$ tending to infinity as $i \to \infty$ and such that*

(i) $v(\eta_{i1}) \leq c_1$, *for all* $i \in I$.

(ii) $v(\eta_{ij}) \geq c_2(i)$ *for all* $i \in I$ *and* $2 \leq j \leq N(i)$.

(iii) $v(\eta_{ij}) \geq c_3$ *for all* $i \in I$ *and* $j \in \mathbb{Z}_{\geq 0}$.

Then the a_i do not tend to zero as $i \to \infty$, and hence F does not extend to a function on $M_0[r]$.

Proof. Assume $a_i \to 0$. Recall that we assume $a_1 \neq 0$. By throwing away the first few terms of I if necessary, we may then assume that for all $i \in I$ we have

(1) $c_2(i) > v(a_1) + c_1 - \min\{v(a_j) : j \geq 1\}$, and

(2) $\min\{v(a_j) : j > N(i)\} > v(a_1) + c_1 - c_3$.

We now claim that for all $i \in I$ we have $v(a_1\eta_{i1}) < v(a_j\eta_{ij})$ for all $j > 1$. The reason is that if $j \leq N(i)$ the inequality follows from equation (1) above, and if $j > N(i)$ it follows from (2). Now from the equality

$$a_i = -\sum_{j=1}^{\infty} a_j\eta_{ij}$$

we deduce that $v(a_i) = v(a_1\eta_{i1})$ is bounded for all $i \in I$, contradicting the fact that $a_i \to 0$. □

The rest of this section is devoted to establishing these inequalities for suitable I and r. We start with some preliminary lemmas.

Lemma 6.2. *1. If $m \geq 1$ then $v(m!) \leq m - 1$, with equality if and only if m is a power of 2.*

2. If $m \geq 0$ then $v(m!) \geq (m-1)/2$, with equality if and only if $m = 1, 3$.

3. If $n \geq 0$ and $0 \leq m < 2^n$ then setting $t = 2^n - m$ we have $m - v(m!) \geq n - (t/2)$.

Proof. 1 and 2 follow easily from

$$v(m!) = \lfloor m/2 \rfloor + \lfloor m/4 \rfloor + \lfloor m/8 \rfloor + \ldots.$$

For 3, we have $m!(m+1)(m+2)\ldots(2^n-1)(2^n) = (2^n)!$ and for $0 < d < 2^n$ we have $v(d) = v(2^n - d)$, so $v((m+1)(m+2)\ldots(2^n-1)) = v((t-1)!) \geq (t-2)/2$ by 2. Finally $v((2^n)!) = 2^n - 1$ by 1. Hence $v(m!) \leq 2^n - 1 - n - (t-2)/2 = 2^n - n - (t/2)$ and so $m - v(m!) \geq 2^n - t - (2^n - n - (t/2)) = n - (t/2)$. □

Lemma 6.3. *Let $m \in \mathbb{Z}$ be arbitrary and set $\beta = \beta(x)$ and $\nu = \nu(x)$ as in Definition 5.1.*

1. *If $\beta \leq 0$ then $v(x+n) = \nu$ for all $n \in \mathbb{Z}$, hence the valuation of $\prod_{t=1}^{N}(x+m+t)$ is $N\nu$.*
2. *If $0 < \beta < \infty$ and if N is a power of 2 with $N \geq 2^{\lceil\beta\rceil}$ then the valuation of*
$$\prod_{t=1}^{N}(x+m+t)$$
is exactly $N\nu$.
3. *If $0 < \beta < \infty$ and if $N \geq 0$ is an arbitrary integer then the valuation of*
$$\prod_{t=1}^{N}(x+m+t)$$
is v, where $|v - N\nu| < \beta$.
4. *If $\beta = \infty$ and if $N \geq 0$ is an arbitrary integer then the valuation of $\prod_{t=1}^{N}(x+m+t)$ is at least $v(N!)$.*

Proof. (1) is obvious and (2) is easy to check (note that $v(x+n)$ is periodic with period $2^{\lceil\beta\rceil}$). For part (3), say $n = \lfloor\beta\rfloor$. Now about half of the terms in this product are divisible by 2, about a quarter are divisible by 4, and so on. More precisely, this means that the largest possible power of 2 that can divide this product is

$$\begin{aligned}&\lceil N/2\rceil + \lceil N/4\rceil + \ldots + \lceil N/2^n\rceil + (\beta - n)\lceil N/2^{n+1}\rceil\\ <&(N/2+1) + (N/4+1) + \ldots + (N/2^n+1) + (\beta-n)(N/2^{n+1}+1)\\ =&N\nu + \beta.\end{aligned}$$

A similar argument shows that the lowest possible power of 2 dividing this product is strictly greater than $N\nu - \beta$.
For part (4), if $\beta = \infty$ then $x \in \mathbb{Z}_2$ and by a continuity argument it suffices to prove the result for x a large positive integer, where it is immediate because the binomial coefficient $\binom{x+m+N}{N}$ is an integer.

□

Now set $x = 2s$ and let $\beta = \beta(2s), \nu = \nu(2s)$. Note that if $\beta \leq 0$ then $\mu = \beta - 1$, and if $\beta \geq 1$ then $\mu = 0$.
Recall $\eta_{ij} = 0$ if $i < j$, $\eta_{ii} = (-1)^i$, and if $i > j$ we have

$$\eta_{ij} = \frac{3(j+2s)2^{(1-\nu)(i-j)}(-1)^i}{(i-j)!}\prod_{t=1}^{i-j-1}(i+2j+t+6s).$$

In particular, for $i > j$ we have

$$(*) \quad v(\eta_{i,j}) = (1-\nu)(i-j) - v((i-j)!) + v(j+2s) + v\left(\prod_{t=1}^{i-j-1}(i+2j+t+6s)\right).$$

We shall continually refer to $(*)$ in what follows.

Proposition 6.4. *Say $\beta \leq 0$ (and hence $\nu = \beta$).*

1. *If $j \geq i$ then $v(\eta_{ij}) \geq 0$, and if $j < i$ then $v(\eta_{ij}) = i - j - v((i-j)!) \geq 1$.*
2. *If $i = 2^n + 1$ then $v(\eta_{i1}) = 1$ and if $1 < j < i$ then $v(\eta_{ij}) \geq n - (j-1)/2$.*

Proof. 1 is immediate from $(*)$ and Lemma 6.3(1). Now 2 can be deduced from 1, using part 1 of Lemma 6.2 for the first part and part 3 of Lemma 6.2 for the second. □

We now prove:

Lemma 6.5. *Theorem 5.3 is true if $-1 < \beta \leq 0$ (i.e., if $2 \leq |s| < 4$).*

Equivalently, if $2 \leq |s| < 4$ and $\kappa = \langle\cdot\rangle^{-12s}$, and if $G = q + \ldots$ is a non-zero weight κ overconvergent form in $\ker(U)$, then $F = h^s G$ does not converge as far as $M_0[1/4 + \nu/12]$, where $\nu = \nu(2s)$ as above.

Proof. This will be a direct application of lemma 6.1. We set $I = \{2^n + 1 : n \in \mathbb{Z}_{>0}\}$, and if $i = 2^n + 1$ we define $c_2(i) = (n+1)/2$ and $N(i) = n$. We set $c_1 = 1$ and $c_3 = 0$. Now assumptions (i) and (ii) of Lemma 6.1 follow from Proposition 6.4(2), and (iii) follows from Proposition 6.4(1). □

Let us now consider the case when $0 < \beta < \infty$.

Proposition 6.6. *Let $0 < \beta < \infty$.*

1. *If $j < i$ then $v(\eta_{i,j}) - \big((i-j) - v((i-j)!) - \nu\big) \in [-\beta, 2\beta]$.*
2. *If $j < i$ then*
$$v(\eta_{ij}) \geq 1 - \beta - \nu.$$
If $i = 2^n + 1$ then
$$v(\eta_{i1}) \leq 2\beta - \nu + 1$$
and if $1 < j < i$ then
$$v(\eta_{ij}) \geq n - (j+1)/2 - \nu - \beta.$$

Proof. From the definition of β, the valuation of $j + 2s$ lies in $[0, \beta]$. The result then follows from $(*)$ and lemma 6.3, part 3. Part 2 follows from part 1 and Lemma 6.2, parts (1) and (3), applied to $(i-j)!$. □

Lemma 6.7. *Theorem 5.3 is true if* $0 < \beta < \infty$*, that is, if* $|s| \leq 2$ *and* $2s \notin \mathbb{Z}_2$*.*

Proof. Again this is an application of lemma 6.1. Set $I = \{2^n + 1 : n \in \mathbb{Z}_{>0}\}$, $c_1 = 2\beta - \nu + 1$, $c_3 = \min\{0, 1 - \beta - \nu\}$, and if $i = 2^n + 1$ then set $N(i) = n$ and $c_2(i) = (n+1)/2 - \nu - \beta$. Conditions (i)–(iii) of Lemma 6.1 hold by Proposition 6.6(2). □

The only cases of Theorem 5.3 left to deal with are those with $\beta = +\infty$, that is, $2s \in \mathbb{Z}_2$. Because the theorem does not deal with the case $2s \in \mathbb{Z}_2^\times$ we may assume from now on that $2s \in 2\mathbb{Z}_2$, so $s \in \mathbb{Z}_2$. We next deal with the case $s \in \mathbb{Z}_2$ and $6s \notin \mathbb{N}$, where $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the positive integers. In this case, we shall again use Lemma 6.1 with i of the form $i = 2^n + 1$. However, it will turn out that only certain (although infinitely many) n will be suitable.
Since we assume $s \in \mathbb{Z}_2$ we have $\beta = +\infty$, so $\nu = 1$ and hence

$$(**) \quad \eta_{ij} = \frac{3(j+2s)(-1)^i}{(i-j)!} \prod_{t=1}^{i-j-1} (i + 2j + t + 6s).$$

Let $u \in \mathbb{Z}_2$. Define functions $f_n(u)$ as follows:

$$f_n(u) = (2^n + u)(2^n + u + 1) \cdots (2^{n+1} - 1 + u) = \prod_{\tau=0}^{2^n - 1} (2^n + u + \tau).$$

Lemma 6.8. *For any* $u \in \mathbb{Z}_2$ *there exist infinitely many values of* n *for which*

$$v_n(f(u)) = v((2^n)!) \text{ or } v((2^n)!) + 1.$$

Proof. For each n, define an integer $0 < u_n \leq 2^n$ by setting $u \equiv u_n \mod 2^n$. If $0 \leq \tau \leq 2^n - 1$ and $\tau \neq 2^n - u_n$, then

$$v(2^n + u + \tau) = v(u_n + \tau).$$

Since τ takes on every equivalence class modulo 2^n, It follows from the definition of f_n that

$$v(f_n(u)) = v((2^n - 1)!) + v(2^{n+1} + u - u_n).$$

If $u \not\equiv u_n \mod 2^{n+1}$ then $v(2^{n+1} + u - u_n) = v(2^n)$ and $v(f_n(u)) = v((2^n)!)$. There are infinitely many n satisfying this condition unless $u \equiv u_n \mod 2^{n+1}$ for all sufficiently large n. Yet this implies $u_n = u_{n+1}$ for all sufficiently large n, and subsequently that $u = u_n$. In this case we have $v(2^{n+1} + u - u_n) = v(2^{n+1})$, and $v(f_n(u)) = v((2^n)!) + 1$. □

Corollary 6.9. *There are infinitely many* n *such that if* $i = 2^n + 1$ *then* $v(\eta_{i1}) \in \{0, 1\}$*.*

Proof. Let $i = 2^n + 1$ and $j = 1$, and assume $n \geq 1$. By $(**)$ we have

$$\eta_{i1} = \frac{3(1+2s)(-1)}{(2^n)!} \prod_{t=1}^{2^n-1} (2^n + 3 + t + 6s).$$

Let $u = 6s + 4 \in 2\mathbb{Z}_2$ and set $\tau = t - 1$. Then

$$\eta_{i1} = \frac{(1-u)}{(2^n)!} \prod_{\tau=0}^{2^n-2} (2^n + u + \tau) = \frac{f_n(u)}{(2^n)!} \cdot \frac{1-u}{u - 1 + 2^{n+1}}$$

and the result follows from Lemma 6.8 and the fact that $u \in 2\mathbb{Z}_2$. □

Let us now turn to estimating η_{ij} for general i, j.

Lemma 6.10. *If $i, j \in \mathbb{Z}_{\geq 0}$ then $v(\eta_{ij}) \geq 0$.*

Proof. By continuity, it suffices to verify the result for $6s$ a large positive even integer. It is clear if $i \leq j$ so assume $i > j$. Now because the product of N successive integers is divisible by $N!$ we see (putting one extra term into the product) that both $x_1 := \frac{i+2j+6s}{3(j+2s)}\eta_{ij}$ and $x_2 := \frac{2i+j+6s}{3(j+2s)}\eta_{ij}$ are integers. The result now follows as $\eta_{ij} = 2x_1 - x_2$. □

Set $I_0 = \{i = 2^n + 1 : v(\eta_{i1}) \in \{0, 1\}\}$. Then I_0 is infinite by Corollary 6.9. We will ultimately let I be a subset of I_0. We must analyze η_{ij} for $i \in I_0$ and $1 < j$ small. Note that if $i = 2^n + 1$ and $j \geq 2$, then

$$\frac{\eta_{i,j}}{\eta_{i,1}} = 2^n \cdot \frac{(j+2s)}{(1+2s)} \cdot \prod_{t=1}^{j-2}(i - j + t) \cdot \frac{\prod_{t=1}^{j-1}(2i + t + 6s)}{\prod_{t=1}^{2j-2}(i + 2 + t + 6s)}$$

Since $6s \notin -\mathbb{N}$, $3 + 6s + t \neq 0$. Thus for any N there exists n_0 depending on N such that for all $n \geq n_0$ we have $v(i + 2 + 6s + t) = v(3 + 6s + t)$ for all $t \leq 2N - 2$. In particular, for fixed N and sufficiently large n (with $i = 2^n + 1$),

$$v(\eta_{ij}) \geq n - v\left(\prod_{t=0}^{2j-2}(3 + 6s + t)\right) + v(\eta_{i1}).$$

Lemma 6.11. *For any constants $c_2 \in \mathbb{R}$ and $N \in \mathbb{Z}_{\geq 1}$, there exists $n_1 = n_1(c_2, N)$ such that for all $n \geq n_1$ such that $i = 2^n + 1 \in I_0$, we have $v(\eta_{ij}) \geq c_2$ for $2 \leq j \leq N$.*

Proof. Set $M = v(\prod_{t=0}^{2N-2}(3+6s+t))$ and choose n_1 such that $n_1 - M \geq c_2$. □

We may now prove:

Lemma 6.12. *Theorem 5.3 is true if $s \in \mathbb{Z}_2$ and $6s \notin -\mathbb{N}$.*

Proof. We apply lemma 6.1 as follows. Set $c_1 = 1$ and $c_3 = 0$. We build I as follows. As m runs through the positive integers, set $N = c_2 = m$, define n_1 as in Lemma 6.11, choose $n \geq n_1$ such that $i := 2^n + 1 \in I_0$ and such that i is not yet in I; now add i to I and define $N(i) = c_2(i) = t$. The conditions of lemma 6.1 are then satisfied. □

The final case in our proof of Theorem 5.3 is the case $6s \in -2\mathbb{N}$, which corresponds to weight $k = -12s \in 4\mathbb{N}$. We shall not use Lemma 6.1 in this case, but give a direct argument.

Because our level structure is so small it is convenient to temporarily augment it to get around representability issues. Choose some auxiliary odd integer N and consider the compact modular curve Y over $\mathbb{Q}_2$ whose cuspidal points parameterize elliptic curves with a subgroup of order 2 and a full level N structure (note that this curve is not in general connected). There is a sheaf ω on Y, and classical modular forms of weight k and level 2 are, by definition, $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-invariant global sections of $\omega^{\otimes k}$ on Y.

For $0 < r \leq 2/3$ let $Y[r]$ denote the pre-image of $X[r]$ via the forgetful functor. Recall that there is a compact operator U on $H^0(Y[r], \omega^{\otimes k})$ for $r < 2/3$ and $k \in \mathbb{Z}$.

Lemma 6.13. *If $k \in \mathbb{Z}$ and $f \in H^0(Y[1/3], \omega^{\otimes k})$ is in the kernel of U, then $f = 0$.*

Remark 6.14. *The lemma is not special to $p = 2$; the proof shows that non-zero p-adic modular forms in the kernel of U are never $1/(p+1)$-overconvergent.*

Proof. Say $f \in H^0(Y[1/3], \omega^{\otimes k})$ is arbitrary. If E is an elliptic curve over a finite extension of $\mathbb{Q}_2$, equipped with with a subgroup C of order 2 and a full level N structure L, and such that the corresponding point $(E, C, L) \in Y$ is in $Y[1/3]$, then one can regard $f(E, C, L)$ as an element of $H^0(E, \Omega^1)^{\otimes k}$. Now define $g \in H^0(Y[2/3], \omega^{\otimes k})$ by

$$g(E, L) = \sum_{D \neq C} (\mathrm{pr})^* f(E/D, \overline{C}, \overline{L}),$$

where the sum is over the subgroups $D \neq C$ of E of order 2, pr denotes the projection $E \to E/D$, and a bar over a level structure denotes its natural push-forward. An easy calculation using Tate curves (see for example Proposition 5.1 of [1]) shows that $g = 2Uf$, and hence if $Uf = 0$ then $g = 0$. In particular if E is an elliptic curve with no canonical subgroup and we fix a full level N structure L on E, then then $(E, C, L) \in Y[2/3]$ for all C, and $g(E, C, L) = 0$ for all C implies that $\sum_{D \neq C} (\mathrm{pr})^* f(E/D, E[2]/D, \overline{L}) = 0$ for all C. Summing, one deduces that $\sum_D (\mathrm{pr})^* f(E/D, E[2]/D, \overline{L}) = 0$ and hence that $f(E/D, E[2]/D, \overline{L}) = 0$ for all D of order 2. This implies that f is identically zero on the "boundary" of $Y[1/3]$ and hence that f is identically zero. □

We deduce

Lemma 6.15. *Theorem 5.3 is true for* $6s \in -2\mathbb{N}$.

Proof. If $G \in M_k[1/3]$ then $G = h^{k/12}F$ and, because $k = -12s \in 4\mathbb{N}$, we know that $h^{k/12}$ is a classical modular form of level 2 and hence an element of $H^0(Y[1/3], \omega^{\otimes(k/12)})$. Thus the preceding lemma applies to G and we conclude that $G = 0$. □

Theorem 5.3 now follows from Lemmas 6.5, 6.7, 6.12 and 6.15.

7 There are not too many holes in the eigencurve.

We begin with a simple rigid-analytic lemma that forms the basis to our approach. Let X be a connected affinoid variety, and let V be a non-empty admissible open affinoid subdomain of X. Let $B = \mathrm{Sp}(\mathbb{C}_2\langle T\rangle)$ denote the closed unit disc, and let $A = \mathrm{Sp}(\mathbb{C}_2\langle T, T^{-1}\rangle)$ denote its "boundary", the closed annulus with inner and outer radii both 1.

Lemma 7.1. *If f is a function on $V \times B$ and the restriction of f to $V \times A$ extends to a function on $X \times A$, then f extends to a function on $X \times B$.*

Proof. We have an inclusion $\mathcal{O}(X) \subseteq \mathcal{O}(V)$, as X is connected, and we know $f \in \mathcal{O}(V)\langle T\rangle$ and $f \in \mathcal{O}(X)\langle T, T^{-1}\rangle$. But the intersection of these two rings is $\mathcal{O}(V)\langle T\rangle$. □

Let $\mathcal{E}$ denote the 2-adic eigencurve of tame level 1, and let $\mathcal{W}$ denote 2-adic weight space. We recall that because 2 is a regular prime, $\mathcal{E}$ is a disjoint union $\mathcal{E}^{\mathrm{Eis}} \coprod \mathcal{E}^{\mathrm{cusp}}$, and the natural map from the Eisenstein component $\mathcal{E}^{\mathrm{Eis}}$ to weight space is an isomorphism. One can also check from the definition of the eigencurve in [2] that the cuspidal component $\mathcal{E}^{\mathrm{cusp}}$ of E represents the functor on rigid spaces over $\mathcal{W}$ sending a rigid space $Y \to \mathcal{W}$ to the set of normalized overconvergent finite slope cuspidal eigenforms of "weight Y", that is, formal power series $\sum a_n q^n \in \mathcal{O}(Y)[[q]]$ with $a_1 = 1$ and a_2 a unit, which are eigenforms for all the Hecke operators and, when divided by the pullback of the Eisenstein family to Y, become overconvergent functions on $Y \times X[0]$. Let B denote the closed unit disc and let $B^\times$ denote B with the origin removed. Suppose we have a map $\phi : B^\times \to \mathcal{E}$ such that the induced map $B^\times \to \mathcal{W}$ extends (necessarily uniquely) to a map $B \to \mathcal{W}$. Let $\kappa_0 \in \mathcal{W}(\mathbb{C}_2)$ denote the image $0 \in B(\mathbb{C}_2)$ under this map. The theorem we prove in this section is

Theorem 7.2. *If $\kappa_0 \notin \{\langle\cdot\rangle^{-12s} : 2s \in \mathbb{Z}_2^\times\}$ then the map $\phi : B^\times \to \mathcal{E}$ extends to a map $B \to \mathcal{E}$.*

Proof. If the image of ϕ is contained in $\mathcal{E}^{\mathrm{Eis}}$ then the theorem is automatic, because the projection $\mathcal{E}^{\mathrm{Eis}} \to \mathcal{W}$ is an isomorphism. Hence we may assume that $\phi : B^\times \to \mathcal{E}^{\mathrm{cusp}}$. If $|\kappa_0(5) - 1| > 1/8$ then we are finished by the main theorem of [4]. Assume from now on that $|\kappa_0(5) - 1| \le 1/8$. Then the map ϕ corresponds to a family $\sum a_n q^n$ of overconvergent eigenforms over $B^\times$. Furthermore, the supremum norm of each a_n is at most 1 (because Hecke operators on overconvergent p-adic modular forms have eigenvalues with norm at most 1) and, analogous to the analysis of isolated singularities of holomorphic functions, one checks easily that this is enough to ensure that each a_n extends to a function on B. Our task is to analyze the "limiting" power series $\sum a_n(0)q^n$.

More precisely, we now have a formal power series $\sum_{n\geq 1} a_nq^n$ in $\mathcal{O}(B)[[q]]$. To prove the theorem we must check that this formal power series is a finite slope overconvergent form of weight B. We are assuming $|\kappa_0(5)-1|\leq 1/8$ and hence $\kappa_0=\langle\cdot\rangle^{-12s}$ with $|s|<4$. Now assume also that $2s\notin\mathbb{Z}_2^\times$. Set $r=\frac{3+\nu(2s)}{12}$. After shrinking B if necessary, we may assume that for all $b\in B$ we have $\kappa_b=\langle\cdot\rangle^{-12s'}$ with $|s-s'|\leq 1$. By Lemma 5.2 we have $(\kappa_b,r)\in\mathcal{X}$ for all $b\in B$, and by Corollary 3.8 we see that on the boundary of B our function $\sum a_nq^n$ is r-overconvergent, it being a finite slope eigenform for U here. Moreover, the coefficients a_n are all bounded by 1 on all of B. Now applying Lemma 7.1 with $X=X[r]$ and V a small disc near infinity such such that q (the q-expansion parameter) is a well-defined function on V, we deduce that $\sum a_nq^n$ is r-overconvergent on all of B.

All that we need to show now is that $a_2\in\mathcal{O}(B)^\times$. It suffices to prove that $a_2(0)\neq 0$, as we know that $a_2(b)\neq 0$ for all $0\neq b\in B$. But $\sum a_n(0)q^n=q+\ldots$ is an r-overconvergent form of weight κ_0, so by Theorem 5.3 (note that this is where all the work is) we deduce $a_2(0)\neq 0$. Hence $a_2\in\mathcal{O}(B)^\times$ and $\sum a_nq^n$ is an overconvergent cuspidal finite slope eigenform of weight B, which induces the map $B\to\mathcal{E}^{\mathrm{cusp}}$ which we seek. □

8 There are no holes in the eigencurve

In the previous section we showed that if there are any holes in the eigencurve, then they lie above weights of the form $\{\langle\cdot\rangle^{-12s}:2s\in\mathbb{Z}_2^\times\}$. To show that in fact there are no holes in the eigencurve, we redo our entire argument with a second, even more non-standard, twist and show that using this twist we may deduce that the only holes in the eigencurve lie above the set $\{\langle\cdot\rangle^{2-12s}:2s\in\mathbb{Z}_2^\times\}$. Because there is no $s\in\frac{1}{2}\mathbb{Z}_2^\times$ such that $\frac{12s-2}{12}\in\frac{1}{2}\mathbb{Z}_2^\times$ this finishes the argument. We sketch the details.

Let $E_2=1+24q+24q^2+96q^3+\ldots$ denote the holomorphic Eisenstein series of weight 2 and level $\Gamma_0(2)$. We define $\mathcal{X}'=\{(\kappa\langle\cdot\rangle^2,r):(\kappa,r)\in\mathcal{X}\}$. If $|s|<8$ then set $\kappa'=\langle\cdot\rangle^{2-12s}$. If r is such that $(\kappa',r)\in\mathcal{X}'$, we define $M'_{\kappa'}[r]$ to be the vector space of formal q-expansions $F\in\mathbb{C}_2[[q]]$ such that Fh^s/E_2 is the q-expansion of an element of $M_0[r]$. For $r>0$ sufficiently small this definition is easily checked to coincide with the usual definition. We shall be using this definition with r quite large and again we neglect to verify whether the two definitions coincide in the generality in which we use them. We give $M'_{\kappa'}[r]$ the Banach space structure such that multiplication by h^s/E_2 is an isometric isomorphism $M'_{\kappa'}[r]\to M_0[r]$, and endow $M'_{\kappa'}[r]$ once and for all with the orthonormal basis $\{E_2h^{-s},E_2h^{-s}(2^{12r}f),E_2h^{-s}(2^{12r}f)^2,\ldots\}$. Note that the reason that this definition gives us more than our original definition of $M_\kappa[r]$ is that if k is an even integer with $2||k$ then $(k, 1/3) \notin \mathcal{X}$ but $(k, 1/2-\epsilon) \in \mathcal{X}'$, so we can "overconverge further" for such weights.

If $\theta = q(d/dq)$ is the operator on formal q-expansions, then one checks that $U\theta = 2\theta U$. Moreover, it is well-known that $\theta f = fE_2$ and hence $\theta f^j = jf^jE_2$ for any $j \geq 0$. Hence our formulae for the coefficients of U acting on $M_0[r]$ will give rise to formulae for the coefficients of U acting on $M_2'[r]$, which was the starting point for the arguments in section 3. We give some of the details of how the arguments should be modified. If $m \in \mathbb{Z}_{\geq 0}$ and $k' = 2 - 12m$ then we define a continuous operator $U_{k'}'$ on $M_0[r]$ by $U_{k'}'(\phi) = E_2^{-1}h^mU(E_2h^{-m}\phi)$. One checks that this is indeed a continuous operator by verifying that it has a basis $(u_{ij}'(m))_{i,j\geq 0}$ defined by $u_{ij}'(m) = 0$ for $2i < j$ or $2j - i + 3m < 0$, $u_{00}'(0) = 1$, and

$$u_{ij}'(m) = \frac{3(i+j+3m-1)!(i+m)2^{8i-4j+12r(j-i)}}{(2i-j)!(2j-i+3m)!}$$

otherwise. One checks that for i, j fixed there is a polynomial $u_{ij}'(S)$ interpolating $u_{ij}'(m)$ and that for $|s| < 8$ with $\mu = \min\{v(s), 0\}$ we have $v(u_{ij}'(s)) \geq (\mu + 3 - 6r)(2i - j) + 6rj$ as before. Hence for $|s| < 8$, $\kappa' = \langle\cdot\rangle^{2-12s}$ and $r \in \mathbb{Q}$ such that $(\kappa', r) \in \mathcal{X}'$, the matrix $(u_{ij}'(s))_{i,j\geq 0}$ defines a compact operator $U'(s)$ on $M_0[r]$. Furthermore we have $U'(s)(\phi) = E_2^{-1}h^sU(E_2h^{-s}\phi)$, and in particular $U : M_{\kappa'}'[r] \to M_{\kappa'}'[r]$ is well-defined and compact. Moreover, $U'(s)$ increases overconvergence and any eigenvector for $U'(s)$ on $M_0[r]$ with non-zero eigenvalue extends to $M_0[r']$ for any r' such that $0 < r' < 1/2 + \mu(s)/6$. Finally, these arguments also work for families of modular forms and the analogue of Corollary 3.8 remains true in this setting.

Similar arguments work in section 4. One checks that $2V\theta = \theta V$ and hence $VU\theta = 2V\theta U = \theta VU$. Hence θ commutes with W and one now deduces from our explicit formulae for W in weight $-12m$ that in weight $2-12m$ the matrix for W is given by $W_k = [\eta_{ij}']$, where:

$$\eta_{ij}' = \frac{(2i+j-1+6m)!3(i+2m)\cdot 2^{(4-12r)(i-j)}(-1)^i}{(i-j)!(i+2j+6m)!}.$$

We remark that the only difference in this formula is that $(j+2m)$ has been replaced by $(i+2m)$. One finds that the arguments at the end of this section apply *mutatis mutandis* in this case.

The analogue of Theorem 5.3 is that if $|s| < 4$ and $2s \notin \mathbb{Z}_2^\times$ and $\kappa' = \langle\cdot\rangle^{2-12s}$ then an overconvergent infinite slope form of weight κ' is not r-overconvergent, for $r = \frac{3+\nu(2s)}{12}$. The proof follows the same strategy, although some of the lemmas in section 6 need minor modifications; for example in Lemma 6.10 we set $x_1 = \frac{i+2j+6s}{3(i+2s)}\eta_{ij}'$ and $x_2 := \frac{2i+j+6s}{3(i+2s)}\eta_{ij}'$, and the result follows as $\eta_{ij}' = 2x_2 - x_1$. Note that E_2 can be regarded as an element of $H^0(Y[1/3], \omega^{\otimes 2})$ so that Lemma 6.13 does not need modification.

We deduce our main theorem:

Theorem 8.1. *If $\phi : B^\times \to \mathcal{E}$ and the induced map $B^\times \to \mathcal{W}$ extends to a map $\psi : B \to \mathcal{W}$, then ϕ extends to a map $B \to \mathcal{E}$.*

Proof. If $\psi(0) \notin \{\langle\cdot\rangle^{-12s} : 2s \in \mathbb{Z}_2^\times\}$ then we use Theorem 7.2, and if it is then we use the modification explained above. □

References

[1] K. Buzzard, *Analytic continuation of overconvergent eigenforms*, Journal of the American Math. Society 16 (2003), 29–55.

[2] K. Buzzard, *Eigenvarieties*, to appear in the proceedings of the 2004 LMS Durham conference on L-functions and arithmetic.

[3] K. Buzzard, F. Calegari, *Slopes of overconvergent* 2*-adic modular forms*, Compositio Math. 141 (2005), 591–604.

[4] K. Buzzard, L. Kilford. *The 2-adic eigencurve at the boundary of weight space*, Compositio Math. 141 (2005), 605–619.

[5] R. Coleman, *p-adic Banach spaces and families of modular forms* Invent. math. 127, 417–479 (1997).

[6] R. Coleman, F. Gouvêa, N. Jochnowitz. *E_2, Θ, and overconvergence*, Internat. Math. Res. Notices 1995, no. 1, 23–41

[7] R. Coleman, B. Mazur, *The eigencurve*, Galois representations in algebraic geometry, (Durham, 1996), 1–113, London Math Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[8] M. Emerton, *The Eisenstein ideal in Hida's ordinary Hecke algebra*, IMRN 1999, No. 15.

[9] N. Katz, *p-adic properties of modular schemes and modular forms.*, in "Modular functions of one variable, III" (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 69–190. Lecture Notes in Mathematics, Vol. 350, Springer, Berlin, 1973.

[10] Jean-Pierre Serre. Endomorphismes complètement continus des espaces de Banach p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (12):69–85, 1962.

Kevin Buzzard
Department of Mathematics
Imperial College
180 Queen's Gate
London SW7 2AZ, UK
buzzard@imperial.ac.uk

Frank Calegari
Department of Mathematics
Harvard University
1 Oxford Street, Cambridge
MA 02138, USA
fcale@math.harvard.edu

Equidistribution Adélique des Tores et Équidistribution des Points CM

Pour John Coates, à l'occasion de son soixantième anniversaire.

L. Clozel, E. Ullmo

Received: January 4, 2006
Revised: April 28. 2006

Abstract. This paper discusses the relations between a conjecture, proposed by the authors, concerning the equidistribution of homogeneous subvarieties in arithmetic quotients; and the André–Oort conjecture.

1 Introduction

Dans un article récent [3] nous avons étudié la question suivante. Soient G un groupe algébrique connexe sur $\mathbb{Q}$, $G(\mathbb{R})^+$ la composante neutre de $G(\mathbb{R})$ et $\Gamma \subset G(\mathbb{R})^+$ un sous-groupe de congruence. Soit par ailleurs $H_\alpha \subset G$ $(\alpha \geqslant 1)$ une suite de sous-groupes connexes définis sur $\mathbb{Q}$. On suppose la suite stricte :

(1.1) Pour tout sous-groupe $H \subsetneq G$ (connexe, défini sur $\mathbb{Q}$), $H_\alpha \not\subset H$ pour α assez grand.

Si $\Gamma_\alpha = \Gamma \cap H_\alpha(\mathbb{R})^+$, on obtient alors naturellement une suite de mesures de probabilité μ_α sur $S(G,\Gamma) = \Gamma\backslash G(\mathbb{R})^+$. (On suppose G, H_α "de type $\mathcal{F}$" [3] de sorte que les mesures invariantes sont finies). On se demande si, pour $\alpha \to \infty$, μ_α tend vers la mesure de probabilité naturelle μ_G sur $S(G,\Gamma) = \Gamma\backslash G(\mathbb{R})^+$. Dans certains cas il n'en est rien [3, § 2.3]. Nous avons donc donné une reformulation adélique de la conjecture [3]. Soit $K \subset G(\mathbb{A}_f)$ le sous-groupe compact ouvert définissant Γ, de sorte que $S(G,\Gamma) = S(G,K)^+$ où

$$S(G,K) = G(\mathbb{Q})\backslash G(\mathbb{A})/K\ .$$

Pour $H \subset G$, soit $S^+(H, K_H)$ la réunion des composantes connexes de $S(H, K_H) = H(\mathbb{Q})\backslash H(\mathbb{A})/K_H \subset S(G,K)$ contenues dans $S(G,K)^+$. Elle est munie d'une mesure de probabilité naturelle (H de type $\mathcal{F}$); notons-la $\mu_{a,\alpha}$ si $H = H_\alpha$. Alors la conjecture est

(1.2) $(\mathcal{E}_a)$ - La suite de mesures $\mu_{a,\alpha}$ tend vers μ_G (pour la convergence faible) si $\alpha \to +\infty$.

Nous ne connaissons pas de contre-exemple à $(\mathcal{E}_a)$. Noter que cette conjecture se formule naturellement de façon adélique : par exemple, si G est simple et simplement connexe (et $G(\mathbb{R})$ non compact) $(\mathcal{E}_a)$ est équivalente à la conjecture analogue pour les sous-espaces

$$H_\alpha(\mathbb{Q})\backslash H_\alpha(\mathbb{A}) \subset G(\mathbb{Q})\backslash G(\mathbb{A}).$$

Dans [3], $(\mathcal{E}_a)$ est démontrée dans de nombreux cas, essentiellement quand la théorie de Ratner s'applique, i.e., quand les groupes H_a "contiennent assez d'unipotents" (mais voir a contrario [3, Théorème 3.3] où l'on démontre $\mathcal{E}$ mais non $(\mathcal{E}_a)$). Le cas pur et inaccessible à ces méthodes est celui où G est semi-simple et où les H_α sont des tores; dans [3, § 5-7] on vérifie qu'il est lié à des questions profondes de théorie analytique des nombres.

La théorie de Ratner a par ailleurs été appliquée dans [2] à des questions issues de la conjecture d'André-Oort. On y démontre l'équidistribution de familles de sous-variétés modulaires de dimension positive d'une variété de Shimura, associées à des sous-groupes semi-simples du groupe ambiant. Au contraire, il est bien connu [3, 16] que l'équidistribution des familles de points CM est lié au problème d'équidistribution des orbites toriques.

Le but de cet article est d'éclaircir cette dernière relation, dans le cadre de la conjecture d'André-Oort. Notons maintenant S une variété de Shimura, associée à un groupe réductif $G/\mathbb{Q}$ est aux données usuelles (§ 2), et soit $z_\alpha \in S$ une suite de points CM. Ainsi tout point z_α est associé à un tore $T_\alpha \subset G$, son groupe de Mumford-Tate. La variété S est définie sur un corps de nombres E (le corps reflex); z_α est défini sur la clôture algébrique $\bar{E}$ de E et son orbite sous $\mathfrak{g}_E = \mathrm{Gal}(\bar{E}/E)$ est décrite par Shimura et Deligne, et liée à l'action de $T_\alpha(\mathbb{A}_f)$ sur S, $\mathbb{A}_f$ désignant l'anneau des adèles finis.

Plus précisément, soit $E_\alpha = E(z_\alpha)$ le corps reflex de z_α (c'est le corps $E(T_\alpha, h_\alpha)$ de [4,§ 2.5] où $h_\alpha : \mathbb{S} \to G_\mathbb{R}$ est associé à z_α). Pour simplifier la notation, écrivons simplement T pour T_α et soit $R = \mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m$, un $\mathbb{Q}$-tore. Il existe alors un morphisme surjectif de tores algébriques dit de réciprocité

$$\mathrm{rec} : R \to T$$

et l'orbite de z_α sous $\mathfrak{g}_{E_\alpha}$ est contrôlée par l'image de $R(\mathbb{A}_f)/\overline{R(\mathbb{Q})}$. Notons U le noyau de l'application de réciprocité: c'est un groupe diagonalisable sur $\mathbb{Q}$. Nous démontrons (Théorème 3.3) l'énoncé suivant.

Théorème 1.1 *Soit (G,X) une donnée de Shimura de type adjoint. Il existe un entier k tel que pour toute sous-donnée de Shimura spéciale (T,h) telle* *que T est le groupe de Mumford-Tate de h et telle que $U = \mathrm{Ker}(R \to T)$ est connexe, l'ordre du conoyau de rec (vu comme morphisme des tores à valeurs dans $\mathbb{A}_f$, modulo l'adhérence des points rationnels) est fini, d'ordre borné par k. Il en résulte que la taille de l'orbite sous $\mathfrak{g}_E$ d'un point CM z, associé à une sous-donnée de Shimura spéciale (T, h) vérifiant les hypothèses précédentes, est (à un facteur majoré près) celle de $T(\mathbb{A}_f)$.*

Il est donc crucial de comprendre la connexité de U, et c'est ce que nous avons fait dans la première partie (§ 2, 3), au moins pour les groupes classiques. Nous nous sommes limités en général aux points z_α (ou aux tores T_α) "Galois-génériques". Ceci veut dire tout d'abord que le groupe de Mumford-Tate est de dimension maximale (si G est adjoint, c'est en fait un tore maximal); puis, que l'image de $\mathfrak{g}_E = \mathrm{Gal}(\bar{E}/E)$ dans $\mathrm{Aut}(X^*(T))$, $X^*(T)$ étant le groupe des caractères, est aussi maximale (cf. § 2, 3). On peut alors calculer le groupe $\pi_0(U)$.
Dans le § 2, ceci est fait pour les groupes adjoints classiques, à l'aide du formalisme de Shimura et Deligne. Dans le § 3, on reprend le problème pour $G = GSp(g, \mathbb{Q})$ ou $G = GU(h)$, groupe de similitudes unitaires.
Ces groupes sont plus naturels que les groupes adjoints, en relation avec les problèmes de modules des variétés abéliennes. De plus, pour les groupes unitaires quasi-déployés à la place réelle, on verra que le noyau U est connexe alors que son analogue ne l'est pas pour le groupe adjoint. Le § 3 contient aussi la démonstration du Théorème mentionée plus haut.
Enfin, le § 4, plus géométrique, contient une application (conditionnelle) à la Conjecture d'André-Oort (Théorème 4.7):

Théorème 1.2 *Soit S une variété de Shimura associée à une donnée de Shimura (G, X) avec G un groupe de type adjoint. Soit $Z \subset S$ est une sous-variété Hodge-générique (condition naturelle, cf. § 4) contenant une famille infinie bornée (pour la topologie usuelle) de points CM tels que le noyau U est connexe. Si la conjecture $(\mathcal{E}_a)$ est vérifiée alors $Z = S$.*

En particulier, sous $(\mathcal{E}_a)$, on peut donc démontrer la conjecture d'André-Oort pour des familles de points CM (bornées) "Galois-génériques" quand les résultats de § 2 et du § 3 nous assurent la connexité du noyau U. Notons aussi que dans notre situation l'analogue de la conjecture $(\mathcal{E}_a)$ sur la variété de Shimura est l'équidistribution des orbites toriques des points CM de S. Une conséquence surprenante de l'étude de la conjecture $(\mathcal{E}_a)$ initiée dans [3] est que la conjecture $(\mathcal{E}_a)$ semble plus facile à obtenir que son analogue sur la variété de Shimura. Si G est le groupe $PGL(2, F)$ pour un corps de nombres totalement réel, la conjecture $(\mathcal{E}_a)$ et son analogue sur la variété modulaire de Hilbert se ramènent via une formule de Waldspurger à des estimations analytiques de la valeur $L(\Pi, \frac{1}{2})$ de la fonction L du changement de base Π d'une représentation automorphe π pour $PGl(2, F)$ à un corps de multiplication complexe $E = F[\sqrt{d}]$. La preuve de $(\mathcal{E}_a)$ se déduit de propriétés élémentaires de convexité des fonctions L alors que l'analogue sur la variété de Shimura est une conséquence de la sous-convexité bien plus difficile à obtenir. L'hypothèse de Lindelöf conséquence de l'hypothèse de Riemann généralisée donnerait des résultats plus précis dans les deux situations.

Le Théorème 3.3 de cet article est étroitement lié à des arguments déjà utilisés par Edixhoven et Yafaev [7]. On se référera aussi à un article récent de Zhang [16] où des résultats plus complets sont obtenus dans un cas particulier. Néanmoins, Edixhoven et Yafaev appliquent ces idées en une place, ou un nombre fini de places, p-adiques; ils n'ont donc pas besoin de la connexité du noyau. La portée réelle, globale, du résultat, dans la situation particulière de ce texte (quand le noyau du morphisme de réciprocité est connexe) ne semble pas avoir été remarquée.

Dans tout l'article, notre référence implicite pour la théorie des variétés de Shimura est à Deligne [4].

2 Connexité des noyaux de réciprocité : groupes adjoints

2.1

Dans tout ce paragraphe, G est un groupe semi-simple connexe sur $\mathbb{Q}$ et de type adjoint (= de centre trivial). Notons $T \subset G$ un tore maximal; soit $T_{\mathbb{C}} \subset G_{\mathbb{C}}$ les groupes obtenus par extension des scalaires à $\mathbb{C}$ et B un sous-groupe de Borel de $G_{\mathbb{C}}$ contenant $T_{\mathbb{C}}$. (Si X est un groupe sur k et k'/k une extension, $X_{k'} = X \times_k k'$).

Soient $X^*(T)$ le groupe des caractères de $T_{\bar{\mathbb{Q}}}$, $R \subset X^*(T)$ l'ensemble des racines de (G,T) et $W = W(R)$ le groupe de Weyl. Soit Γ le groupe d'automorphismes de R préservant les racines de B. Alors $A(R) = W \rtimes \Gamma$ est le groupe d'automorphismes de R; soient $\{\alpha_1, \dots \alpha_\ell\}$ les racines simples.

L'image I de $\mathfrak{g} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans $\mathrm{Aut}(X^*(T))$ est contenue dans $A(R)$. Soit $\pi : A(R) \to \Gamma$ la projection et soit $I_\Gamma = \pi(I)$. Alors I_Γ est indépendant (à isomorphisme unique près) du choix de T et B; l'application $\mathfrak{g} \to I_\Gamma$ définit en fait la classe des formes intérieures de G parmi les $\mathbb{Q}$-formes de $G_{\bar{\mathbb{Q}}}$. On a $I \subset W \rtimes I_\Gamma$. On dira que T est Galois-générique s'il est maximal et si $I = W \rtimes I_\Gamma$.

On se donne par ailleurs une classe de conjugaison X, sous $G(\mathbb{R})$, d'homomorphismes $h : \mathbb{S} \to G(\mathbb{R})$ où $\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$. On suppose que X vérifie les conditions de Deligne [4, 2.1.1, 1-3]. Pour $h \in X$ on note $\mu : \mathbb{G}_{m,\mathbb{C}} \to G_{\mathbb{C}}$ le groupe à un paramètre associé, "$z \mapsto h(z,1)$" [4, 1.1.1]. On rappelle que si $H \subset G$ est un $\mathbb{Q}$-sous-groupe, $h(\mathbb{C}^\times) \subset H(\mathbb{R})$ si et seulement si $\mu(\mathbb{C}^\times) \subset H(\mathbb{C})$ [4, Lemme 1.2.4]. Pour $h \in X$ soit $MT(h) \subset G$ le plus petit $\mathbb{Q}$-sous-groupe H tel que $H(\mathbb{R})$ contienne $h(\mathbb{C}^\times)$ – ou que $H(\mathbb{C})$ contienne $\mu(\mathbb{C}^\times)$.

Proposition 2.1 *Il existe un sous-ensemble X' de X, dense pour la topologie complexe, tel que, si $h \in X'$, $MT(h)$ est un tore maximal Galois-générique.*

Notons en effet M l'espace de modules des tores maximaux de G : c'est une variété rationnelle définie sur $\mathbb{Q}$ (Platonov-Rapinchuk [12, p. 104]) et on dispose d'un espace fibré tautologique $\mathcal{T} \to M$ tel que $\mathcal{T}_m$ est le tore maximal associé à $m \in M$. En particulier, soit $\mathcal{T}_\eta$ le tore au-dessus du point générique η de M : c'est donc un tore sur $\mathbb{Q}(X_1, \dots, X_N)$. Si L est le corps de décomposition de $\mathcal{T}_\eta$, on sait d'après Voskresenskii [15] que $\mathrm{Gal}(L/\mathbb{Q}(X_1, \dots, X_N))$ est égal à $W \rtimes I_\Gamma$. D'après le théorème d'irréductibilité de Hilbert (cf. Serre [13, Prop. 1 p. 122]) on sait alors que

$$V = \{m \in M(\mathbb{Q}) : \mathcal{T}_m \text{est Galois-générique}\}$$

est le complémentaire d'un ensemble mince; il en résulte que V est dense dans $M(\mathbb{R})$ pour la topologie réelle (voir Lang [10, Cor. 2.5 p. 231] pour une variété M de dimension 1. En général, on peut combiner ce théorème avec un balayage de $\mathbb{P}^N$ ou $\mathbb{A}^N$ par des droites, cf. Serre [13, Theorem p. 127]).
Si $U \subset M(\mathbb{R})$ est l'ensemble des tores compacts de $G(\mathbb{R})$, alors U est ouvert dans $M(\mathbb{R})$. On en déduit :

Lemme 2.2 *L'ensemble des tores maximaux Galois-génériques T tels que $T(\mathbb{R})$ est compact est dense dans U.*

Soit $T \subset G$ un $\mathbb{Q}$–tore maximal et $\mu : \mathbb{G}_{m,\mathbb{C}} \to T_\mathbb{C}$. On a par ailleurs :

Lemme 2.3 (cf. Serre [14, Lemme 3 (b)])
Supposons que $Im(\mu)$ n'est contenu dans $H(\mathbb{C})$ pour aucun $\mathbb{Q}$-sous-groupe normal propre H de G. Alors l'orbite $\mathfrak{g} \cdot W\mu$ de μ dans $X_*(T_\mathbb{C}) = X_*(T_{\bar{\mathbb{Q}}})$ engendre le $\mathbb{Q}$-espace vectoriel $X_*(T_{\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$.

En effet les sous-espaces de $X_*(T_{\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$ stables par W et $\mathfrak{g}$ correspondent aux $\mathbb{Q}$-sous-groupes normaux connexes de G.
Soit (G, X) une donnée de Shimura, on rappelle que le groupe de Mumford-Tate générique de X est le plus petit $\mathbb{Q}$-sous-groupe $G'_\mathbb{Q}$ de $G_\mathbb{Q}$ tel que les $x \in X$ se factorisent par $G'_(\mathbb{R})$. Un point x de X est dit Hodge-générique si son groupe de Mumford-Tate est le groupe de Mumford-Tate générique de X. Il existe toujours des points Hodge-génériques. Rappelons que G, étant adjoint, est égal au groupe de Mumford-Tate d'un point Hodge-générique de X. Si $h \in X$ et μ est associé à h, on en déduit aussitôt que l'hypothèse du Lemme 2.3 est vérifiée puisqu'elle est invariante par conjugaison de h sous $G(\mathbb{R})$.
Le lemme suivant permet de calculer simplement le groupe de Mumford-Tate associé à un paramètre h dont l'image est contenue dans un tore.

Lemme 2.4 *Soit $T \subset G$ un $\mathbb{Q}$-tore, de sorte que $\mathfrak{g}$ opère sur $X = X_*(T_{\bar{\mathbb{Q}}})$. Soient $h : \mathbb{S} \to T_\mathbb{R}$ et μ le paramètre associé. Soient V l'espace engendré par $\mathfrak{g}\mu$ dans $X \otimes \mathbb{Q}$ et $\Lambda = X \cap V$. Alors Λ est le réseau des cocaractères de $MT(h) \subset T$.*

En effet Λ est un réseau primitif de X, invariant par $\mathfrak{g}$, et définit donc un sous-tore rationnel de T contenant l'image de μ et évidemment minimal.

Lemme 2.5 *Si $T \subset G$ est un $\mathbb{Q}$-tore maximal Galois-générique et si*

$$h : \mathbb{S} \to T_{\mathbb{R}},$$

alors T est le groupe de Mumford-Tate de h.

Avec les notations du Lemme précédent, soit en effet $V_\mu \subset X \otimes \mathbb{Q}$ le sous-espace engendré par $\mathfrak{g} \cdot \mu$. Puisque T est Galois-générique, $W \cdot \mu \subset \mathfrak{g} \cdot \mu$. D'après le Lemme 2.3, $V_\mu = V$. On conclut grâce au Lemme 2.4.

2.2

Nous supposons maintenant que G, toujours adjoint, est absolument simple sur $\mathbb{Q}$. Puisqu'il existe une donnée de Shimura pour G, $G_{\mathbb{R}}$ est absolument simple et la conjugaison complexe agit sur le diagramme de Dynkin par l'involution d'opposition [4].
Soit $h \in X$ une donnée dont le groupe de Mumford-Tate est un tore maximal Galois générique (i.e., une donnée passant par $T_{\mathbb{R}}$ où T est Galois-générique, cf. Lemme 2.5). Soient $\mu : \mathbb{G}_{m,\mathbb{C}} \to G_{\mathbb{C}}$ associé à h et $E = E(T, h)$ le corps reflex: ainsi μ est défini sur E:

$$\mu : \mathbb{G}_{m,E} \to T_E \subset G_E.$$

On dispose alors d'un morphisme de réciprocité

$$\mathrm{rec} : R = \mathrm{Res}_{E/\mathbb{Q}} \mathbb{G}_m \to T\ ,$$

défini sur $\mathbb{Q}$, d'où par fonctorialité

$$\mathrm{rec}_* : X_*(R_{\bar{\mathbb{Q}}}) \to X_*(T_{\bar{\mathbb{Q}}}).$$

Rappelons que les corps reflex sont, par hypothèse, contenus dans $\mathbb{C}$; on note $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. On a alors naturellement

$$X_*(R_{\mathbb{C}}) \cong \bigoplus_{\sigma : E \to \mathbb{C}} \mathbb{Z} \cdot [\sigma]$$

et $\mathrm{rec}([\sigma]) = \sigma(\mu) := \mu_\sigma \in X_*(T)$, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ opérant naturellement sur $X_*(T_{\bar{\mathbb{Q}}})$. (Si T est un tore sur $\mathbb{Q}$, on écrira simplement $X_*(T)$ pour le groupe $X_*(T_{\mathbb{C}}) = X_*(T_{\bar{\mathbb{Q}}})$ des cocaractères géométriques de T).
Notons L_μ le sous $\mathbb{Z}$-module de $X_*(T)$ engendré par les μ_σ ($\sigma : E \to \mathbb{C}$). Puisque T est le groupe de Mumford-Tate, l'application $R \to T$ est surjective. Du point de vue des cocaractères, ceci se traduit par le fait que $L_\mu \otimes \mathbb{Q} = X_*(T) \otimes \mathbb{Q}$. Notre but est d'expliciter L_μ pour les groupes de type A, B, C, D et les cocaractères minuscules associés aux variétés de Shimura. Dans les énoncés, T est un tore maximal Galois-générique du groupe (du type indiqué) G, et h se factorise par T. Le groupe de Galois opère donc sur T par

$I = W \rtimes I_\Gamma$. Enfin, les possibilités pour μ sont décrites par Deligne [4]: ce sont les poids minuscules de Bourbaki [1].
Dans tous les calculs qui suivent, nous avons utilisé sans commentaire les notations de Bourbaki [1] relatives aux systèmes de racines; en particulier nous n'avons pas rappelé la description des bases naturelles, des poids fondamentaux associés, etc.

2.3 Type C_ℓ ($\ell \geqslant 2$)

Proposition 2.6 *Si $T \subset G$ et G est de type C_ℓ,*

$$L_\mu = X_*(T).$$

Notons $X_\mathbb{R} = X \bigotimes_\mathbb{Z} \mathbb{R}$ et $Y_\mathbb{R}$ le dual de $X_\mathbb{R}$, engendré par les coracines. On peut alors identifier $X_\mathbb{R}$ et $Y_\mathbb{R}$ à $\mathbb{R}^\ell$, la dualité étant le produit scalaire usuel. On a les racines et coracines [1] :

$$R = \{\pm 2\varepsilon_i \ , \ 1 \leqslant i \leqslant \ell\} \cup \{\pm\varepsilon_i \pm \varepsilon_j \ , \ i < j\}$$

$$R^\vee = \{\pm\varepsilon_i \ , \ \pm\varepsilon_i \pm \varepsilon_j\}.$$

Le groupe $A(R)$ est $W(R) = \mathfrak{S}_\ell \rtimes (\mathbb{Z}/2\mathbb{Z})^\ell$, opérant de la façon usuelle; il est égal à I.
Le seul cocaractère minuscule est $\mu = \omega_\ell^\vee = \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_\ell)$, ℓ-ième copoids (Bourbaki [1]); son orbite sous I, de cardinal 2^ℓ, est l'ensemble $\{\frac{1}{2}(\pm\varepsilon_1 \pm \varepsilon_2 \cdots \pm \varepsilon_\ell)\}$. Donc L_μ contient $\varepsilon_1, \ldots \varepsilon_\ell$ ainsi que $\frac{1}{2}(\varepsilon_1 + \cdots \varepsilon_\ell)\}$; G étant adjoint $X_*(T)$ est le réseau des copoids de T, qui est engendré par ces $(\ell+1)$ éléments.

2.4 Type B_ℓ ($\ell \geqslant 2$).

Avec les notations précédentes,

$$R = \{\pm\varepsilon_i \ , \ \pm\varepsilon_i \pm \varepsilon_j\}$$
$$R^\vee = \{\pm 2\varepsilon_i \ , \ \pm\varepsilon_i \pm \varepsilon_j\}.$$

Le groupe de Weyl opère comme dans le cas C_ℓ. L'unique copoids minuscule est $\mu = \omega_1^\vee = \varepsilon_1$ (Bourbaki [1, p. 255); on a fixé la base usuelle de R et donc de $R^\vee$). Alors $L_\mu = X_*T = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_\ell$, réseau des copoids (Bourbaki, loc. cit.). Ainsi :

Proposition 2.7 (G *de type* B_ℓ)

$$L_\mu = X_*(T).$$

[1] On a utilisé, sans risque de confusion, R pour un système de racines ainsi que pour le tore $\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m \ldots$

2.5 Type D_ℓ ($\ell \geqslant 4$).

Nous excluons pour l'instant, dans le cas où $\ell = 4$, les groupes associés à la trialité. Distinguons deux cas :

– Si ℓ est pair, le groupe réel déployé de type D_ℓ est forme intérieure de sa forme compacte. D'après l'hypothèse qui précède, le groupe I_Γ est isomorphe à $\{1\}$ ou à $\mathbb{Z}/2\mathbb{Z}$. Dans le second cas, $\mathfrak{g}_{\mathbb{Q}}$ opère donc sur le diagramme de Dynkin par $\mathrm{Gal}(F/\mathbb{Q})$ où F est une extension quadratique réelle de $\mathbb{Q}$ (cf. Deligne [4, 2.3.4]).

– Si ℓ est impair, le groupe compact de type D_ℓ correspond à une action non triviale de $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ sur le diagramme de Dynkin. Donc $I_\Gamma \cong \mathbb{Z}/2\mathbb{Z}$.

Dans ce cas

$$\begin{aligned} &R = \{\pm\varepsilon_i \pm \varepsilon_j : 1 \leqslant i < j \leqslant \ell\} \\ &R^\vee = R \quad (\mathbb{R}^\ell \text{ étant identifié à son dual}). \end{aligned}$$

$W(R) = \mathfrak{S}_\ell \rtimes (\pm 1)^{\ell-1}$, $(\pm 1)^{\ell-1}$ étant donné par les changements de signe de produit égal à 1 des coordonnées et par hypothèse $\mathfrak{g}_{\mathbb{Q}}$ opère par $W(R)$ ou par $W(R) \rtimes \{1, c\}$ où c permute les racines $\alpha_{\ell-1} = \varepsilon_{\ell-1} - \varepsilon_\ell$ et $\alpha_\ell = \varepsilon_{\ell-1} + \varepsilon_\ell$; alors $W(R) \rtimes \{1, c\} = \mathfrak{S}_\ell \rtimes (\pm 1)^\ell$.

Il y a deux possibilités pour le cocaractère μ [4, p. 261] :

– si $G_{\mathbb{R}}$ est un vrai groupe orthogonal, $\mu = \omega_1^\vee = \varepsilon_1$

– si $\ell \geqslant 5$ et si $G_{\mathbb{R}}$ est le groupe symplectique d'un module hermitien sur une algèbre de quaternions, $\mu = \omega_\ell^\vee = \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_\ell)$.

Enfin, $X_*(T) = P(R^\vee) = \bigoplus\limits_{i=1}^{\ell} \mathbb{Z}\varepsilon_i + \mathbb{Z}(\dfrac{1}{2}\sum\limits_{1}^{\ell} \varepsilon_i)$.

– Si $\mu = \omega_1^\vee$, l'orbite de μ est, quelle que soit l'image de $\mathfrak{g}_{\mathbb{Q}}$, égale à $\oplus\mathbb{Z}\varepsilon_i$. On a donc une suite exacte

$$1 \to L_\mu \to X_*(T) \to \mathbb{Z}/2\mathbb{Z} \to 0 \tag{2.1}$$

$\mathbb{Z}/2\mathbb{Z}$ étant identifié à $P(R^\vee) \bigoplus \mathbb{Z}\varepsilon_i$.

– Si $\mu = \omega_\ell^\vee$, et si $\mathfrak{g}_{\mathbb{Q}}$ est d'image $\mathfrak{S}_\ell \rtimes (\pm 1)^\ell$, L_μ contient $\omega_\ell^\vee$ et $\frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_{\ell-1} - \varepsilon_\ell)$ donc ε_ℓ, donc $\bigoplus\limits_i \mathbb{Z}\varepsilon_i \oplus \mathbb{Z}\omega_\ell^\vee = X_*(T)$.

Si l'image de $\mathfrak{g}_{\mathbb{Q}}$ n'est pas totale, ℓ est pair; $X_*(T)/\mathbb{Z}R^\vee \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, engendré par les images de $\omega_\ell^\vee$ et ε_1; L_μ contient $\frac{1}{2}\sum \varepsilon_i$, donc $\frac{1}{2}(\varepsilon_1 + \varepsilon_2 - \sum\limits_{i>2} \varepsilon_i)$, donc $\varepsilon_1 + \varepsilon_2$, donc enfin $R^\vee$.

Enfin $X_*(T) = \{x = (x_i \in (\frac{1}{2}\mathbb{Z})^\ell : x_i \equiv x_j[1]\}$. L'homomorphisme $X_*(T) \to \mathbb{Z}/2\mathbb{Z}$, $x \mapsto \sum\limits_{i \leqslant \ell} x_i - \sum\limits_{i > \ell} x_i$ $[2]$ annule $\mathbb{Z}R^\vee$ et $\omega_\ell^\vee$ est invariant par l'action de $W(R)$. Il n'est pas trivial sur ε_1, d'où de nouveau une suite exacte de la forme (2.1), $\mathbb{Z}/2\mathbb{Z}$ étant l'image de ε_1.

Revenons sur le cas de la trialité. L'image I de $\mathfrak{g}_{\mathbb{Q}}$ dans $A(R)$ contient $W(R)$ qui est d'indice 1, 2 ou 6 dans I. Dans le second cas, nous pouvons supposer pour un choix de base convenable de R que $I = \mathfrak{S}_4 \rtimes (\pm 1)^4$. Les deux caractères $\omega_1^\vee$ et $\omega_\ell^\vee$ ne sont pas conjugués par I et la relation entre L_μ et $X_*(T)$ est celle décrite précédemment. Enfin, si $|I/W(R)| = 6$, $\omega_1^\vee$ et $\omega_4^\vee$ sont conjugués par I. Ils sont donc indiscernables de notre point de vue, et le calcul précédent montre que $L_\mu = X_*(T)$. Pour résumer :

Proposition 2.8 *(G de type D_ℓ; si $\ell = 4$, $\omega_1^\vee$ et $\omega_4^\vee$ sont définis comme ci-dessus).*
(1) *Si $\mu = \omega_1^\vee$ et si G n'est pas trialitaire sur $\mathbb{Q}$, L_μ est d'indice 2 dans $X_*(T)$.*
(2) *Si $\mu = \omega_\ell^\vee$ et si G n'est pas trialitaire, $|X_*(T)/L_\mu| = 1$ si $|I/W(R)| = 2$; $|X_*(T)/L_\mu| = 2$ si $I = W(R)$.*
(3) *Si $\ell = 4$ et G est trialitaire, $L_\mu = X_*(T)$.*

2.6 Type A_ℓ ($\ell \geqslant 2$)

C'est le cas le plus riche, puisque tous les poids fondamentaux sont associés à des variétés de Shimura. On pose $n = \ell + 1$, donc G est une forme de $\mathrm{PGL}(n)$. On identifie $X_\mathbb{R} = X_*(T) \otimes \mathbb{R}$ à

$$H = \{x \in \mathbb{R}^n : \sum x_i = 0\} .$$

La dualité euclidienne sur $\mathbb{R}^n$ permet d'identifier H à son dual. Alors

$$\begin{aligned} R = R^\vee &= \{\varepsilon_i - \varepsilon_j : i, j \leqslant n \ , \ i \neq j\} \\ B = B^\vee &= \{\alpha_1 = \varepsilon_1 - \varepsilon_2, \dots \alpha_\ell = \varepsilon_{n-1} - \varepsilon_n\} . \end{aligned}$$

Le groupe $W(R) = \mathfrak{S}_n$ opère par permutation; $A(R) = W(R) \rtimes \mathbb{Z}/2\mathbb{Z}$, égal à I car $G(\mathbb{R})$ doit être forme extérieure de $\mathrm{PGL}(n, \mathbb{R})$.
Le réseau des racines est

$$Q(R) = Q(R^\vee) = \{x \in \mathbb{Z}^n : \sum x_i = 0\} ;$$

le réseau des poids est engendré par les poids

$$\begin{aligned} \omega_p = \omega_p^\vee &= \text{projection sur } H \text{ de } \varepsilon_1 + \cdots + \varepsilon_p \\ &= \varepsilon_1 + \cdots + \varepsilon_p - \frac{p}{n} \sum_{i=1}^n \varepsilon_i \qquad (1 \leqslant p \leqslant \ell). \end{aligned}$$

On a donc :

$$P(R) = P(\check{R}) = (x \in \frac{1}{n}\mathbb{Z}^n : \sum x_i = 0 \ , \ x_i \equiv x_j \ [1]\} ;$$

L'isomorphisme, qu'on notera det : $P(\check{R})/Q(\hat{R}) \to \mathbb{Z}/n\mathbb{Z}$ est donné par $x = (x_i) \mapsto x_i$ [mod 1] où l'on a identifié $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, et i est arbitraire.
Fixons $p \in \{1, \dots \ell\}$ et soit $r = (n, p)$.

Proposition 2.9 (*G de type A_ℓ, $n = \ell + 1$, $\mu = \omega_p^\vee$*).

(i) *L_μ contient $Q(R^\vee)$*

(ii) *On a une suite exacte*

$$0 \to L_\mu \to X_*(T) \underset{\det}{\to} < \frac{n}{r} \cdot 1 > \to 0$$

le quotient étant donc isomorphe à $\mathbb{Z}/(r)\mathbb{Z}$.

Notons π la projection de $\mathbb{R}^n$ sur H. Alors L_μ contient $\pi(\varepsilon_1 + \cdots + \varepsilon_p)$ donc, étant stable par $\mathfrak{S}_n$, $\pi(\varepsilon_2 + \cdots + \varepsilon_{p+1})$, donc $\pi(\varepsilon_1 - \varepsilon_{p+1})$; l'action de $\mathfrak{S}_n$ montre alors que L_μ contient $Q(R^\vee)$. Par ailleurs

$$\det(\omega_p^\vee) = -\frac{p}{n}(\in \frac{1}{n}\mathbb{Z}/\mathbb{Z}) \equiv -p(\in \mathbb{Z}/n\mathbb{Z}),$$

qui engendre le sous-groupe $< r \cdot 1 >$ de $\mathbb{Z}/n\mathbb{Z}$. Mais l'image inverse de ce sous-groupe dans $P(R^\vee) = X_*(T)$ est stable par $A(R)$ car $\det(\sigma x) = \det(x)$ si $\sigma \in \mathfrak{S}_n$ et $\det(\theta x) = -\det(x)$ si θ est le générateur du sous-groupe $\mathbb{Z}/2\mathbb{Z}$ de $A(R)$, qui opère par $(x_1, \ldots, x_n) \mapsto (-x_n, \ldots, -x_1)$.

Corollaire 2.10 *$L_\mu = X_*(T)$ si, et seulement si, $(p, n) = 1$.*

C'est le cas, en particulier, si $p = 1$ ou si $n = 2p + 1$: dans ce dernier cas $G_\mathbb{R}$ est quasi déployé. Dans le paragraphe suivant on vérifiera que si $n = 2p$ (donc $G_\mathbb{R}$ quasi-déployé) on peut améliorer le résultat en considérant un groupe de similitudes unitaire.

2.7

La signification de ces calculs pour le contrôle de l'application de réciprocité est donnée par le résultat évident qui suit :

Proposition 2.11 *Si $L_\mu = X_*(T)$, $U = \ker(\mathrm{rec} : R \to T)$ est connexe. En général, $X_*(T)/L_\mu$ s'identifie à U/U^0 où U^0 est la composante neutre (géométrique) de U.*

Si en effet X est un tore, $\mathrm{Ext}^1(\mathbb{G}_m, X) = \{0\}$, sur $\bar{\mathbb{Q}}$ ou $\mathbb{C}$; si X est un groupe (diagonalisable) fini, $\mathrm{Ext}^1(\mathbb{G}_m, X)$ est naturellement isomorphe à $X(\bar{\mathbb{Q}})$ (ou $X(\mathbb{C})$).
La suite exacte

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{G}_m, R) \arrow[r] \arrow[d, equal] & \mathrm{Hom}(\mathbb{G}_m, T) \arrow[r] \arrow[d, equal] & \mathrm{Ext}^1(\mathbb{G}_m, U) \arrow[r] & \mathrm{Ext}^1(\mathbb{G}_m, X) \arrow[d, equal] \\
X_*(R) & X_*(T) & & \{0\}
\end{tikzcd}$$

permet de conclure.
On remarquera que (pour G de type A_ℓ) la description explicite du conoyau donnée par la Proposition 2.9 contient l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur U/U^0.
Enfin, terminons sur l'espoir qu'un expert des calculs relatifs aux groupes exceptionnels pourra résoudre ce problème pour les groupes de type E_6 et E_7 (Deligne [4, p. 261]).

3 Connexité des noyaux de réciprocité : une autre approche

Dans ce paragraphe nous ne supposons pas G adjoint; nous supposerons en fait que G est associé, à la Shimura-Deligne-Langlands, à un problème de modules pour des variétés abéliennes (cf. tout particulièrement [8] pour une description précise.) Nous reprenons dans ce cadre l'étude de la surjectivité de l'application $R \to T$ du § 2. Dans ce cas la question ne se réduit pas à un problème relatif aux systèmes de racines. Nous avons décrit les tores, et les applications, en restant proche du problème de modules. Nous nous limitons au groupe symplectique et aux groupes unitaires.

3.1 Le formalisme de la multiplication complexe

Soient E un corps CM, F son sous-corps totalement réel maximal et $c \in \mathrm{Aut}(E/\mathbb{Q})$ la conjugaison complexe. Notons E^{gal} la clôture galoisienne de E dans $\bar{\mathbb{Q}}$ (comme dans le § 2, on suppose les corps de nombres plongés dans $\mathbb{C}$). Soient J l'ensemble des plongements $E \to \bar{\mathbb{Q}}$ et $\Sigma \subset J$ un type CM : ainsi $J = \Sigma \amalg {}^c\Sigma$.
Notons $\mathfrak{g} = \mathrm{Gal}(E^{\mathrm{gal}}/\mathbb{Q})$. Alors $\mathfrak{g}$ opère sur J, transitivement et fidèlement, $c \in \mathfrak{g}$ et $c\sigma = \sigma c$ ($\sigma \in \mathfrak{g}$).
Soit $g = [F : \mathbb{Q}]$.
Nous pouvons indexer Σ par les indices $\{1, \dots g\}$ et ${}^c\Sigma$ par les indices $\{g+1, \dots 2g\}$ de sorte que c s'identifie à la permutation $(1, 2g)(2, 2g-1) \cdots (g, g+1)$. Le centralisateur de c dans $\mathfrak{S}_{2g}$ s'identifie à $C_g = \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$; si $\sigma \in \mathfrak{S}_g$ l'élément associé de $\mathfrak{S}_{2g}$ laisse stable Σ et ${}^c\Sigma$, opère sur $\Sigma \cong \{1, \dots g\}$ de la façon naturelle et sur ${}^c\Sigma \cong \{g+1, \dots 2g\}$ par $2g+1-i \mapsto 2g+1-\sigma(i)$ ($i = 1, \dots g$). Un élément $\varepsilon = (\varepsilon_i)$ de $(\mathbb{Z}/2\mathbb{Z})^g$ opère par le produit $\prod_{i=1}^{g} s_i^{\varepsilon_i}$ où $s_i = (i, 2g+1-i) \in \mathfrak{S}_{2g}$. Noter que le groupe C_g est bien sûr isomorphe au groupe de Weyl de type C_g. On a ainsi associé à un corps CM un groupe $\mathfrak{g} \subset C_g \subset \mathfrak{S}_{2g}$ transitif sur $J \equiv \{1, \dots 2g\}$.

3.2 Le cas de $GSp(g)$

Fixons une forme bilinéaire alternée – par exemple, de matrice $\begin{pmatrix} & -1_g \\ 1_g & \end{pmatrix}$ – sur $\mathbb{Q}^{2g}$ et soit $G = GSp(g)$ le groupe de similitudes symplectiques associé.

Soit $h : \mathbb{S} \to G_{\mathbb{R}}$ un paramètre associé au problème de modules usuel des variétés abéliennes (Kottwitz [8] : avec la description donnée de G, h est conjugué à

$$h_0 : z = x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

où les blocs sont de taille g). On suppose que h définit un point CM d'une variété S_K associée à G, avec $K \subset G(\mathbb{A}_f)$. Soit T un tore maximal de G contenant l'image de h.

Alors $T_{\mathbb{R}}$ est un tore maximal elliptique de $G_{\mathbb{R}}$ et T est donc un tore maximal elliptique de G. Rappelons que ceux-ci sont décrits par les données suivantes. Posons $g = g_1 + \cdots + g_r$ $(r \leqslant g)$ et donnons-nous, pour tout j, un corps de nombres F_j de degré g_j et une extension quadratique E_j de F_j ; on note simplement $z \mapsto \bar{z}$ la conjugaison de E_j par rapport à F_j. Pour tout j soit $\iota_j \in E_j$ tel que $\bar{\iota}_j = -\iota_j$. On munit E_j d'une forme $\mathbb{Q}$-linéaire alternée donnée par $< x, y >= Tr_{E_j/\mathbb{Q}}(\bar{x}\iota_j y)$. Alors le tore $\{x \in E_j : x\bar{x} \in \mathbb{Q}^\times\}$ se plonge dans le groupe des similitudes symplectiques de E_j. Lorsque les données proviennent de h, les paires (E_j, F_j) doivent être des données CM. Le tore rationnel T associé a pour points rationnels :

$$T(\mathbb{Q}) = \{(x_j \in E_j : x_j\bar{x}_j = x \in \mathbb{Q}^\times)\} ,$$

de dimension $g+1$. On le plonge dans G en identifiant les espaces symplectiques $\bigoplus E_j$ et $\mathbb{Q}^{2g}$.

Nous dirons que h, ou T est Galois-générique s'il en est de même pour les données à eux associées pour le groupe adjoint. Ceci veut dire que le corps CM E est unique, de dimension $2g$, et que le groupe $\mathfrak{g}$ décrit dans le § 3.1 est égal à C_g. (On vérifie que ceci ne dépend pas du choix d'un type CM). La Proposition 2.1 nous garantit l'existence de (nombreux) tores Galois-génériques.

Notons S le tore associé à T dans $GL(\mathbb{Q}^{2g})$ – son centralisateur. Alors $S \cong \mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_m)$ et $h : \mathbb{S}(\mathbb{R}) \to (\mathbb{C}^\times)^{2g}$ s'écrit à permutation près des coordonnées sous la forme

$$z \mapsto (z, \ldots, z, \bar{z}, \ldots, \bar{z}) \quad (z \in \mathbb{C}^\times).$$

Le paramètre μ associé est

$$z \mapsto (z, \ldots, z, 1, \ldots, 1).$$

Si on note (x_i) $(i \leqslant 2g)$ les coordonnées de $x \in S$, T est décrit par

$$T = \{(x_1, \ldots, x_{2g}; x) : x_i x_{2g+1-i} = x\} \subset S \times \mathbb{G}_m$$

(l'indexation étant choisie, pour l'action de la conjugaison complexe, conformément au § 3.1) et

$$\mu : z \mapsto ((z, \ldots, z, 1, \ldots 1); z). \tag{3.1}$$

Nous utiliserons aussi ces descriptions sur $\bar{\mathbb{Q}}$, l'action du groupe de Galois $\mathfrak{g}$ (ou $\mathfrak{g}_{\mathbb{Q}}$) s'y lisant de façon évidente. On a aussi

$$\mu = ((1, \dots 1, 0, \dots 0); 1) \in X_*(S \times \mathbb{G}_m) = \mathbb{Z}^{2g+1}.$$

Le réseau $X_*(T) \subset X_*(S \times \mathbb{G}_m)$ s'identifie à l'ensemble des

$$\underline{\lambda} = \{(\lambda_1, \dots \lambda_{2g}; \lambda) : \lambda_i + \lambda_{2g+1-i} = \lambda\} \ . \tag{3.2}$$

Calculons d'abord le corps reflex, que l'on notera ici K. C'est le corps de rationalité de μ, donc

$$\mathrm{Gal}(E^{\mathrm{gal}}/K) = \{\sigma = (s, \varepsilon) \in \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g : \sigma \text{ fixe } \mu\} = \mathfrak{S}_g.$$

Donc $\mathrm{Gal}(E^{\mathrm{gal}}/\mathbb{Q})/\mathrm{Gal}(E^{\mathrm{gal}}/K) \cong \{j : K \to \bar{\mathbb{Q}}\} \cong (\mathbb{Z}/2\mathbb{Z})^g$ (isomorphismes d'ensembles). On remarquera que $|\mathrm{Gal}(E^{\mathrm{gal}}/K)|$ est le degré de la représentation du groupe dual associée par Langlands à la variété de Shimura : tous deux sont en effet égaux au cardinal de l'orbite de μ par le groupe de Weyl.

A ce point du calcul on peut vérifier que T est le groupe de Mumford-Tate du paramètre h, ce qu'on pourrait bien sûr déduire du § 2. On a en effet une suite exacte

$$0 \to \underline{E}_1^\times \to T \to \mathbb{G}_m \to 0$$

où $\underline{E}_1^\times$ est le $\mathbb{Q}$-tore défini par le noyau de $N_{E/F} : E^\times \to F^\times$. Le groupe de Mumford-Tate s'envoie surjectivement sur $\mathbb{G}_m$, cf. (3.1); C_g opère naturellement sur $X^*(S) = \mathbb{Z}^{2g}$ et commute à la conjugaison complexe c (§ 3.1). Décomposons $\mathbb{R}^{2g} = V = V^+ \oplus V^-$ sous l'action de c. Alors l'action de C_g sur $X^*(\underline{E}_1^\times) \otimes \mathbb{R}$ est sa représentation sur V^-, qui est l'action naturelle, irréductible, du groupe de Weyl. Le groupe de Mumford-Tate doit donc contenir $\underline{E}_1^\times$ et est égal à T.

Vérifions la surjectivité de $\mathrm{rec}_* : X_*(R) \to X_*(T)$. On a $X_*(R) = \bigoplus_{\varepsilon \in (\mathbb{Z}/2\mathbb{Z})^g} \mathbb{Z}\varepsilon$, et $X_*(T)$ s'identifie à $\mathbb{Z}^{g+1}$ par les coordonnées $(\lambda_1, \dots, \lambda_g, \lambda)$ de (3.2). Alors $\mu = (1, \dots, 1; 1) \in \mathbb{Z}^{g+1}$; si $\varepsilon = (1, \dots, 1, 0, 1, \dots, 1) \in (\mathbb{Z}/2\mathbb{Z})^g$ (0 à la place i), $\varepsilon(\mu) = (0, \dots, 1, \dots 0; 1)$ (1 à la place i). Notons ε_i cet élément de $(\mathbb{Z}/2\mathbb{Z})^g$, et soit $\theta = (1, \dots 1) \in (\mathbb{Z}/2\mathbb{Z})^g$.

L'application

$$\mathrm{rec}_* : \bigoplus_{\varepsilon = \varepsilon_j, \theta} \mathbb{Z}\varepsilon \to X_*(T) = \mathbb{Z}^{g+1}$$

a pour matrice

$$\begin{pmatrix} 1 & 0 & & & 0 \\ 0 & 1 & & & \vdots \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \\ 1 & 1 & & 1 & 1 \end{pmatrix}$$

de déterminant 1. L'application $X_*(R) \to X_*(T)$ est donc surjective. On en déduit, par la Proposition 2.11, la connexité du noyau.

Remarquons qu'il est vraisemblable que la connexité du noyau du morphisme de réciprocité pour le groupe adjoint (et un morphisme μ^{ad}) devrait l'impliquer pour le groupe de similitudes (et μ d'image μ^{ad}). Nous n'avons pas su le démontrer.

Terminons par quelques calculs dans le cas $g = 2$; G est alors associé à l'espace de modules de surfaces abéliennes. Supposons que T est un tore maximal irréductible, i.e., défini par un corps CM E de degré 4. On ne suppose plus E Galois-générique. D'après le § 3.1, $\mathrm{Gal}(E^{\mathrm{gal}}/\mathbb{Q})$ s'identifie à un sous-groupe $\mathfrak{g}$ de $C_2 = \mathfrak{S}_2 \ltimes (\mathbb{Z}/2\mathbb{Z})^2$, contenant la conjugaison complexe $c = (14)(23)$, et transitif sur I_4. Soit $s := \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}$ le générateur du facteur $\mathfrak{S}_2$. Il y a deux possibilités pour $\mathfrak{g} \neq C_2$:

(a) $\mathfrak{g} = \{1, c, s, sc\} \cong (\mathbb{Z}/2\mathbb{Z})^2$

(b) $\mathfrak{g} = \{1, \tau, \tau^2, \tau^3\}$ où $\tau = s\varepsilon$, $\varepsilon = (14)$ ou $(23) \in (\mathbb{Z}/2\mathbb{Z})^2$. Alors $\tau^2 = c$ et $\mathfrak{g}$ est cyclique d'ordre 4.

Soit $V = \mathbb{Q}^4$, muni de la représentation naturelle de $\mathfrak{g}$; on a $V = V^+ \oplus V^-$ sous l'action de c, et le groupe de Mumford-Tate M est déterminé par le sous-espace de V^- stable par $\mathfrak{g}$, tel que le tore associé à ce sous-espace et au facteur de V^+ correspondant au sous-espace diagonal de V contienne l'image de h : $z \mapsto (z, z, \bar{z}, \bar{z})$. Dans le cas (a), c'est le cas pour $(V^-)^s$. On a un diagramme d'extensions

$$\begin{tikzcd}
& E \arrow[dl, dash, "<c>"'] \arrow[dr, dash, "<s>"] & \\
F \arrow[dr, dash] & & E_0 \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

avec F quadratique réel, E_0 quadratique imaginaire, et

$$M(\mathbb{Q}) = E_0^\times \subset T(\mathbb{Q}) = \{z \in E^\times : N_{E/F} z \in \mathbb{Q}^\times\}.$$

Le corps reflex est $K = E_0$. Identifiant $X_*(M)$ à $\mathbb{Z}^2$ de la façon naturelle, on a $X_*(R) \to X_*(M)$ donné par $\mathrm{Gal}(R/\mathbb{Q}) = \{R \to \bar{\mathbb{Q}}\} = \{1, c\}$

$$\begin{aligned} 1 &\mapsto (1,0) \in X_*(M) \\ c &\mapsto (0,1). \end{aligned}$$

Le morphisme de réciprocité est donc l'isomorphisme canonique $E_0^\times \to E_0^\times$ et donc bijectif.

Considérons le cas (b), par exemple pour $\varepsilon = (14)$; alors $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$. Puisque τ^2 opère par (-1) sur V^-, τ n'a pas de sous-espace rationnel stable. Par conséquent $M = T$. On vérifie que le corps reflex est E.

L'application de réciprocité est donnée par

$$\begin{aligned} 1 &\mapsto (1,1,0,0;1)\\ \tau &\mapsto (1,0,1,0;1)\\ \tau^2 &\mapsto (0,0,1,1;1)\\ \tau^3 = c\tau &\mapsto (0,1,0,1;1) \end{aligned}$$

On vérifie aisément qu'elle est surjective de $X_*(R)$ vers $X_*(T)$.
Il serait bien sûr intéressant d'étudier la surjectivité pour les corps CM arbitraires, mais ceci semble difficile.

3.3 Groupes de similitudes unitaires

Dans cette section $E_0/\mathbb{Q}$ est un corps quadratique imaginaire, et G est le groupe de similitudes unitaires d'un espace hermitien de dimension n sur E_0. (Les calculs qui suivent s'appliquent aussi aux groupes unitaires définis par des algèbres à division).

Rappelons la description des tores maximaux (elliptiques) de G : soit $n = \sum_1^r n_i$ et pour tout i soit F_i une extension de $\mathbb{Q}$ linéairement disjointe de E_0 de degré n_i et $E_i = E_0F_i$. Sur E_i notons simplement $z \mapsto \bar{z}$ la conjugaison par rapport à F_i. Alors

$$T(\mathbb{Q}) = \{(z_i \in E_i^\times) : z_i\bar{z}_i = x \in \mathbb{Q}^\times\}.$$

Le tore T ne peut être Galois-générique que si $r = 1$; pour que $T(\mathbb{R})$ contienne l'image d'un paramètre de Shimura, il faut que F soit totalement réel; E est alors un corps CM.
Choisissons un plongement complexe ι_0 de E_0. (E_0 n'est pas a priori un corps reflex, donc n'a pas de plongement préféré dans $\mathbb{C}$). Les places complexes de E s'identifient alors aux plongements complexes $E \to \mathbb{C}$ par le choix, pour toute place w, d'un plongement ι, ι_0-linéaire, définissant w; ceci définit un type CM pour E. Si T est associé à E,

$$T(\mathbb{Q}) = \{z \in E^\times : N_{E/F}z \in \mathbb{Q}^\times\} \tag{3.3}$$

et $T(\mathbb{R})$ est défini par la relation déduite de (3.3) dans

$$S(\mathbb{R}) = (E \otimes \mathbb{R})^\times = E_{w_1}^\times \times \cdots \times E_{w_n}^\times \cong (\mathbb{C}^\times)^n; \tag{3.4}$$

on a noté S le tore $\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m$.
Les paramètres h déduits des problèmes de module naturels, pour les variétés abéliennes, associés à G sont décrits par Kottwitz [8]. Si h se factorise par $T(\mathbb{R})$ on a alors

$$h : z \mapsto (z, \dots z, \bar{z} \dots \bar{z}) \quad (z \in \mathbb{S}(\mathbb{R}) = \mathbb{C}^\times) \tag{3.5}$$

avec p occurences de z et $q = n - p$ occurences de $\bar{z}$. Noter que l'image de h est bien dans $T(\mathbb{R})$ défini, dans la description (3.4) par

$$T(\mathbb{R}) = \{(z_i = z_{w_i}) : z_i \bar{z}_i = x \in \mathbb{R}^\times\}.$$

On a naturellement

$$X_*(S) = \bigoplus_w (\mathbb{Z}\iota \oplus \mathbb{Z}\bar{\iota}) \cong \mathbb{Z}^{2n}$$

où pour tout $w = w_1, \ldots, w_n, \iota$ est défini comme ci-dessus, et $X_*(T)$ s'identifie alors à

$$X_*(T) = \{(\lambda_\iota, \lambda_{\bar{\iota}} : \lambda_\iota + \lambda_{\bar{\iota}} = \lambda)\}$$

isomorphe à $\mathbb{Z}^{n+1}$ par le choix des coordonnées (λ_ι, λ). Le paramètre μ déduit de h est alors

$$\mu : z \mapsto (z, \ldots z, 1, \ldots, 1; z) \quad (z \in \mathbb{G}_m)$$

ou de façon équivalente

$$\mu = (1, \ldots 1, 0 \ldots 0; 1) \in \mathbb{Z}^{n+1}$$

(p occurences de 1).

Enfin, le tore adjoint associé T^{ad} est Galois-générique si et seulement si $\mathrm{Gal}(E^{\mathrm{gal}}/\mathbb{Q})$ est isomorphe à $\mathfrak{S}_n \times \mathbb{Z}/2\mathbb{Z}$, $\mathfrak{S}_n$ permutant les plongements $\{\iota\}$ et le générateur c de $\mathbb{Z}/2\mathbb{Z}$ opérant par conjugaison complexe.

Calculons le groupe de Mumford-Tate. Soit d'abord $V = X_*(S) \otimes \mathbb{Q} \cong \mathbb{Q}^{2n}$. Sous l'action de c, V est la somme de deux modules V^+ et V^-, chacun somme d'un module irréductible $V^\pm_{n-1}$ sous $\mathfrak{S}_n$ et d'un module trivial $V^\pm_1$. La représentation de $\mathfrak{S}_n \times < c >$ sur $X_*(T) \otimes \mathbb{Q}$ est somme de V_1^+, V_1^- et V^-_{n-1}.

On a une application naturelle (rapport de similitude)

$$T \to \mathbb{G}_{m,\mathbb{Q}}, \qquad z \mapsto N_{E/F}(z), \qquad (z \in T(\mathbb{Q})),$$

et l'on sait que le groupe de Mumford-Tate $M \subset T$ a pour image $\mathbb{G}_m$. De plus son image dans T^{ad} est égale à T^{ad}, par exemple d'après le § 2 (T^{ad} est son groupe de Mumford-Tate). Il en résulte que $X_*(M) \otimes \mathbb{Q} \subset X_*(T) \otimes \mathbb{Q}$ est égal à $V_1^+ \oplus V_1^- \oplus V^-_{n-1}$ ou à $V_1^+ \oplus V^-_{n-1}$. Le second module correspond au sous-tore T_1 de T défini par

$$T_1(\mathbb{Q}) = \{z \in E^\times : N_{E/F} z \in \mathbb{Q}^\times, N_{E/E_0} z \in \mathbb{Q}^\times\}.$$

Si $z \in T_1(\mathbb{R}) \subset S(\mathbb{R})$ s'écrit (z_i) avec $z_i \in E^\times_{w_i} \cong \mathbb{C}^\times$ (3.4), les relations définissant T_1 donnent alors :

$$z_i \bar{z}_i = x \in \mathbb{R}^\times \tag{3.6}$$

$$z_1 \cdots z_n = y \in \mathbb{R}^\times. \tag{3.7}$$

Revenons à l'expression (3.5) de h : h vérifie (3.6), et (3.7) si, et seulement si, $p = q$. On a donc démontré :

Lemme 3.1 *Si $p \neq q$, T est égal à son groupe de Mumford-Tate. Si $p = q$, le groupe de Mumford-Tate d'un paramètre h passant par T est égal à T_1.*

Soit K le corps reflex de μ, donc $K \subset E^{\rm gal}$. Un calcul simple montre que $\mathrm{Gal}(E^{\rm gal}/K) = \mathfrak{S}_p \times \mathfrak{S}_q \subset \mathfrak{S}_n$ si $p \neq q$, et que $\mathrm{Gal}(E^{\rm gal}/K)$ est le produit semi-direct de $\mathfrak{S}_p \times \mathfrak{S}_p$ avec $\{1, c\}$ si $p = q$.
Supposons maintenant $p \neq q$ $(p, q \geqslant 1)$ et considérons le morphisme de réciprocité

$$r_* : X_*(R) \to X_*(T) = \mathbb{Z}^{n+1} \tag{3.8}$$

où $X_*(R) \cong \mathbb{Z}^{2N}$ $(N = \begin{pmatrix} n \\ p \end{pmatrix})$, et où l'on a utilisé le fait que T est le groupe de Mumford-Tate. Une base de $X_*(R)$ correspond à la réunion des sous-ensembles $I \subset \{1, \dots, n\}$ de cardinal p (action de $\mathfrak{S}_n$) et des sous-ensembles I de cardinal q (action de $\mathfrak{S}_n \times c$). Si e_I sont les éléments de $\mathbb{Z}^n$ donnés par $e_I = \sum_{i \in I} e_i$ dans la base canonique, et si l'on choisit $(n+1)$ éléments $I_1, \dots, I_{n+1}$ ($I_j \subset \{1, \dots, n\}$ de cardinal p ou q), le mineur correspondant de r_* est

$$\det \begin{pmatrix} e_{I_1} & \cdots & e_{I_{n+1}} \\ 1 & \cdots & 1 \end{pmatrix} .$$

Si $(p, q) = (p, n) = r$, on vérifie aisément que ce déterminant est divisible par r (remplacer la première ligne par la somme des n premières lignes). Les résultats du § 2 ne peuvent donc être améliorés.
Considérons, au contraire, le cas où $p = q$ et $n = 2p$. On note toujours T_1 le groupe de Mumford-Tate, de sorte que $T_1 \subset T \subset S$. On a naturellement

$$X_*(T) = \{(\lambda_1, \dots \lambda_n, \lambda_{n+1}, \dots, \lambda_{2n})\} \subset \mathbb{Z}^{2n} = X_*(S)$$

où $\lambda_j + \lambda_{j'} = \lambda \quad (j' = 2n + 1 - j)$; $X_*(T)$ s'identifie donc à $\mathbb{Z}^{n+1} = \{(\lambda_j, \lambda)\}$.
La relation (3.7) définit alors $X_*(T_1) \subset X_*(T)$ par

$$\sum \lambda_j = \sum \lambda_{j'} = \sum (\lambda - \lambda_j)$$

donc $X_*(T_1)$ est défini par $\{(\lambda_j, \lambda) : 2 \sum \lambda_j = 2p\lambda\}$ soit enfin

$$\begin{aligned} X_*(T_1) &= \{(\lambda_j, \lambda) : \sum_1^n \lambda_j = p\lambda\} \\ &\cong \mathbb{Z}^{2p-1} \times \mathbb{Z} \end{aligned}$$

par les coordonnées $((\lambda_j)_{j \leqslant 2p-1}, \lambda)$.
Pour tout $I \subset \{1, \dots 2p - 1\}$ de cardinal p, l'image de $X_*(R)$ dans $X_*(T_1)$ contient, avec la notation précédente, le vecteur $(e_I, 1)$; si $I' \subset I$ est de cardinal $p - 1$, elle contient aussi $(e_{I'}, 1)$: remplacer I par $I' \cup \{n\}$. Donc l'image

contient les vecteurs $(e_i, 0)$ $(i = 1, \dots 2p-1)$ ainsi qu'un vecteur quelconque $(e_I, 1)$. Puisque le déterminant d'ordre $2p$

$$\begin{pmatrix}
1 & & & & & & & 1 \\
& 1 & & & & & & 1 \\
& & \ddots & & & & & \vdots \\
& & & \ddots & & & & 1 \\
& & & & \ddots & & & 0 \\
& & & & & \ddots & & \vdots \\
& & & & & & \ddots & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1
\end{pmatrix}$$

est égal à 1, on a démontré :

Proposition 3.2 *Si $G(\mathbb{R})$ est de type (p, p), le noyau de réciprocité est connexe pour les tores maximaux Galois-génériques.*

3.4 Uniformité du conoyau de l'application de réciprocité

Dans cette section nous supposons simplement que (G, X) est une donnée de Shimura vérifiant les conditions de Deligne [4, § 2.1]. Soit $T \subset G$ un tore; on suppose qu'il existe un élément de X $h : \mathbb{S} \to T_{\mathbb{R}}$ et que T est le groupe de Mumford-Tate de h. Soit E le corps reflex, $R = \mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m$ et

$$\mathrm{rec} : R \to T$$

le morphisme de réciprocité.
Si T est un tore, $\pi_0(T(\mathbb{A})/T(\mathbb{Q}))$ est son groupe de composantes connexes, qui s'identifie à $\pi_0(T(\mathbb{R})) \times T(\mathbb{A}_f)/T(\mathbb{Q})^-$ (adhérence topologique). On notera simplement $\pi(T)$ le groupe $T(\mathbb{A}_f)/T(\mathbb{Q})^-$, modifiant un peu la notation de Deligne.
Si $T \to S$ est un morphisme de $\mathbb{Q}$-tores tel que l'application $T(\mathbb{A})/T(\mathbb{Q}) \to S(\mathbb{A})/S(\mathbb{Q})$ soit de conoyau fini, il en est de même de l'application induite au niveau des composantes connexes ; si l'on dispose, pour une famille de tores, d'une borne universelle pour l'ordre du conoyau, il en est de même pour l'application induite.
Le groupe $\pi_0(R(\mathbb{R})) \times \pi(R)$ s'identifie, par la théorie du corps de classes, au groupe $\mathrm{Gal}(E^{ab}/E)$. Rappelons que le composé

$$\mathrm{Gal}(E^{ab}/E) \to \pi(R) \overset{\mathrm{rec}}{\to} \pi(T)$$

décrit l'action du groupe de Galois abélien sur les points z des variétés de Shimura $S_K(G, X)$ $(K \subset G(\mathbb{A}_f))$ déduits de h ([4 ,p. 269]; § 4).
Dans l'énoncé suivant, $h : \mathbb{S} \to G_{\mathbb{R}}$ varie parmi les paramètres CM; T est le groupe de Mumford-Tate associé; R est le tore associé au corps reflex $E = E(h)$.

Théorème 3.3 *Si (h,T) varie parmi les sous-données CM de (G,X) telles que le noyau*

$$U=\ker(\mathrm{rec}:R\to T)$$

est connexe, le conoyau de rec : $\pi(R)\to\pi(T)$ *est de taille uniformément bornée.*

Noter que si G est adjoint, $T(\mathbb{R})$ est compact et connexe et l'application de réciprocité envoie $\mathrm{Gal}(E^{ab}/E)$ vers $T(\mathbb{A}_f)/T(\mathbb{Q})$.
Pour la démonstration, on utilise la description de la dualité de Tate-Nakayama donnée par Kottwitz et Shelstad [9]. Considérons la suite exacte

$$1\to U\to R\underset{\mathrm{rec}}{\to}T\to 1 \tag{3.9}$$

Puisque U est un tore, elle se scinde sur $\bar{\mathbb{Q}}$; avec les notations de [9] on en déduit une suite exacte

$$1\to U(\bar{\mathbb{A}})/U(\bar{\mathbb{Q}})\to R(\bar{\mathbb{A}})/R(\bar{\mathbb{Q}})\to T(\bar{\mathbb{A}})/T(\bar{\mathbb{Q}})\to 1\ . \tag{3.10}$$

Si X est un module continu sur $\mathfrak{g}_{\mathbb{Q}}=\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, on écrira simplement $H^\bullet(\mathbb{Q},X)$ pour $H^\bullet_{ct}(\mathfrak{g}_{\mathbb{Q}},X)$. Alors (3.9) donne

$$H^0(\mathbb{Q},R(\bar{\mathbb{A}})/R(\bar{\mathbb{Q}}))\to H^0(\mathbb{Q},T(\bar{\mathbb{A}})/T(\bar{\mathbb{Q}}))\to H^1(\mathbb{Q},U(\bar{\mathbb{A}})/U(\bar{\mathbb{Q}})). \tag{3.11}$$

Le dernier terme de (3.11) est dual de $H^1(\mathbb{Q},X^*(U))$ donc fini ([9, p. 621]) ; noter que le terme suivant est $H^1(\mathbb{Q},X^*(R))^\vee=H^1(E,\mathbb{Z})^\vee=\{0\}$ d'après le lemme de Shapiro, donc (3.11) est surjective à droite.
Par ailleurs, pour tout tore T sur $\mathbb{Q}$, la suite exacte

$$1\to T(\bar{\mathbb{Q}})\to T(\bar{\mathbb{A}})\to T(\bar{\mathbb{A}})/T(\bar{\mathbb{Q}})\to 1$$

donne

$$1\to T(\mathbb{A})/T(\mathbb{Q})\to H^0(\mathbb{Q},T(\bar{\mathbb{A}})/T(\bar{\mathbb{Q}}))\to H^1(\mathbb{Q},T)\to H^1(\mathbb{Q},T(\bar{\mathbb{A}}));$$

avec les notations de [9], cf. en particulier [9, 3.4.3], si on note $H^1(\mathbb{Q},T(\bar{\mathbb{A}}))=\bigoplus_{p,\infty}H^1(\mathbb{Q}_v,T(\bar{\mathbb{Q}}_v))$ alors

$$\ker^1(\mathbb{Q},T)=\ker[H^1(\mathbb{Q},T)\to H^1(\mathbb{Q},T(\bar{\mathbb{A}})],$$

est le groupe de Shafarevich-Tate, fini pour un tore. Réécrivons donc la suite exacte précédente comme

$$1\to T(\mathbb{A})/T(\mathbb{Q})\to H^0(\mathbb{Q},T(\bar{\mathbb{A}})/T(\bar{\mathbb{Q}}))\to\ker^1(\mathbb{Q},T)\to 1\ . \tag{3.12}$$

Le morphisme de suites exactes (3.12) appliquées aux groupes R et T de (3.9) donne un diagramme

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d] & A' \arrow[r] \arrow[d] & A'' \arrow[r, dashed] \arrow[d] & {} \\
1 \arrow[r] & R(\mathbb{A})/R(\mathbb{Q}) \arrow[r] \arrow[d] & H^0(\mathbb{Q}, R(\bar{\mathbb{A}})/R(\bar{\mathbb{Q}})) \arrow[r] \arrow[d] & \ker^1(\mathbb{Q}, R) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & T(\mathbb{A})/T(\mathbb{Q}) \arrow[r] \arrow[d] & H^0(\mathbb{Q}, T(\bar{\mathbb{A}})/T(\bar{\mathbb{Q}})) \arrow[r] \arrow[d] & \ker^1(\mathbb{Q}, T) \arrow[r] \arrow[d] & 1 \\
{} \arrow[r, dashed] & B \arrow[r] & B' \arrow[r] & B'' \arrow[r] & 1
\end{tikzcd}$$

où d'ailleurs $A'' = \ker^1(\mathbb{Q}, R) = \{1\}$ d'après le théorème 90 de Hilbert. D'après (3.11),

$$B' = H^1(\mathbb{Q}, U(\bar{\mathbb{A}})/U(\bar{\mathbb{Q}})) = H^1(\mathbb{Q}, X^*(U))^\vee$$

(dualité de Pontryagin); $B'' = \ker^1(\mathbb{Q}, T)$ et le conoyau B du morphisme de réciprocité s'identifie donc à

$$\ker[H^1(\mathbb{Q}, X^*(U))^\vee \to \ker^1(\mathbb{Q}, T)]. \tag{3.13}$$

B est donc fini, les deux groupes figurant dans (3.13) l'étant; pour borner uniformément $\# B$, il suffit de borner $\# H^1(\mathbb{Q}, X^*(U))$. Le lemme très simple qui suit est fondamental (cf. [7]).

Lemme 3.4 *Quand h varie parmi les paramètres CM,* $\dim U = \dim R - \dim T$ *est uniformément borné.*

Pour démontrer le Lemme, on n'a pas à supposer la connexité de U. Il suffit bien sûr de borner $\dim R = [E : \mathbb{Q}] =$ cardinal de l'orbite de μ sous $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Le corps reflex est un sous corps du corps de décomposition d'un $\mathbb{Q}$-tore de G donc est de degré uniformément borné par le maximum des cardinaux des sous groupes finis de $GL(s, \mathbb{Z})$ où s désigne le rang de G (considérer l'action de $\mathfrak{g}_{\mathbb{Q}}$ sur le groupe des caractères d'un tore de G) .

Terminons la démonstration du Théorème. On considère $H^1(\mathbb{Q}, X^*(U)) \cong H^1(\mathbb{Q}, \mathbb{Z}^r)$ où r est borné d'après le Lemme; $\mathfrak{g}_{\mathbb{Q}}$ opère par un sous-groupe fini $\mathfrak{g} \subset \mathrm{GL}(r, \mathbb{Z})$; à conjugaison près le nombre de possibilités pour $\mathfrak{g}$ est fini. Considérons la suite exacte

$$1 \to \mathfrak{h} \to \mathfrak{g}_{\mathbb{Q}} \to \mathfrak{g} \to 1 .$$

Elle donne une suite exacte

$$1 \to H^1(\mathfrak{g}, H^0(\mathfrak{h}, \mathbb{Z}^r)) \to H^1(\mathfrak{g}_{\mathbb{Q}}, \mathbb{Z}^r) \to H^1(\mathfrak{h}, \mathbb{Z}^r)^{\mathfrak{g}}.$$

Le dernier terme, égal aux invariants de $\mathfrak{g}$ dans $\mathrm{Hom}_{ct}(\mathfrak{h}, \mathbb{Z}^r)$, est trivial. Le premier est égal à $H^1(\mathfrak{g}, \mathbb{Z}^r)$. Puisque le nombre de sous-groupes $\mathfrak{g}$, munis de leur plongement, à conjugaison près, dans $\mathrm{GL}(r, \mathbb{Z})$, est fini il n'y a qu'un nombre fini de possibilités.

4 Une conséquence géométrique

4.1

Soient G un groupe réductif sur $\mathbb{Q}$, X une classe de conjugaison de morphismes $\mathbb{S} \to G_{\mathbb{R}}$, vérifiant les conditions de Deligne [4, 2.1]. Soient $K \subset G(\mathbb{A}_f)$ et $S = S_K(G,X)$ la variété associée.
Si E_0 est le corps de rationalité de la classe de conjugaison de $\mu : \mathbb{G}_m \to G$ déduit d'un élément arbitraire $h \in X$, la théorie des modèles canoniques définit S sur E_0. (Pour un exposé des résultats finaux, voir Milne [11]).
Soit $h : \mathbb{S} \to T$ un point CM, T étant le groupe de Mumford-Tate. Le corps reflex $E = E(h,T)$ contient E_0. Dans ce qui suit, on notera souvent x le point de X défini par (égal à) h. Si $(x,g) \in X \times G(\mathbb{A}_f)$ on note $[x,g]$ sa classe dans S_K. L'action de $\mathrm{Gal}(E^{ab}/E)$ sur x est décrite par le morphisme de réciprocité [§ 3.4].
Soit S^+ la composante connexe de l'image de $X^+ \times 1$ dans S, où l'on a fixé une composante connexe X^+ de X. On considère une sous-variété fermée $Z \subset X^+$. On dit que Z est Hodge-générique si Z n'est pas contenue dans une sous-variété de type Hodge propre [3] de S^+.
Fixons un domaine fondamental $\mathcal{F} \subset X^+$ pour l'action de $\Gamma = G(\mathbb{Q}) \cap K$. Si $z \in S^+$ et si $x \in \mathcal{F}$ relève z, on note $MT(z) \subset G$ le groupe de Mumford-Tate de x.

Proposition 4.1 *Supposons Z Hodge-générique et que G est le groupe de Mumford-Tate générique de X. Si H est un sous-groupe connexe propre de G défini sur $\mathbb{Q}$, l'ensemble des points $CM\{z \in Z : MT(z) \subset H\}$ n'est pas Zariski-dense dans Z.*

La condition que G est le groupe de Mumford-Tate générique est nécessaire (prendre H le groupe de Mumford-Tate générique). On peut en fait supposer que G est adjoint. Soit en effet $\pi : G \to G^{ad}$ le morphisme canonique et H un sous-groupe propre connexe de G tel que l'ensemble des points $CM\{z \in Z : MT(z) \subset H\}$ soit Zariski-dense dans Z. La proposition pour la donnée adjointe (G^{ad}, X^{ad}) nous assure que $\pi(H) = G^{ad}$ donc que $H^{der} = G^{der}$. L'hypothèse que G est Hodge générique assure alors que $H = G$.
On suppose donc G de type adjoint. Fixons $H \subsetneq G$ sur $\mathbb{Q}$ et soit (z_α) une suite Zariski-dense de Z telle que $MT(z_\alpha) \subset H$.

Lemme 4.2 *$H_{\mathbb{Q}}$ est réductif.*

Soit en effet $H_{\mathbb{Q}} = N\ H'_{\mathbb{Q}}$, où N est unipotent et $H'_{\mathbb{Q}}$ est réductif, une décomposition de Levi. Puisque $MT(z_\alpha)$ est un tore on peut choisir cette décomposition de sorte que $MT(z_\alpha) \subset H'_{\mathbb{Q}}$. Alors $Z_G(H'(\mathbb{R})) \subset Z_G(h_\alpha(\sqrt{-1}))$ où $h_\alpha : \mathbb{S} \to G$ est associé à x_α, donc $Z_G(H'(\mathbb{R}))$ est compact. En particulier H' n'admet pas de caractère rationnel non trivial. Rappelons un lemme d'Eskin, Mozes et Shah [6, Lemme 5.1].

Lemme 4.3 *Soit $F \subset G$ un $\mathbb{Q}$-sous-groupe sans caractère non trivial. Les propriétés suivantes sont équivalentes.*

(i) *$Z_G(F)$ est anisotrope (réductif).*

(ii) *Tout $\mathbb{Q}$-sous-groupe de G contenant F est réductif.*

Appliquant le Lemme à H' on en déduit que $H = H'$ est réductif.
Revenant à la démonstration de la Proposition, soit

$$H = S\ H_1 \cdots H_r$$

(produit quasi-direct) où S est un tore – tel que $S(\mathbb{R})$ est compact – et les H_i sont semi-simples et irréductibles sur $\mathbb{Q}$. Soit π_i la projection de H sur $H/S \prod_{j \neq i} H_j$. On peut supposer dans cette démonstration que $\pi_i \circ h_\alpha \neq 1$ pour tout i.

Lemme 4.4 *Pour tout $\alpha \in \mathbb{N}$ soit X_α la $H(\mathbb{R})$-classe de conjugaison de h_α; donc $X_\alpha \subset X$.*

(i) *(H, X_α) est une sous-donnée de Shimura de (G, X).*

(ii) *Pour α variable il n'y a qu'un nombre fini de possibilités pour X_α.*

Pour les définitions précises relatives aux données et sous-données de Shimura on renvoie à [2].
La partie (i) est une variante de [2, Prop. 3.2]. Fixons α tel que $MT(x_\alpha) \subset H$. Si $C = h_\alpha(\sqrt{-1})$, C est de carré central dans $H(\mathbb{R})$. Alors $\mathrm{Lie}(G/\mathbb{R})$ définit une représentation fidèle et C-polarisable de $H_\mathbb{R}$, selon la terminologie de Deligne; d'après celui-ci [4, 1.1.15] $\mathrm{Int}(C)$ est une involution de Cartan de $H(\mathbb{R})$. Par ailleurs $G(\mathbb{R})$ opère fidèlement sur $\mathfrak{g}_\mathbb{C} = \mathrm{Lie}(G/\mathbb{C}) = k_\mathbb{C} \oplus \mathfrak{p}_\mathbb{C} \oplus \bar{\mathfrak{p}_\mathbb{C}}$, $z \in \mathbb{C}^\times = \mathbb{S}(\mathbb{R})$ opérant par $(1, z/\bar{z}, \bar{z}/z)$ via h_α et C par $(1, -1, -1)$. Puisque $\pi_i \circ h_\alpha \neq 1$, $h_\alpha(z)$ n'opère pas trivialement sur $\mathrm{Lie}(H_i)$ par l'action adjointe. Il en résulte que C n'est pas triviale sur $H_i(\mathbb{R})$. Enfin, la représentation de $\mathbb{S}$ sur $\mathrm{Lie}(H/\mathbb{R})$ est de type $(0; (1, -1); (-1, 1))$ comme sous-représentation de $\mathrm{Lie}(G/\mathbb{R})$. Ainsi (H, X_H) vérifie les conditions d'une sous-donnée de Shimura [3, 3.1].
Pour la partie (ii), noter tout d'abord qu'il n'y a qu'un nombre fini de possibilités pour les classes de conjugaison géométrique des $h_\alpha : \mathbb{S} \to H/\mathbb{C}$ par $H(\mathbb{C})$. Si $h : \mathbb{S} \to H/\mathbb{R}$ est donnée, et si $L \subset H$ est le stabilisateur de h pour la conjugaison, le nombre de classes de conjugaison réelles de h dans le classe de h sous $H(\mathbb{C})$ est $\# \ker((H^1(\mathbb{R}, L) \to H^1(\mathbb{R}, H))$ donc fini.
Complétons la démonstration de la Proposition 4.1. On peut supposer donnée (z_α) telle que z_α soit défini par $x_\alpha \in X^+$ et que la donnée (H, X_α) soit constante; notons X_H la classe X_α. Alors pour tout α, z_α est donné par $[x_\alpha, 1] \in S_{K^+}$, qui est contenu dans l'image de $Sh_{K \cap H(\mathbb{A}_f)}(H, X_H) = H(\mathbb{Q}) \backslash X_H \times H(\mathbb{A}_f)/K \cap H(\mathbb{A}_f)$. Pour un sous-ensemble Zariski-dense de Z,

z_α est donc contenu dans une composante irréductible d'une sous-variété de Shimura, i.e., une variété de type Hodge. Donc Z est contenu dans cette sous-variété, contrairement à l'hypothèse.
On déduit aussitôt de la Proposition :

Corollaire 4.5 *Soit Z une sous-variété Hodge-générique. Supposons que Z contient une suite dense de points $CM, (z_\alpha)$, et soit $T_\alpha = MT(z_\alpha)$. Alors Z contient une suite Zariski-dense de points $CM, (z_\beta)$, tels que la suite (T_β) soit stricte.*

En effet Z, contenant un ensemble dense D de points algébriques, est définie sur $\bar{\mathbb{Q}}$; les adhérences de Zariski des sous-ensembles de D sont définies sur $\bar{\mathbb{Q}}$ et donc forment un ensemble dénombrable. Si l'on ordonne, $Z_1, Z_2, \dots Z_k, \dots$ ces adhérences $\neq Z$ on peut trouver une suite extraite (z_{α_j}) telle que $z_{\alpha_j} \notin Z_k$ $(j \geqslant k)$. Alors, pour tout $H \underset{\neq}{\subset} G$, $T_{\alpha_j} \not\subset H$, si j est assez grand, d'après la Proposition.

4.2

Avec les hypothèses énoncées au début du § 4.1, et G étant adjoint, soit alors $Z \subset S^+$ une sous-variété Hodge-générique contenant une suite dense de points CM. On en extrait une sous-suite, qu'on notera simplement (z_α), ayant la propriété du Corollaire 4.5.
Supposons pour l'instant que Z est définie sur E_0, et que la suite T_α associée à z_α est telle que rec : $\pi(R_\alpha) \to \pi(T_\alpha)$ soit surjective (cf. Thm. 3.3 ; les notations sont évidentes). Noter que ceci apparaît par exemple dans un des exemples traités à la fin du § 3.2. Puisque $z_\alpha \in S^+$ on peut écrire

$$z_\alpha = [x_\alpha, 1] \in Z \ . \tag{4.1}$$

Alors x_α définit le tore T_α; sous notre hypothèse de surjectivité, on a alors

$$[x_\alpha, t] \in Z \quad \forall t \in T_\alpha(\mathbb{A}_f)/T_\alpha(\mathbb{Q}) \tag{4.2}$$

Notons $\tilde{S}_K(G)$ ou simplement $\tilde{S}$, l'espace $G(\mathbb{R})$-homogène $G(\mathbb{Q})\backslash G(\mathbb{A})/K$. On notera $[[g_\infty, g]]$ la classe d'un élément $(g_\infty, g) \in G(\mathbb{R}) \times G(\mathbb{A}_f)$. Enfin, $\tilde{S}^+$ est la composante connexe de (la classe de) 1 dans $\tilde{S}$.
Supposons alors l'hypothèse $\mathcal{E}_a$ (§ 1) vérifiée pour la famille T_α, et soit $g_\infty \in G(\mathbb{R})^+$. La convergence de la suite de mesures implique évidemment, pour tout α, la densité de

$$\bigcup_{\beta \geqslant \alpha} \tilde{S}^+(T_\beta, K_\beta)$$

dans $\tilde{S}^+$, avec $K_\beta = K \cap T_\beta(\mathbb{A}_f)$.
En particulier

$$[[g_\infty, 1]] = \lim_\alpha [[t_\alpha^\infty, t_\alpha]]$$

où $(t_\alpha^\infty, t_\alpha) \in T_\alpha(\mathbb{A})$ et la convergence est dans $\tilde{S}^+$. On en déduit qu'il existe une suite $\gamma_\alpha \in G(\mathbb{Q})$ telle que

$$\gamma_\alpha(t_\alpha^\infty, t_\alpha) \to (g_\infty, 1)$$

dans $G(\mathbb{R}) \times G(\mathbb{A}_f)/K$. Le second facteur étant discret, ceci veut dire que

$$\begin{cases} \gamma_\alpha \; t_\alpha^\infty \to g_\infty \; , \\ \gamma_\alpha \; t_\alpha \in K \qquad\quad (\alpha >> 0). \end{cases} \tag{4.3}$$

Par ailleurs d'après (4.2)

$$[\gamma_\alpha \; x_\alpha, \gamma_\alpha \; t_\alpha] \in Z \; .$$

Si $\gamma_\alpha \; t_\alpha \in K$, on a donc

$$[\gamma_\alpha \; x_\alpha, \gamma_\alpha \; t_\alpha] = [\gamma_\alpha \; x_\alpha, 1] \in Z \; .$$

Mais t_α^∞ appartient au centralisateur de $x_\alpha := h_\alpha$, donc

$$[\gamma_\alpha \; t_\alpha^\infty \; x_\alpha, 1] \in Z \; . \tag{4.4}$$

Supposons alors que la suite (z_α) admet une sous-suite convergente dans S^+. On peut alors choisir le relèvement x_α de (4.1) convergent dans X^+ en choisissant un domaine fondamental comme dans le § 4.1. Soit donc $x_\alpha \to x_\infty \in X^+$. Alors $\gamma_\alpha \; t_\alpha^\infty \; x_\alpha \to g_\infty \; x_\infty \in X^+$ et (4.4) implique $[g_\infty \; x_\infty, 1] \in Z$. Puisque g_∞ était arbitraire, ceci implique que $S^+ \subset Z$. (Noter que X^+ étant connexe est une orbite de $G(\mathbb{R})^+$).

Nous supposons maintenant que G est adjoint, Z Hodge-générique dans S^+; soit E' un corps de rationalité de Z, et supposons seulement que les conoyaux de rec : $\pi(R_\alpha) \to \pi(T_\alpha)$ sont uniformément bornés. Pour tout α, l'image de $\mathrm{Gal}(E_\alpha^{ab}/E_\alpha E')$ (où E_α est le corps reflex du tore T_α) est un sous-groupe d'indice uniformément borné dans $\pi(T_\alpha)$. Notons $\bar{T}_\alpha^0$ ce sous-groupe de $\bar{T}_\alpha = T_\alpha(\mathbb{A}_f)/T_\alpha(\mathbb{Q})$. L'argument qui précède donne alors :

Lemme 4.6 *Supposons $g_\infty \in G(\mathbb{R})^+$, et*

(i) $x_\alpha \to x_\infty \in X$

(ii) $[[g_\infty, 1]] = \lim[[h_\alpha^\infty, h_\alpha]])$

avec $h_\alpha \in T_\alpha(\mathbb{A}_f)$ d'image contenue dans $\bar{T}_\alpha^0$. Alors $[g_\infty x_\infty, 1] \in Z$.

Notons alors $\tilde{Z} \subset \tilde{S}^+$ l'image inverse de Z par l'application $\tilde{S}^+ \to S$,

$$[[g_\infty, 1]] \to [g_\infty x_\infty, 1].$$

Cette application est une submersion, donc $\tilde{Z}$ est une sous-variété (différentielle) de $\tilde{S}^+$, sous-variété propre si $Z \neq S^+$.

Considérons par ailleurs les plongements

$$(T_\alpha(\mathbb{Q})\backslash T_\alpha(\mathbb{A})/K_\alpha)^+ \to (G(\mathbb{Q})\backslash G(\mathbb{A})/K)^+ = \tilde{S}^+ \tag{4.5}$$

(notations du § 1 : le terme de gauche est l'ensemble des éléments du quotient dont l'image est dans $\tilde{S}^+$). D'après la loi de réciprocité des modèles canoniques pour les composantes connexes de S_K (Deligne [4]) le groupe $G(\mathbb{A}_f)$ opère sur les composantes connexes de $\tilde{S}$ via l'action transitive d'un quotient abélien. On en déduit que la composante (+) du membre de gauche de 4.5 est un sous-groupe. Il contient un sous-groupe ouvert d'indice fini, l'image de $\bar{T}^0_\alpha$, et l'indice de cette image est uniformément borné.
Si $\mu_{a,\alpha}$ est la mesure de Haar du membre de gauche de (4.5), identifiée à son image sur $\tilde{S}^+$, l'hypothèse $(\mathcal{E}_a)$ est

$$\mu_{a,\alpha} \to \mu_G \ ; \tag{4.6}$$

quitte à supposer l'indice de l'image de $\bar{T}^0_\alpha$ constant, égal à r, on peut écrire

$$\mu_{a,\alpha} = \sum_{i=1}^{r} \mu^i_\alpha$$

où $r\ \mu^1_\alpha$ est la mesure de Haar normalisée sur cette image, et $\mu_{a,i}$ est positive de masse $\frac{1}{r}$.
Soit alors f une fonction continue à support compact, telle que $f(x) \leqslant 1$ $(x \in \tilde{S}^+)$, $f(x) = 0$ $(x \in \tilde{Z})$ et $\mu_G(f) = 1 - \varepsilon$. Si $\mu^1_\alpha(f) \neq 0$ pour une suite infinie de α, Supp(f) doit rencontrer $\tilde{Z}$ d'après le Lemme 4.6. On a donc $\mu^1_\alpha(f) = 0$ $(\alpha >> 0)$ et donc

$$\mu_{a,\alpha}(f) = \sum_{2}^{r} \mu^i_\alpha(f) \leqslant \frac{r-1}{r}$$

ce qui contredit (4.6) pour $\varepsilon < \frac{1}{r}$. On a ainsi démontré le théorème suivant dans le cas où $Z \subset S^+$; le cas général s'en déduit de la façon usuelle en translatant Z par un élément de $G(\mathbb{A}_f)$.

Théorème 4.7 (*G adjoint*).
Soit Z une sous-variété de $S = S_K(G,h)$ et supposons :

(i) *Z contient un sous-ensemble Zariski-dense de points CM (z_α) dont le groupe de Mumford-Tate T_α vérifie :*

$$\ker(\mathrm{rec} : \pi(R_\alpha) \to \pi(T_\alpha)) \ \textit{est connexe.}$$

(ii) *(z_α) contient une sous-suite convergente pour la topologie complexe.*

(iii) *Z est Hodge-générique.*

Alors, SOUS L'HYPOTHÈSE $\mathcal{E}_a$ *pour les groupes* $T_\alpha \subset G$*,* Z *est une composante connexe de* S*.*

D'après les § 2-3, l'hypothèse (i) sera très souvent vérifiée si Z contient un ensemble dense de points CM Galois-génériques.

Pour terminer (et pour justifier notre § 3.3), notons que l'hypothèse "G adjoint", si elle est commode, n'est pas cruciale. Expliquons l'argument quand G est un groupe de similitudes (de type (p,p) à l'infini, cf. § 3.3) et quand les points z_α sont Galois génériques. Soit E_0 le corps quadratique imaginaire associé à G. On notera ici $\underline{E}_0^\times$ le $\mathbb{Q}$-tore $\mathrm{Res}_{E_0/\mathbb{Q}}\, \mathbb{G}_m$.

Le tore $T = T_\alpha$ est décrit par $T(\mathbb{Q}) = \{z \in E^\times : N_{E/F}\, z \in \mathbb{Q}^\times, N_{E/E_0}\, z \in \mathbb{Q}^\times\}$. Le centre Z de G s'identifie à $\underline{E}_0^\times \supset \mathbb{G}_m$. Soit $\bar{G} = G/\mathbb{G}_m$: on a donc des morphismes naturels

$$G \to \bar{G} \to G^{ad}.$$

Pour des choix de compacts naturels, les variétés de Shimura associées sont identiques (sur $\mathbb{C}$). Si (z_α) est une suite de points de $S_K(G)$, dense dans une variété Hodge-générique, un sous-groupe $H \subset G$ contenant les T_α doit être d'image totale dans G^{ad}. Son image dans $\bar{G}$ doit donc être $\bar{G}$ ou le groupe dérivé de celui-ci. Mais la composante neutre de l'image inverse dans G de $\bar{G}^{\mathrm{der}}$ est G^{der}, avec $G^{\mathrm{der}}(\mathbb{R}) \cong \mathrm{SU}(p,p)$ et le paramètre $h : z \mapsto (z, \dots z, \bar{z}, \dots \bar{z})$ ne passe pas par ce sous-groupe. Par conséquent les arguments du § 4.1 s'appliquent à $\bar{G}$.

Rappelons que la conjecture d'équidistribution n'est naturelle que pour les groupes de type $(\mathcal{F})$, ce qui exclut G à cause de son centre déployé. On procède donc dans $\bar{G}$, de centre $\underline{E}_0^\times/\mathbb{G}_m$. Les arguments du § 4.1 s'étendent : il reste donc à vérifier l'essentielle surjectivité des applications $\pi(R) \to \pi(\bar{T})$ ($\bar{T} \subset \bar{G}$ Galois-générique).

Si $\mu : \mathbb{G}_m \to T \to \bar{T}$ est un paramètre Galois-générique, on vérifie tout d'abord que le corps reflex coïncide dans T et $\bar{T}$. Ceci résulte immédiatement de la trivialité de $H^1(\mathbb{Q}, \mathbb{G}_m)$ où $\mathbb{G}_m = \ker(T \to \bar{T})$. Considérons alors le diagramme

$$\begin{tikzcd}
1 \arrow[r] & 1 \arrow[r] \arrow[d] & R \arrow[r, equal] \arrow[d] & R \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & T \arrow[r] & \bar{T} \arrow[r] & 1\,.
\end{tikzcd}$$

On en déduit une suite exacte

$$1 \to \ker(R \to T) \to \ker(R \to \bar{T}) \to \mathbb{G}_m \to 1\ ;$$

puisque les deux termes extrêmes sont connexes, il en est de même du terme médian.

Bibliographie

[1] N. Bourbaki, *Groupes et algèbres de Lie* (Ch. VII-VIII), Hermann, Paris, 1975.

[2] L. Clozel, E. Ullmo, *Equidistribution de sous-variétés spéciales*, Ann. of Math 161 (2005), 1571-1588.

[3] L. Clozel, E. Ullmo, *Equidistribution de mesures algébriques*, Compositio Math 141 (2005), 1255-1309.

[4] P. Deligne, *Variétés de Shimura : Interprétation modulaire, et techniques de construction de modèles canoniques*, in Automorphic forms, Representations and L-functions (Borel, Casselman eds.), Proc. Symp. Pure Math. XXXIII 33 (Part II), Providence, R.I. 1979, 247-290.

[5] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Inv. Math. 92 (1988), 73-90.

[6] A. Eskin, S. Mozes, N. Shah, *Non divergence of translates of certain algebraic measures*, Geom. Funct. Analysis 7 (1997), 48-80.

[7] B. Edixhoven, A. Yafaev, *Subvarieties of Shimura varieties*, Ann. of Math. (2) 157 (2003), 621-645.

[8] R. Kottwitz, *Points on some Shimura varieties over finite fields*, J. A. M. S. 5 (1992), 373-444.

[9] R. Kottwitz, D. Shelstand, *Foundations of twisted endoscopy*, Astérisque 255, Paris, S.M.F., 1999.

[10] S. Lang, *Fundamentals of diophantine geometry*, Springer 1983.

[11] J.S. Milne, *Shimura varieties and motives*, in Motives, Jannsen, Kleiman, Serre eds., Proc. Symp. Pure Math. 55 vol. II, AMS, Providence 1994, 447-524.

[12] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Academic Press, 1994.

[13] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Math., Vieweg & Sohn, Braunschweig, 1989.

[14] J.-P. Serre, *Groupes algébriques associés aux modules de Hodge-Tate*, Astérisque 65 (1969), 155-188 [= Oeuvres, vol. III, 469-502].

[15] V.E. Voskresenskii, *Maximal tori without effect in semi-simple algebraic groups*, Math. Notes 44 (1988), 651-655. [russe : Mat. Zametki 44 (1988), 309-318].

[16] S.-W. Zhang, *Equidistribution of CM points on quaternion Shimura varieties*, preprint.

L. Clozel
UMR 8628 du CNRS
Mathématique Bât 425
Univesité Paris Sud
91405 Orsay
France
laurent.clozel@math.u-psud.fr

E. Ullmo
UMR 8628 du CNRS
Mathématique Bât 425
Univesité Paris Sud
91405 Orsay
France
Emmanuel.Ullmo@math.u-psud.fr

Fake CM and the Stable Model of $X_0(Np^3)$

Robert Coleman[1] and Ken McMurdy

Received: September 11, 2005
Revised: October 5, 2006

Abstract. We complete the determination of the stable model of $X_0(Np^3)$, $p \geq 5$, $(N,p) = 1$ begun in [CMc] and compute the inertial action on the stable reduction of $X_0(p^3)$.

2000 Mathematics Subject Classification: Primary 11G18; Secondary 14G22, 11G07
Keywords and Phrases: stable reduction, modular curve

1 Introduction

In [CMc] we found a stable model for the modular curve, $X_0(p^3)$, over the ring of integers in $\mathbb{C}_p$, for a prime $p \geq 13$. The stable models of $X_0(p)$ and $X_0(p^2)$ were previously known, due to work of Deligne-Rapoport and Edixhoven (see [CMc, §1] for a more complete list of relevant results). Finding a stable model for $X_0(p^n)$ for $n > 3$ remains an open problem, although a conjectural stable model for $X_0(p^4)$ is given in [M2, §5].

The results and main ideas of the argument used in [CMc] are summarized below in Section 2. Nevertheless, we still refer to [CMc] frequently, and do recommend that it be read first. Indeed, the purpose of this paper is to refine and extend those results. First, we prove results which enable us to define our model over an explicit finite extension of $\mathbb{Q}_p$, and to compute the inertia action on the stable reduction. More precisely, we show that a stable model for $X_0(p^3)$ can be defined over any field over which a stable model for $X_0(p^2)$ exists, and which contains the j-invariants of all elliptic curves whose formal groups have endomorphism rings isomorphic to $\mathbb{Z}_p[p\sqrt{-p}]$ or $\mathbb{Z}_p[p\sqrt{-Dp}]$ for D a non-square (mod p). Such elliptic curves, whose formal groups have endomorphism rings bigger than $\mathbb{Z}_p$, are said to have fake CM. In Section 4, we show that (real) CM points are dense in these fake CM points. Thus we are able to

[1] Supported by NSF grant DMS-0401594

apply the theory of CM elliptic curves when we determine, in Section 5, an explicit field of definition for our model. Once this is done, we compute the action of the inertia group on the stable reduction (in Section 6). This uses the results of Sections 3-5 and the fact (which we show) that the formal groups of elliptic curves with fake CM are relative Lubin-Tate groups as in [dS2]. As a consequence, we show that the extension of $\mathbb{Q}_p^{nr}$ found by Krir in [K], over which the Jacobian of $X_0(p^3)$ has semi-Abelian reduction, is minimal.

We also extend the results of [CMc] in two other ways. In order to do the explicit analysis in [CMc], it was necessary to have an approximation formula for the forgetful map, $\pi_f : X_0(p) \to X(1)$, over some supersingular annulus. Such a formula followed from a result of de Shalit (recalled in Section 2) for any region corresponding to a supersingular elliptic curve $A/\mathbb{F}_p$ whose j-invariant, $j(A)$, does not equal 0 or 1728. By a result of Everett Howe (see [CMc, §10]), one always has such an A as long as $p \geq 13$. So the only nontrivial cases which were left open were the three specific primes: $p = 5$, 7, and 11. This shortcoming of our construction could be resolved by either generalizing de Shalit's result or by adding level structure to the more symmetric deformation space of formal groups studied by Gross-Hopkins in [GH]. We handle the open cases here, however, by applying explicit known formulas (in Section 7). It is our hope that these calculations not only deal with the remaining open cases, but also serve to make the constructions of [CMc] more concrete and understandable. Finally, in Section 8 we extend the result of [CMc] by adding tame level, i.e. we compute the stable reduction of $X_0(Np^3)$ when $(N, p) = 1$. This is done by first viewing $X_0(Np^3)$ as the fiber product of $X_0(N)$ and $X_0(p^3)$ over $X(1)$. We construct semi-stable maps (as in [C2]) which extend both forgetful maps, and prove a lemma which implies that the product of semi-stable maps is semi-stable in this case. Then we compute the reductions of the components of $X_0(Np^3)$ by crossing pairs of components in $X_0(N)$ and $X_0(p^3)$ which have the same image in $X(1)$. Two specific examples are then worked out in some detail.

2 Stable Reduction of $X_0(p^3)$ for $p \geq 13$

In this section we summarize the content of [CMc] and in particular the construction of the stable model of $X_0(p^3)$ for $p \geq 13$. The goal will be to present the main ideas, along with the specific details which pertain directly to the results in this paper.

2.1 Foundations

Over $\mathbb{C}_p$, we may think of points on the modular curve, $X_0(p^n)$, as corresponding to pairs (E, C) where $E/\mathbb{C}_p$ is an elliptic curve and C is a cyclic subgroup of order p^n. One way of studying the p-adic geometry of $X_0(p^n)$ is to study regions where the pair, (E, C), has prescribed properties. The most basic distinction which one can make is whether E has ordinary (including multiplicative) or supersingular reduction, and the geometry of the ordinary region of $X_0(p^n)$ is well understood. Indeed, if E is an elliptic curve with ordinary reduction, we define the canonical subgroup $K(E)$ to be the p-power torsion of $E(\mathbb{C}_p)$ in the kernel of reduction. For each $a, b \geq 0$ with $a + b = n$, we then have rigid subspaces of the ordinary locus of $X_0(p^n)$ given by

$$\mathbf{X}_{a\,b} := \{\ (E, C)\ :\ |C \cap K(E)| = p^a\ \}.$$

Then $\mathbf{X}_{a\,b}$ is an affinoid disk when $ab = 0$. Otherwise, it is shown in [C1, §1] that $\mathbf{X}_{a\,b}$ is the disjoint union of two irreducible affinoids, $\mathbf{X}^{\pm}_{a\,b}$, which reduce to the Igusa curve, $Ig(p^c)$, where $c = \min\{a, b\}$. This curve is studied in [Ig] and classifies pairs, (E, α), where $E/\overline{\mathbb{F}}_p$ is an elliptic curve and $\alpha : \mu_{p^c} \hookrightarrow E$ is an embedding.

The supersingular locus is not as well understood, but there are a number of tools which can provide a line of attack. One of the most important is the theory of the canonical subgroup for curves with supersingular reduction, for which we take [B, §3, §4] as our primary reference. When $E/\mathbb{C}_p$ has supersingular reduction, one can still define the canonical subgroup of order p^n, $H_n(E)$, to be the cyclic subgroup of order p^n which is (p-adically) closest to the origin. For each E with supersingular reduction, however, there is a largest n for which $H_n(E)$ exists, and we denote this subgroup by $K(E)$. The size of $K(E)$ is then completely determined by the valuation of the Hasse invariant of $\bar{E}$. Denoting this valuation by $h(E)$, from [B, Thm 3.3, Def 3.4] we have

$$|K(E)| > p^n \iff h(E) < p^{1-n}/(p+1).$$

The theory of canonical subgroups is intimately connected to the geometry of the supersingular region of $X_0(p)$. For a fixed supersingular elliptic curve, $A/\mathbb{F}_{p^2}$, we let $W_A(p^n)$ be the subspace of $X_0(p^n)$ consisting of pairs (E, C) where $\bar{E} \cong A$. It is well-known (from [DR, §VI 6.16], for example) that $W_A(p)$ is an annulus of width $i(A) = |\mathrm{Aut}(A)|/2$. Furthermore, one can choose a parameter x_A on this annulus, which identifies it with $0 < v(x_A) < i(A)$, and such that

$$v(x_A(E, C)) = \begin{cases} i(A)h(E), & \text{if } |C \cap K(E)| = p \\ i(A)(1 - h(E/C)), & \text{if } |C \cap K(E)| = 1. \end{cases}$$

Inside the annulus, $W_A(p)$, there are two circles of fundamental importance. The "too-supersingular circle," denoted $\mathbf{TS}_A$, is where

$$v(x_A(E, C)) = (p/(p+1))i(A)$$

or (equivalently) $K(E)$ is trivial. The self-dual circle, $\mathbf{SD}_A$, consists of all pairs (E, C) where C is potentially self-dual, equivalently those points where $v(x_A(E, C)) = i(A)/2$. When $A/\mathbb{F}_p$, this circle is fixed by the Atkin-Lehner involution, w_1 (recalled below), and hence can be called the "Atkin-Lehner circle."

Another tool for the analysis of the supersingular region of $X_0(p^n)$ is Woods Hole Theory [WH], which essentially says that lifting an elliptic curve is equivalent to lifting its formal group. More precisely, if $R_p \subseteq \mathbb{C}_p$ is the ring of integers, we have the following theorem.

Theorem 2.1. *The category of elliptic curves over R_p is equivalent to the category of triples (F, A, α), where F/R_p is a formal group, $A/\bar{\mathbb{F}}_p$ is an elliptic curve, and $\alpha : \bar{F} \to \hat{A}$ is an isomorphism. A morphism between two triples, (F, A, α) and (F', A', β), is either the* 0 *map or a pair (σ, τ), where $\sigma : F \to F'$ and $\tau : A \to A'$ are isogenies such that the following diagram commutes.*

$$\begin{tikzcd}
\bar{F} \arrow[r, "\bar{\sigma}"] \arrow[d, "\alpha"'] & \bar{F}' \arrow[d, "\beta"] \\
\hat{A} \arrow[r, "\hat{\tau}"'] & \hat{A}'
\end{tikzcd}$$

The theorem is used in two specific ways in [CMc]. First of all, for any two supersingular elliptic curves, A and A', there is an isogeny $\phi : A \to A'$ whose degree is prime to p and which therefore passes to an isomorphism on formal groups. By taking (F, A, α) to $(F, A', \hat{\phi} \circ \alpha)$, we can define a surjection of $W_A(p^n)$ onto $W_{A'}(p^n)$ as long as $i(A) = 1$ (see [CMc, §4.1]). Note that here we have added level structure to Theorem 2.1 in the obvious way. So this implies that all of the supersingular regions are nearly isomorphic, which enables us to analyze $W_A(p^n)$ under the simplifying assumptions that $A/\mathbb{F}_p$ and $j(A) \neq 0, 1728$ (as long as $p \geq 13$, by the result of Howe). In particular, much of our explicit analysis depends on an approximation formula for the forgetful map from the annulus, $W_A(p)$, to the disk, $W_A(1)$. For $A/\mathbb{F}_p$ with $j(A) \neq 0, 1728$, such a formula was essentially found by de Shalit in [dS1, §3]. Let $\pi_f : W_A(p) \to W_A(1)$ denote the forgetful map, and $w_1 : W_A(p) \to W_A(p)$ the Atkin-Lehner involution, given by $\pi_f(E, C) = E$ and $w_1(E, C) = (E/C, E[p]/C)$ respectively. We reformulate de Shalit's result as the following theorem.

Theorem 2.2. *Let $R = W(\mathbb{F}_{p^2})$ and $A/\mathbb{F}_p$ be a supersingular curve with $j(A) \neq 0, 1728$. There are parameters s and t over R which identify $W_A(1)$ with the disk $B(0, 1)$ and $W_A(p)$ with the annulus $A(p^{-1}, 1)$, and series, $F(T), G(T) \in TR[[T]]$, such that*
(i) $w_1^*(t) = \kappa/t$ for some $\kappa \in R$ with $v(\kappa) = 1$.
(ii) $\pi_f^* s = F(t) + G(\kappa/t)$, where
(a) $F'(0) \equiv 1 \pmod{p}$, and
(b) $G(T) \equiv (F(T))^p \pmod{p}$.

The other way we use Woods Hole Theory is by letting $\mathrm{Aut}(\hat{A})$ act on $W_A(p^n)$ in the obvious way (here, as in Theorem 2.1, $\hat{A}$ denotes the formal group of A). From [T], we can identify $\mathrm{End}_{\bar{\mathbb{F}}_p}(\hat{A})$ with $B := \mathbb{Z}_p[i, j, k]$, where $i^2 = -r$ (a non-residue), $j^2 = -p$, and $ij = -ji = k$. When $A/\mathbb{F}_p$, j can also be identified with the Frobenius endomorphism. The action of $B^* \cong \mathrm{Aut}(\hat{A})$

on $W_A(1)$ commutes with the Gross-Hopkins period map, Φ, which can be viewed as a map from $W_A(1)$ to $\mathbf{P}^1$ whenever $j(A) \neq 0, 1728$. Furthermore, for $\alpha, \beta \in \mathbb{Z}_p[i]$ and $\rho = \alpha + j\beta \in B^*$, Gross-Hopkins show in [GH, §25] that the action of B^* on $\mathbf{P}^1$ is given explicitly by

$$\rho(t) = \frac{-p\bar{\beta} + \bar{\alpha}t}{\alpha + \beta t}.$$

It is important to note here that the action of B^* on $W_A(1)$ is then only completely determined by the explicit formula of Gross-Hopkins for B^*-invariant subspaces on which Φ is an injection. Fortunately, the Atkin-Lehner circle, or rather $\pi_f(\mathbf{SD}_A)$, is such a subspace and is identified with the circle described by $v(t) = 1/2$. So as an immediate consequence, the action of B^* induces a faithful action of

$$B^*/\mathbb{Z}_p^*(1 + jB) \cong \mu_{p^2-1}/\mu_{p-1}$$

on $\overline{\mathbf{SD}}_A$ (still when $j(A) \neq 0, 1728$). Also, on $\mathbf{SD}_A$ the involution w_1 can be identified with j in the above sense. We use this in [CMc, §4.2] to show that an involution on $\mathbf{SD}_A$ can be defined by $w_\rho := \rho \circ w_1$, for any $\rho = a + bi + dk \in B^*$ (this subset of B^* is called B').

Remark 2.3. *An affinoid* $\mathbf{X}$ *defined over a complete subfield of* $\mathbb{C}_p$ *has a canonical reduction over the ring of integers, which is what we mean by* $\overline{\mathbf{X}}$. *Later, we adopt the convention of un-bolding affinoid names to refer to associated components of the stable reduction. Thus, whenever both make sense,* $\overline{\mathbf{X}}$ *and* X *are birational but not isomorphic.*

2.2 Stable Model Construction

Our approach to constructing a stable model is purely rigid-analytic, in the sense that we actually construct a stable covering by wide open spaces. This equivalent notion is explained in detail in [CMc, §2]. Roughly, the wide open subspaces in a semi-stable covering intersect each other in disjoint annuli, and have underlying affinoids with (almost) good reduction. Each component in the stable reduction is (almost) the reduction of one of these underlying affinoids, and the annuli of intersection reduce to the ordinary double points where components intersect.

With this rigid analytic reformulation in mind, our strategy for constructing the stable model of $X_0(p^3)$ is basically to construct nontrivial components explicitly and then prove that nothing else interesting can happen (this is done, in part, with a total genus argument). In addition to the components in the ordinary region, we use the above tools to construct three distinct types of components in the supersingular region of $X_0(p^3)$ corresponding to any fixed supersingular elliptic curve, $A/\mathbb{F}_p$, with $j(A) \neq 0$ or 1728. First we consider the affinoid, $\mathbf{Y}_A := \pi_\nu^{-1}(\mathbf{TS}_A) \subseteq W_A(p^2)$, where $\pi_\nu : X_0(p^2) \to X_0(p)$ is given by

$\pi_\nu(E, C) = (E/C[p], C/C[p])$. We show in [CMc, §5] that $\mathbf{Y}_A$ can be identified with the rigid space,

$$T_A := \{\ (x, y) \in \mathbf{TS}_A \times \mathbf{TS}_A \mid x \neq y,\ \pi_f(x) = \pi_f(y)\ \}.$$

Then by applying Theorem 2.2 we compute the reduction of $\mathbf{Y}_A$ explicitly to be $y^2 = x^{p+1} + 1$. This affinoid, $\mathbf{Y}_A$, reduces to the supersingular component which Edixhoven found in [E1, Thm 2.1.1]. It can also be pulled back to $X_0(p^3)$ via π_f and π_ν (defined as above) to obtain nontrivial components of $W_A(p^3)$ (these pullbacks of $\mathbf{Y}_A$ are denoted by $\mathbf{E}_{1\,A}$ and $\mathbf{E}_{2\,A}$). However, there are other nontrivial components as well. Analogous to the above construction, let $\mathbf{Z}_A := \pi_{1\,1}^{-1}(\mathbf{SD}_A) \subseteq W_A(p^3)$, where $\pi_{1\,1} = \pi_f \circ \pi_\nu$. Then $\mathbf{Z}_A$ can be identified with

$$S_A := \{\ (x, y) \in \mathbf{C}_A \times \mathbf{C}_A \mid \tau_f(x) = w_1 \circ \tau_f(y)\ \}.$$

Here $\mathbf{C}_A \subseteq W_A(p)$ is the circle whose points correspond to pairs, (E, C), where $h(E) = 1/2$ and $C \neq H_1(E)$. Then $\tau_f : \mathbf{C}_A \to \mathbf{SD}_A$ is the degree p map which replaces C with $H_1(E)$. The above reformulation of de Shalit's analysis is again sufficient to explicitly compute the reduction of $\mathbf{Z}_A$ (in [CMc, §8]), which is given by

$$X^{p+1} + X^{-(p+1)} = Z^p.$$

Finally, we show that each of the $2(p+1)$ singular residue classes of $\mathbf{Z}_A$ contains an affinoid which reduces to the curve, $y^2 = x^p - x$. We do this by constructing a family of involutions on $\mathbf{Z}_A$, given by $\widetilde{w}_\rho(x, y) = (\rho y, \bar{\rho} x)$ (for $\rho \in B'$) and compatible with the w_ρ's in the sense that $\pi_{1\,1} \circ \widetilde{w}_\rho = w_\rho \circ \pi_{1\,1}$. Thus, fixed points of $\widetilde{w}_\rho$ lie over fixed points of w_ρ. Each singular residue class of $\mathbf{Z}_A$ is shown to be a connected wide open with one end, on which one of these involutions acts with p fixed points. To finish the argument, we show in [CMc, §8.2] that the quotient by $\widetilde{w}_\rho$ of such a residue class is a disk, in which the images of the p fixed points are permuted by an automorphism of order p (reducing to a translation). It is then straightforward analysis to prove that any such wide open is basic (as in [CMc, §2]), with an underlying affinoid that reduces to $y^2 = x^p - x$.

Remark 2.4. *We show in [CMc, Prop 4.9] that the fixed points of w_ρ correspond to pairs, (E, C), where E has fake CM by $\mathbb{Z}_p[\sqrt{-p}]$ or $\mathbb{Z}_p[\sqrt{-Dp}]$ (and $C = H_1(E)$). So this is where fake CM enters into the arithmetic of our stable model.*

The last step in our stable model construction is to form an admissible covering of $X_0(p^3)$ by wide open neighborhoods of the nontrivial affinoids that we know about. Once again, any supersingular region corresponding to $j(A) = 0$ or 1728, or for which $j(A) \notin \mathbb{F}_p$, is dealt with by applying an appropriate surjection from $W_{A'}(p^n)$ onto $W_A(p^n)$. We then total up our lower bounds for the genera of all of these wide opens (and the Betti number of the graph associated to our covering), and compare this with the genus of $X_0(p^3)$. Since the two are equal, we are able to conclude from [CMc, Proposition 2.5] that we haven't missed anything. Thus we have the following theorem.

Theorem 2.5. *The stable reduction of $X_0(p^3)$ for $p \geq 13$ consists of six ordinary components (reductions of the $\mathbf{X}^{\pm}_{a\,b}$) and a "necklace" of components, for each supersingular elliptic curve $A/\mathbb{F}_{p^2}$, whose graph is given below in Figure 1. The reductions of $\mathbf{E}_{1\,A}$ and $\mathbf{E}_{2\,A}$ are isomorphic to $y^2 = x^{(p+1)/i(A)} + 1$, and $\mathbf{Z}_A$ has $2(p+1)/i(A)$ singular residue classes with underlying affinoids that reduce to $y^2 = x^p - x$.*

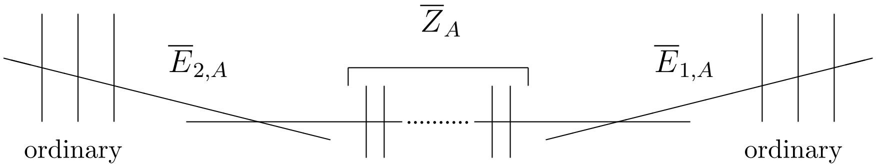


Figure 1: Partial Graph of the Stable Reduction of $X_0(p^3)$

3 Fake CM

Let K be a complete subfield of $\mathbb{C}_p$ with ring of integers R. Then we say that an elliptic curve, E/R, has fake CM if $\mathrm{End}_R(\hat{E}) \neq \mathbb{Z}_p$, and potential fake CM if this happens over $\mathbb{C}_p$. We showed in [CMc] that curves with certain types of fake CM can be used to understand the geometry of $X_0(p)$ and $X_0(p^3)$. In particular, let $\mathcal{R}$ be the set of rings of integers in quadratic extensions of $\mathbb{Q}_p$, and let $S \in \mathcal{R}$ be the ring of integers in a ramified extension. Then by [CMc, Prop 4.9], curves E with potential fake CM by S are precisely those for which $(E, H_1(E))$ is fixed by some involution w_ρ (for $\rho \in B'$, as in Section 2). Moreover, by [CMc, Prop 7.4], any fixed point of some involution, $\widetilde{w}_\rho$, is obtained from one of these by a non-canonical p-isogeny.

In this section we further investigate properties of curves which have fake CM by some $S \in \mathcal{R}$. In particular, we focus on the ways in which the fake endomorphism ring can embed into $B \cong \mathrm{End}(\hat{A})$ (via Woods-Hole theory), when A is supersingular and E corresponds to a point of $W_A(1)$. First we show that all subrings of B which are isomorphic to the same $S \in \mathcal{R}$ are B^* conjugate, and hence (using results from [G]) that all the curves in $W_A(1)$ with fake CM by the same ramified S make up a B^* orbit. Then we suppose that (E, C) is fixed by the involution w_ρ, for some $\rho \in B'$, and give alternative characterizations of the image of $\mathrm{End}(\hat{E})$ in B in terms of ρ.

3.1 Fake CM Curves and Orbits of B^*

With notation as in Section 2.1, we fix a supersingular elliptic curve $A/\mathbb{F}_{p^2}$ and an isomorphism between $\mathrm{End}(\hat{A})$ and $B = \mathbb{Z}_p[i,j,k]$. Then $B^* \cong \mathrm{Aut}(\hat{A})$ acts on $W_A(1)$ by $\rho(F,\alpha) = (F, \rho \circ \alpha)$. It is immediate that this restricts to an action of B^* on the subset of $W_A(1)$ corresponding to curves E with fake CM by a fixed $S \in \mathcal{R}$. We want to describe the orbits of this (restricted) action.

Lemma 3.1. *If S_1 and S_2 are subrings of B which are isomorphic to S, there is a $\rho \in B^*$ such that $S_2 = \rho^{-1} S_1 \rho$.*

Proof. We can assume without loss of generality that $S_1 = \mathbb{Z}_p[\iota]$, where $\iota = i$, j or k. Note that for each of these ι, and for any α, we have

$$Tr(\alpha\iota) = 0 \;\Rightarrow\; \iota\alpha = \bar{\alpha}\iota.$$

Suppose first that $S_1 = \mathbb{Z}_p[i]$. Since S_1 and S_2 are isomorphic, there must be an $\alpha \in S_2$ such that $\alpha^2 = -r$. Hence we have $N(\alpha) = r$ and $Tr(\alpha) = 0$. Now set $\gamma = \alpha/i \in B$, from which it follows that $N(\gamma) = 1$ (and therefore $\gamma^{-1} = \bar{\gamma}$). Finally, choose $\epsilon = \pm 1$ so that $\rho := 1 + \epsilon\gamma$ is a unit. Then using $Tr(\rho i) = 0$ we calculate:

$$\frac{\rho i \bar{\rho}}{N(\rho)} = (\bar{\rho})^{-1}\rho i = (\bar{\rho})^{-1}\rho\gamma^{-1}\alpha = (\bar{\rho})^{-1}(\epsilon + \gamma^{-1})\alpha = \epsilon\alpha.$$

In other words, $\rho i \rho^{-1} = \epsilon\alpha$, and therefore $\rho^{-1} S_2 \rho = \mathbb{Z}_p[i] = S_1$.

Now suppose that $S_1 = \mathbb{Z}_p[j]$. In this case there must be an $\alpha \in S_2$ such that $\alpha^2 = -p$, and hence $\alpha = bi + cj + dk$, for some $b, c, d \in \mathbb{Z}_p$ such that

$$-b^2 r - c^2 p - d^2 rp = -p.$$

Thus, we see that $p|b$. So $b = (ej)j$ for some $e \in \mathbb{Z}_p$, and $\alpha = \gamma j$ where $\gamma := ek + c + di \in B$. Again take $\rho = 1 \pm \gamma$. The remaining case, when $S_1 = \mathbb{Z}_p[k]$, is similar. □

Corollary 3.2. *When S is ramified, any two formal S-module structures,*

$$\sigma_1, \sigma_2 : S \to B = End(\hat{A}),$$

are conjugate in the sense that there is a $\rho \in B^*$ with

$$\rho^{-1}\sigma_1(s)\rho = \sigma_2(s) \qquad \forall s \in S.$$

Proof. From Lemma 3.1, there exist $\gamma_1, \gamma_2 \in B^*$ such that $\gamma_i^{-1}\sigma_i(S)\gamma_i = \mathbb{Z}_p[\iota]$ where $\iota = j$ or k. Note that $i\iota i^{-1} = -\iota$ in either case. Therefore we obtain two distinct automorphisms of S (over $\mathbb{Q}_p$) by taking

$$s \to \sigma_2^{-1}(\rho^{-1}\sigma_1(s)\rho),$$

where ρ is either $\gamma_1\gamma_2^{-1}$ or $\gamma_1 i^{-1}\gamma_2^{-1}$. One of these automorphisms must be the identity, which proves the corollary. □

THEOREM 3.3. *Suppose that $a := (E, C)$ and $b := (E', C')$ are points in $W_A(p)$ such that E and E' have (potential) fake CM by S (ramified), and such that C and C' are either both canonical or both not. Then $a = \rho b$ for some $\rho \in B^*$.*

Proof. Let $E = (F, \alpha)$ and $E' = (F', \beta)$. By the lemma, there is a $\rho \in B^*$ such that

$$\alpha\overline{\mathrm{End}(F)}\alpha^{-1} = (\rho\beta)\overline{\mathrm{End}(F')}(\rho\beta)^{-1}.$$

Moreover, by the corollary, we can choose ρ so that (F, α) and $(F', \rho \circ \beta)$ are two liftings of the same formal S-module structure on $\hat{A}$ (in the sense of [G]). Hence by [G, Prop 2.1], we have $\rho(E') = E$.

Now, if C and C' are canonical, it is immediate that $a = \rho b$ for this same ρ. So suppose that C and C' are both non-canonical. Then the isomorphism between $(F', \rho\circ\beta)$ and (F, α) at least takes C' to some non-canonical subgroup $D \subseteq F$. But $\mathrm{Aut}(F)$ transitively permutes the non-canonical subgroups by Remark 4.11 of [CMc]. Therefore we may choose an automorphism σ with $\sigma(D) = C$, and thus we have $a = \rho_1 b$ for $\rho_1 = (\alpha \circ \sigma \circ \alpha^{-1})\rho$. □

REMARK 3.4. *If E is defined over $W(\mathbb{F}_{p^2})$, and $\bar{E} \cong A$ for some supersingular A with A defined over $\mathbb{F}_p$ or with $j(A) \neq 0$ or 1728, then E has fake CM. Indeed, the Frobenius endomorphism of $\bar{E}$ over $\mathbb{F}_{p^2}$ is $[\pm p]_{\bar{E}}$. Since this endomorphism lifts to E, $\hat{E}$ is a Lubin-Tate formal group.*

For example, suppose that $p = 2$ and E is given by $y^2 + 2xy - Ay = x^3$, where $A^3 = 1$. Then in characteristic 2, we have $[2](x, y) = (Ax^4, y^4)$. So if $A \neq 1$, we don't know if E has fake CM 2-adically.

3.2 EMBEDDINGS OF FAKE ENDOMORPHISM RINGS

Now suppose that A is defined over $\mathbb{F}_p$ and that $j(A) \neq 0, 1728$. Recall (from [CMc, §4.2]) that for any $\rho \in B'$, the involution of $\mathbf{SD}_A$ given by $w_\rho = \rho \circ w_1$ has two fixed points. Let $x = (E, C) = (F, \alpha, C)$ be one of the them. As in the previous section, Woods Hole theory gives us an embedding of $\mathrm{End}(F)$ into B:

$$\alpha_*\mathrm{End}(F) := \alpha^{-1}\overline{\mathrm{End}(F)}\alpha \subseteq \mathrm{End}(\hat{A}) = B.$$

In this section, we use the embedding to reprove the result that E has fake CM by the ring of integers in a ramified quadratic extension of $\mathbb{Q}_p$. We also give alternate descriptions of the embedding which depend only on ρ, in particular showing that the fake endomorphism rings of both fixed points embed onto the same subring of B.

DEFINITION 3.5. *For $\rho = a + bi + cj + dk \in B$, we let $\rho' = a - bi + cj - dk$.*

LEMMA 3.6. *(i) For all $\rho \in B$, $\rho j = j\rho'$.*
(ii) $B' = \{ \rho \in B^* \mid \rho\rho' \in \mathbb{Z}_p^* \}$
(iii) If $\rho_1, \rho_2 \in B^*$, $(\rho_1\rho_2)' = \rho_1'\rho_2'$.
(iv) If $\rho \in B'$, $\rho\rho' = \rho'\rho$.

PROPOSITION 3.7. *Let $\rho \in B'$, and let $x := (E, C) = (F, \alpha, C)$ be fixed by w_ρ. Then $\alpha_* End(F) = \mathbb{Z}_p[\gamma]$, where $\gamma = \rho j$ and hence $\gamma^2 \in p\mathbb{Z}_p^*$.*

Proof. This is basically proven in [CMc, Prop 4.9], although we repeat the argument here. By Theorem 2.1 (and the fact that the only degree p endomorphisms of A are $\pm j$) we can choose isogenies,

$$\beta : \overline{F/C} \xrightarrow{\sim} \hat{A} \qquad \iota_C : F \to F/C,$$

such that $E/C = (F/C, \beta)$, and such that (ι_C, j) represents the natural isogeny from E to E/C. In fact, ι_C can be taken to be the natural map.

Now, the fact that $\rho(E/C) = E$ implies that there is an isomorphism, $\sigma : F/C \to F$, such that $\rho \circ \beta = \alpha \circ \bar{\sigma}$. So let $\pi_0 = \sigma \circ \iota_C \in \mathrm{End}(F)$, and then take $\gamma = \alpha\overline{\pi}_0\alpha^{-1}$. Then $\gamma \in \alpha_*\mathrm{End}(F)$ by definition, $\gamma = \rho j$ by commutativity, and from Lemma 3.6 we have

$$\gamma^2 = \rho j \rho j = -p\rho\rho' \in -p\mathbb{Z}_p^*.$$

Furthermore, since this implies that $\mathbb{Z}_p[\gamma]$ is a maximal order, it must be all of $\alpha_*\mathrm{End}(F)$. □

COROLLARY 3.8. *Let $x = (F, \alpha, C)$ be fixed by w_ρ for $\rho \in B'$, and let $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ for D a quadratic non-residue (mod p). Then x is defined over K, and*

$$End(F) = End_K(F) \cong \mathbb{Z}_p\Big[\sqrt{-\rho\rho' p}\Big].$$

Proof. The fixed points of w_ρ are defined over K, by the explicit formula for w_ρ (given in [CMc, Eq 3]). Therefore, F/C and the natural map, $\iota_C : F \to F/C$, are defined over K. Hence, the endomorphism, π_0 (as in Proposition 3.7), is defined over K. □

PROPOSITION 3.9. *If $\rho \in B'$ and $x := (F, \alpha, C)$ is fixed by w_ρ, then*

$$\alpha_* End(F) = S_\rho := \{\tau \in B \colon \rho\tau' = \tau\rho\}.$$

Proof. One direction is easy. In particular, from the previous proposition, everything in $\alpha_*\mathrm{End}(F)$ can be written as $a + b\gamma$. This is in S_ρ since

$$\rho(a + b\rho j)' = a\rho + b\rho\rho' j = (a + b\rho j)\rho.$$

For the other direction, Lemma 3.6 implies that S_ρ is at least a ring. We want to show that $S_\rho \subseteq \alpha_*\mathrm{End}(F)$. So first choose a $\tau \in S_\rho^*$. From the fact that $\rho \circ w_1 = w_1 \circ \rho'$ on $\mathbf{SD}_A$ (basically just $\rho j = j\rho'$, see [CMc, Cor 4.6]), we have

$$w_\rho(\tau x) = \rho\tau' w_1 x = \tau\rho w_1 x = \tau x,$$

which means that τx is one of the two fixed points of w_ρ. Suppose first that $\tau x = x$, i.e., $(F, \alpha) \cong (F, \tau \circ \alpha)$. Then by Theorem 2.1, there is a $\sigma \in \mathrm{End}(F)$ such that

$$\alpha \circ \bar{\sigma} = \tau \circ \alpha,$$

and hence $\tau \in \alpha_*\mathrm{End}(F)$. We conclude that if $\tau \in S_\rho^*$, at least $\tau^2 \in \alpha_*\mathrm{End}(F)$. But then, since $(1 \pm \tau)^2 = 1 \pm 2\tau + \tau^2$, it follows that $\tau \in \alpha_*\mathrm{End}(F)$. Finally, if $c \in S_\rho$, one of either $1+c$ or $1-c$ must be in S_ρ^*. Thus, $S_\rho \subseteq \alpha_*\mathrm{End}(F)$. □

Corollary 3.10. *If F and G are formal groups corresponding to the two fixed points of w_ρ, End(F) is canonically isomorphic to End(G).*

Proof. Let $x = (F, \alpha, C)$ and $y = (G, \beta, C')$ be the two fixed points of w_ρ. Then from either proposition, we have

$$\alpha_*\mathrm{End}(F) = \beta_*\mathrm{End}(G).$$

So α_* and β_* identify End(F) and End(G) with the same subring of B. □

Remark 3.11. *Let $x = (F, \alpha, C)$ and $y = (G, \beta, C')$ be the two fixed points of w_ρ, for $\rho \in B'$ (as above). Let S be the ring of integers in the ramified quadratic extension of $\mathbb{Q}_p$ for which End$(F) \cong$ End$(G) \cong S$. Then by [G, Prop 2.1], x and y are the two canonical liftings of the two S-module structures on $\hat{A}$ with image α_*End$(F) = \beta_*$End(G).*

4 Real CM

In this section, we shift our focus to elliptic curves E/R which have real CM, i.e. for which $\mathrm{End}_R(E) \neq \mathbb{Z}$. Our main result is that, inside $\mathbf{SD}_A$, real CM points are dense in the set of fake CM points. The strategy is to use Woods Hole theory and the fact that End(A) is dense in End$(\hat{A})$. First we make B into a topological ring in the usual way, by defining

$$||\rho|| = \max\{|h(\rho)|\colon h \in \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Z}_p)\}.$$

Then from the explicit formula of Gross-Hopkins (see [CMc, §4.2] or Section 2.1), the action,

$$B^* \times \mathbf{SD}_A \to \mathbf{SD}_A,$$

is continuous with respect to both variables.

Now assume that $A/\mathbb{F}_p$, and let $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ and $R = \mathcal{O}_K$. Thus the fake CM curves corresponding to points of $\mathbf{SD}_A$ are all defined and have fake CM over R by Corollary 3.8. Then real CM points are dense in these fake CM points in the following sense.

Theorem 4.1. *Choose $S \in \mathcal{R}$ ramified. Then points of $\mathbf{SD}_A$ corresponding to elliptic curves, E/R, for which End$_R(E) \otimes \mathbb{Z}_p \cong S$ are dense in those for which End$_R(\hat{E}) \cong S$. In fact, if (F, α) has fake CM and $\epsilon \in \mathbb{R}^+$, there exist $\rho \in B^*$ such that $||\rho - 1|| < \epsilon$ and $(F, \rho\alpha) \neq (F, \alpha)$ has real CM.*

Proof. In general, when $E = (F, \alpha)$ is defined over R with residue field k, E has CM over R if and only if $\alpha_*\mathrm{End}_R(F) \cap \mathrm{End}_k(A) \neq \mathbb{Z}$ in $\mathrm{End}_k\hat{A}$. In fact,

$$\mathrm{End}_R(F, \alpha) \cong \alpha_*\mathrm{End}_R F \cap \mathrm{End}_k A.$$

This follows from Theorem 2.1 if $R = R_p$, and an argument for more general R can be made via crystalline cohomology. In our case, $k = \mathbb{F}_{p^2}$, and since $A/\mathbb{F}_p$ is supersingular, this guarantees that $\mathrm{End}_k(A)$ is dense in $\mathrm{End}_k(\hat{A}) = \mathrm{End}(\hat{A})$.

So suppose (F, α) is defined over R (as above) and has fake CM by $S \in \mathcal{R}$ (ramified) and $\alpha_* S = \mathbb{Z}_p[\gamma]$. Fix an $\epsilon > 0$. Then there exists $\delta > 0$ such that for all $g \in \mathrm{End}(\hat{A})$ with $||g - \gamma|| < \delta$, there exists $\rho \in B^*$ with $||\rho - 1|| < \epsilon$ and

$$\rho S \rho^{-1} = \mathbb{Z}_p[g].$$

This follows from the construction of Theorem 3.3, since δ can be chosen so that $\mathbb{Z}_p[g] \cong \mathbb{Z}_p[\gamma]$ for all $||g-\gamma|| < \delta$. In particular, we may then choose $g \in \mathrm{End}(A)$ with $\mathbb{Z}_p[g] \neq \mathbb{Z}_p[\gamma]$, since $\mathrm{End}(A)$ is dense in $\mathrm{End}(\hat{A})$. Then $(F, \rho \circ \alpha)$ has CM because

$$(\rho \circ \alpha)_* \mathrm{End}_R F = \{\rho \circ \alpha \circ \gamma \circ (\rho \circ \alpha)^{-1} \colon \gamma \in \mathrm{End}_R F\} = \rho S \rho^{-1}.$$

Therefore, $g \in (\rho \circ \alpha)_* \mathrm{End}_R(F) \cap \mathrm{End}(A)$. □

Corollary 4.2. *Let A be any supersingular elliptic curve over $\mathbb{F}_{p^2}$. Then points corresponding to elliptic curves E with CM by an order of discriminant pM with $(p, M) = 1$ fill out a $\mu_{2(p+1)/i(A)}$ orbit of $G_m \cong \overline{\mathbf{SD}}_A$. Two such curves correspond to points in the same $\mu_{(p+1)/i(A)}$ orbit if and only if $M_1 M_2$ is a square (mod p).*

Proof. First suppose that $A/\mathbb{F}_p$ and $j(A) \neq 0, 1728$. Recall that curves with fake CM by S (as above) correspond to fixed points of the involutions w_ρ for $\rho \in B'$ by [CMc, Prop 4.10]. Remark 4.8 of [CMc] says that such points fill out a $\mu_{2(p+1)}$ orbit of $G_m \cong \overline{\mathbf{SD}}_A$, and that B^* acts like μ_{p+1}. Now we have Theorem 3.3 which says that curves with the same fake endomorphism ring are B^* translates. So this proves the analogous statement for fake CM curves, and by Theorem 4.1 the statement about real CM curves then follows.

Now suppose that $j(A) = 0$ or 1728. Remark 4.8 is based on the explicit formula for the action of B^* on the deformation space, X_K, for the formal group $\hat{A}$. When $j(A) = 0$ or 1728, $W_A(1)$ can be identified with the quotient of X_K by a faithful action of $\mathrm{Aut}(A)/\pm 1$, in a way which is compatible with the natural embedding of $\mathrm{Aut}(A)$ into B^*. So basically, we can use the same argument as above for the circle of X_K which lies over $\mathbf{SD}_A$, and then apply the degree $i(A)$ map. Similarly, if A is not defined over $\mathbb{F}_p$, we can choose some $A_0/\mathbb{F}_p$ and then apply an isomorphism between $W_{A_0}(p)$ and $W_A(p)$ as in [CMc, §4.1]. □

Remark 4.3. *When $A/\mathbb{F}_p$, a canonical choice of parameter on $\mathbf{SD}_A$ is given by $(j(E) - \mathit{Teich}(j(A)))/\sqrt{p^{i(A)}}$.*

Question: If E and E' both satisfy the above conditions, the residue class of

$$\frac{j(E') - \mathrm{Teich}(j(A))}{j(E) - \mathrm{Teich}(j(A))} \pmod{\sqrt{p}}$$

is the residue class of a $\frac{p+1}{i(A)}$-th root of unity. Which one and when is it 1?

4.1 Heegner Points

By a Heegner point on $X_0(N)$ we mean a pair (E,C) where E is a CM elliptic curve and C is a cyclic subgroup of order N such that $\mathrm{End}(E) \cong \mathrm{End}(E/C)$. Let $\mathcal{X}_0(p^n)$ denote a stable model for $X_0(p^n)$. In this section, we discuss the placement of Heegner points on $\mathcal{X}_0(p^n)$, beginning with those Heegner points which lie in the ordinary region.

Let $R_i(D)$ denote the order of discriminant p^iD in $\mathbb{Q}[\sqrt{p^iD}]$ where $D<0$, and $(D,p)=1$. Suppose $\mathrm{End}(E) \cong R_i(D)$. Then E has ordinary reduction if and only if $(\frac{D}{p})=1$ and i is even.

In order to study ordinary Heegner points, we interpret the irreducible affinoids, $\mathbf{X}^{\pm}_{a\,b}$, which make up the ordinary locus as in [C1]. Recall that $\mathbf{X}_{a\,b}$ (for $a,b \geq 0$ and $a+b=n$) was defined in Section 2.1 as the affinoid in $X_0(p^n)$ whose points correspond to pairs (E,C) where E is ordinary and $|C \cap K(E)| = p^a$. The first author showed (see [C1, §2] or [CMc, §3.2]) that for $a \geq b$ this is equivalent to the affinoid whose points correspond to pairs, $(E,\mathcal{P})$, where E is ordinary and $\mathcal{P}$ is a certain pairing from $K_a(E) := K(E) \cap E[p^a]$ onto μ_{p^b}. Furthermore, let $C_{a\,b}$ denote the set of isomorphism classes of pairings from $\mathbb{Z}/p^a\mathbb{Z}$ onto μ_{p^b} (which has two elements when $a \geq b \geq 1$). Then for any $\beta \in C_{a\,b}$ the subspace, $\mathbf{X}^{\beta}_{a\,b} \subseteq \mathbf{X}_{a\,b}$, consisting of those pairs for which $\mathcal{P} \in \beta$, is an irreducible affinoid which reduces to $Ig(p^a)$. Now, using the Atkin-Lehner involution, the remaining irreducible affinoids (for $a<b$) in the ordinary locus can be defined by

$$\mathbf{X}^{\beta}_{a\,b} = w_n \mathbf{X}^{(\frac{-1}{p})\beta}_{b\,a}.$$

(Note: This is a slight change from the notation of [C1].) Ordinary points of $X_0(p^n)$ all have smooth reduction on one of these components, and we will show that there are in fact infinitely many Heegner points on each.

Lemma 4.4. *For any $b \geq 0$, there are infinitely many Heegner points on $\mathbf{X}_{b\,b}$.*

Proof. Points of $\mathbf{X}_{b\,b}$ can also be thought of as triples, (E,C_1,C_2), where E is an ordinary elliptic curve and C_i is a cyclic subgroup of order p^b such that $C_1 \cap C_2 = (0)$ and $C_i \cap K(E) = (0)$. If we let ι_C denote the natural map from $E \to E/C$, then the triple, (E,C_1,C_2), just corresponds to the pair, $(E/C_1, C(C_1,C_2))$, where

$$C(C_1,C_2) := \ker(\iota_{C_2} \circ \check{\iota}_{C_1}) \subseteq E/C_1.$$

Now, choose any ordinary elliptic curve, E, with CM by $R_{2i}(D)$, and then choose C_1 and C_2 (as above) so that $\mathrm{End}(E/C_1) \cong \mathrm{End}(E/C_2) \cong R_{2(i+b)}(D)$. If $i>0$, any choice of C_1 and C_2 (as above) will do. If $i=0$, one also needs C_i to be disjoint from the kernel of the Verschiebung lifting (which is always possible if $p>2$). Then $(E/C_1, C(C_1,C_2))$ is a Heegner point on $\mathbf{X}_{b\,b}$. □

There are various maps between ordinary affinoids which can now be used (along with Lemma 4.4) to construct Heegner points on every $\mathbf{X}^{\beta}_{a\,b}$. First of all,

w_n takes Heegner points of $\mathbf{X}_{a\,b}$ to Heegner points of $\mathbf{X}_{b\,a}$ by definition. Secondly, the group $\mathbb{Z}_p^*$ acts through $(\mathbb{Z}/p^b\mathbb{Z})^*$ on $\mathbf{X}_{a\,b}$ via $\tau_r \colon (E, \mathcal{P}) \mapsto (E, \mathcal{P}^r)$. Moreover, τ_r fixes $\mathbf{X}_{a\,b}^{\beta}$ (i.e. preserves the class of the pairing in $C_{a\,b}$) if and only if τ_r is a square. Finally, we have a natural isomorphism, $\alpha_{a\,b} \colon \mathbf{X}_{b\,b} \to \mathbf{X}_{a\,b}$, which takes the pair $(E, \mathcal{P})$ to the pair $(E, \mathcal{P}')$ for

$$\mathcal{P}'(R, S) = \mathcal{P}(p^{a-b}R, p^{a-b}S).$$

We now investigate the effect of these maps on Heegner points.

Lemma 4.5. *Let F be a fixed ordinary elliptic curve. Then $(\mathbb{Z}/p^b\mathbb{Z})^*$ acts transitively on the set of points of the form (F, C) which lie in $\mathbf{X}_{b,b}$.*

Proof. Let $B_b(F)$ denote this set. Then points of $B_b(F)$ correspond to triples (E, C_1, C_2) as above where $E = F/K_b(F)$ and $C_1 = F[p^b]/K_b(E)$. There are $p^{b-1}(p-1)$ such triples. The lemma follows because $(\mathbb{Z}/p^b\mathbb{Z})^*$ acts faithfully on $B_b(F)$. □

Lemma 4.6. *If (F, C) is a Heegner point on $\mathbf{X}_{b\,b}$ and End$(F) = R_{2b}(D)$ then $\alpha_{a\,b}(F, C)$ is a Heegner point.*

Proof. The point (F, C) is $(E/C_1, C(C_1, C_2))$, where $E = F/p^bC$, $C_1 = \iota_{p^bC}(F[p^b])$ and $C_2 = \iota_{p^bC}(C)$. In this case, $(p, \mathrm{disc}(\mathrm{End}(E))) = 1$. Let $\phi^c \colon E \to E^{\sigma^c}$ be the lifting of Frobenius. Then $\alpha_{a\,b}(F, C) =$

$$(F, \ker(\iota_{C_2^{\sigma^{a-b}}} \circ \phi^{a-b} \circ \iota_{p^bC})),$$

which is clearly a Heegner point. □

Theorem 4.7. *There are infinitely many Heegner points lying over each ordinary component of $\mathcal{X}_0(p^n)$ for $n \geq 1$ and $p > 2$ (all with smooth reduction).*

Proof. By Lemma 4.6, it suffices to guarantee at least one Heegner point, (F, C), on each $\mathbf{X}_{b,b}^{\beta}$ with End$(F) \cong R_{2b}(D)$. From the proof of Lemma 4.4, such points correspond to triples (E, C_1, C_2) where End$(E) \cong R_0(D)$. For a fixed F, we must have $E = F/K_b(F)$ and $C_1 = F[p^b]/K_b(E)$. Then we get a point of $\mathbf{X}_{b\,b}$ by choosing any C_2 disjoint from C_1 and $K(E)$, and a Heegner point if C_2 is also disjoint from the kernel of the Verschiebung lifting.

At this point, the argument is reduced to simple counting. We have a total of $p^{b-1}(p-2)$ Heegner points in each $B_b(F)$. The cardinality of $B_b(F)$ is $p^{b-1}(p-1)$, and from Lemma 4.5 half of these points lie in each $X_{b\,b}^{\beta}$. So since $p^{b-1}(p-2) > p^{b-1}(p-1)/2$ if $p > 3$, we are done ($p = 3$ can be handled by Atkin-Lehner). □

Heegner points in the supersingular region of $\mathcal{X}_0(p^n)$ are somewhat easier to describe.

Lemma 4.8. *Let E be a CM elliptic curve with supersingular reduction, such that p^m exactly divides the discriminant of End(E). Then we have*

$$h(E) = \begin{cases} p^{1-k}/(p+1), & \text{if } m = 2k \\ p^{1-k}/2, & \text{if } m = 2k-1. \end{cases}$$

Furthermore, if End($\hat{E}$) $= \mathbb{Z}_p[\gamma]$ and $\gamma^2 \in \mathbb{Z}_p$, we have Ker($\gamma$) $\cap K(E) = K(E)$ (which has order p^k).

Proof. This is an exercise in applying [B, Thm 3.3]. The point is that if $E/C \cong E$, we must at least have $h(E/C) = h(E)$. □

Theorem 4.9. *Let E be a CM elliptic curve with supersingular reduction, such that p^m exactly divides the discriminant of End(E). Then $(E, C) \in X_0(p^n)$ (for $n > 0$) is a Heegner point if and only if $m = n$ and $K(E) \subseteq C$.*

Proof. This follows directly from Lemma 4.8 (and [B, Thm 3.3]). Indeed, if E and m are as above, and $C \subseteq E$ is any cyclic subgroup of order p^n, we have

$$\mathrm{disc}(\mathrm{End}(E/C)) = \frac{\mathrm{disc}(\mathrm{End}(E)) \cdot |C|^2}{|K(E) \cap C|^4} \cdot \begin{cases} p, & \text{if } m \text{ is odd and } K(E) \subseteq C \\ 1, & \text{otherwise.} \end{cases}$$

□

Now, when $n \leq 3$, the above results make it possible to be very explicit about the placement of Heegner points on $\mathcal{X}_0(p^n)$. On $\mathcal{X}_0(p)$, the supersingular Heegner points all lie on $\mathbf{SD}_A$ for some A and have singular reduction (although when $j(A) = 1728$ they have smooth reduction on the Deligne-Rapoport model from [DR, §VI.6.16]). They also correspond to pairs, (E, C), where E has CM by $R_1(D)$ and $C = K(E)$. Heegner points of $X_0(p^2)$ correspond to those pairs, (E, C), where E has CM by $R_2(D)$ (with $(\frac{D}{p}) = -1$) and $K(E) = pC$. They all have smooth reduction on the component of $\mathcal{X}_0(p^2)$ which Edixhoven found (and which we call $\overline{\mathbf{Y}}_A$). Finally, Heegner points on $X_0(p^3)$ correspond to pairs where E has CM by $R_3(D)$ and $K(E) = pC$. This implies that they all lie on the affinoid $\mathbf{Z}_A$. By Theorem 4.1, there are infinitely many which are fixed by some $\widetilde{w}_\rho$. Hence, using the discussion at the beginning of [CMc, §8], they have smooth reduction on each of the new components which lie in the singular residue classes of $\mathbf{Z}_A$. However, there are also infinitely many supersingular Heegner points of $X_0(p^3)$ which are *not* fixed by any $\widetilde{w}_\rho$, from the preceding theorem and Proposition 7.4 of [CMc] (see also [CMc, Rem 7.5]), and it is unclear where the reductions of these points lie on $\overline{\mathbf{Z}}_A$.

5 Field of Definition

Suppose L/K is an unramified extension of local fields. It follows from [DM, Thm 2.4] that an Abelian variety A over K has semi-stable reduction (i.e. has a model with semi-stable reduction over $\mathcal{O}_K$) if and only if A_L has semi-stable reduction. Also, in the special case where A is the Jacobian of a curve, C/K, and L/K is the maximal unramified extension, A has semi-stable reduction if and only if C_L does. It is not true, however, that (in this case) C has semi-stable reduction whenever A does. For example, the Jacobian of $X_0(p)$ has a model with semi-stable reduction over $\mathbb{Z}_p$, while $X_0(p)$ may not (for example, when $p = 37$). This is an important point for us, because Krir determined a field over which the Jacobian of $X_0(p^n)$ attains stable reduction in [K, Théorème 1]. Indeed, let $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ for D a quadratic non-residue. Then Krir's result can be stated as follows.

Theorem 5.1 (Krir). *The Jacobian of $X_0(p^n)$ has stable reduction over the class field M_n over K of the subgroup of K^* given by*

$$\{a \in \mathcal{O}_K^* \colon a^2 \in 1 + \sqrt{p^{n-1}}\mathcal{O}_K\}.$$

By the above reasoning, it follows that $X_0(p^n)$ also has a stable model over this same field, M_n. However, one can not conclude from this result which extensions of $\mathbb{Q}_p$ are sufficient for $X_0(p^n)$ to attain stable reduction (and there may not be a minimal such field). What we do in this section is produce a finite extension, $F_3 \supseteq \mathbb{Q}_p$, over which our stable model for $X_0(p^3)$ can be defined, partially using the result of Krir. Fake and real CM also play a role because of the correspondence between w_ρ and $\widetilde{w}_\rho$ fixed points and fake CM curves. Our final result is the following.

Theorem 5.2. *If $1 \leq n \leq 3$, the stable model of $X_0(p^n)$ is defined over the class field F_n over $K := \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ of the subgroup of K^* given by*

$$(p^{2a_n})^{\mathbb{Z}}\{a \in \mathcal{O}_K^* \colon a^{b_n} \in 1 + \sqrt{p^{n-1}}\mathcal{O}_K\},$$

where $(a_n, b_n) = (1,1)$ if $n = 1$, $(3,4)$ if $n = 2$, and $(3,2)$ if $n = 3$. In particular,

$$([F_n \colon \mathbb{Q}_p], e(F_n/\mathbb{Q}_p)) = \begin{cases} (2,1), & \text{if } n = 1; \\ (6(p^2-1), (p^2-1)/2), & \text{if } n = 2; \\ (12(p^2-1)p^2, (p^2-1)p^2) & \text{if } n = 3. \end{cases}$$

5.1 Two Ingredients

One of the main ingredients in our field of definition is the field over which the fixed points of our involutions, $\widetilde{w}_\rho$, are defined. This field is necessary, by our construction, to obtain good reduction for the underlying affinoids in the singular residue classes of $\mathbf{Z}_A$. As real CM curves have been shown to be dense in these points, we are able to apply classical results on CM elliptic curves to determine this field.

PROPOSITION 5.3. *Let A be a supersingular curve over $\mathbb{F}_p$. Let F be the smallest field over which all the fixed points in $W_A(p^3)$ of our involutions $\widetilde{w}_\rho$ are defined. Then,*

$$F = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp}, j(p\sqrt{-p}), j(p\sqrt{-Dp}))$$

where $D \in \mathbb{Z}^+$ is a quadratic non-residue. This is the class field over $K := \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ of the subgroup of K^* given by

$$(\sqrt{p})^{\mathbb{Z}} \mu_{p^2-1}(1 + p\mathcal{O}_K).$$

In particular, $[F : K] = p^2$.

Proof. By Theorem 4.1 and Proposition 7.4 of [CMc] we see that F is the field of definition over $\mathbb{Q}_p$ of the set of points (E, C) where E lifts A and has CM by an order whose discriminant is exactly divisible by p (note that here C is not necessarily $H_1(E)$). The proposition now follows from Theorem 5.5 of [S]. □

REMARK 5.4. *This field F is the same as that mentioned in Remark 8.1 of [CMc].*

We used a surjection from $W_A(p^n)$ onto $W_{A'}(p^n)$, where A and A' are supersingular elliptic curves over $\mathbb{F}_{p^2}$, to deal with those regions for which $j(A') = 0$ or 1728, or for which A' is not defined over $\mathbb{F}_p$. The surjection can be defined over $W(\mathbb{F}_{p^k})$ as long as A and A' are p-prime isogenous over $\mathbb{F}_{p^k}$. Another ingredient in our determination of a field of definition is the following theorem, that $k = 24$ always suffices.

THEOREM 5.5. *Any two supersingular elliptic curves over $\mathbb{F}_{p^2}$ are 2-power isogenous over $\mathbb{F}_{p^{24}}$.*

Proof. Suppose A and B are two supersingular elliptic curves over $\mathbb{F}_{p^2}$. It is well known that there exists a 2^n-isogeny $\alpha\colon A_0 := A \to A_n := B$ over $\bar{\mathbb{F}}_p$ for some n (see [R, Lemma 3.17]). We can factor α as

$$A_0 \xrightarrow{\alpha_1} A_1 \cdots A_{i-1} \xrightarrow{\alpha_i} A_i \cdots A_{n-1} \xrightarrow{\alpha_n} A_n$$

where A_i is an elliptic curve over $\bar{\mathbb{F}}_p$ and α_i is a 2-isogeny. Furthermore, each A_i is supersingular and hence can be defined over $\mathbb{F}_{p^2}$. Thus it suffices to prove the following lemma.

LEMMA 5.6. *Any two elliptic curves A and B over $\mathbb{F}_{p^k}$ which are 2-isogenous over $\bar{\mathbb{F}}_p$ are 2-isogenous over $\mathbb{F}_{p^{12k}}$.*

There exists a subgroup C of $A(\bar{\mathbb{F}}_p)$ of order 2 so that B and A/C are isomorphic over $\bar{\mathbb{F}}_p$. Now, $A \to A/C$ is defined over $\mathbb{F}_{p^{6k}}$ because all the points of order 2 on A are defined over the extension of $\mathbb{F}_{p^k}$ of degree either 2 or 3. In particular, $B \cong A/C$ over $\mathbb{F}_{p^{12k}}$ because two elliptic curves with the same j-invariant are isomorphic over the quadratic extension. □

5.2 Proof of Theorem 5.2

The case $n=1$ follows from [DR, §VI 6.16] and the fact that all supersingular elliptic curves in characteristic p are defined over $\mathbb{F}_{p^2}$. The case $n=2$ over $\mathbb{Q}_p^{nr}$ was handled by Edixhoven in [E1, Thm 2.1.1].

When $n \in \{2,3\}$, we defined an admissible rigid open cover $\mathcal{C}_0(p^n)$ of $X_0(p^n)$ in Theorems 5.3 and 9.2 of [CMc] and showed that it was semi-stable over $\mathbb{C}_p$. We must show that the cover is defined and semi-stable (as in [CMc, Prop 2.5]) over F_n. In particular, we must show that (over F_n) each subspace W in the cover is a basic wide open, and that the subspaces intersect each other in the union of annuli.

Recall from [CMc, §3.2] that wide open neighborhoods, $W^{\pm}_{a\,b}$, of the ordinary affinoids, $\mathbf{X}^{\pm}_{a\,b}$, can be constructed by considering pairs (E,C) where E is "nearly ordinary." So we begin by showing that each $W^{\pm}_{a\,b}$ is a basic wide open (using essentially the same argument as was used in the proofs of [CMc, Thm 5.3, 9.2]). The affinoid, $\mathbf{X}^{\pm}_{a\,b}$, is defined and has good reduction over F_n by Lemma 3.6 of [CMc]. Then the intersections, $W^{\pm}_{a\,b} \cap W_A(p^n)$, are shown to be annuli over F_n by choosing an appropriate map to $X_0(p)$ and applying Lemma 2.3 about extensions of annuli. Thus each $W^{\pm}_{a\,b}$ is a basic wide open over F_n. Furthermore, there isn't anything else to show in the $n=2$ case, since

$$\mathbf{Y}_A = W_A(p^2) - \bigcup W^{\pm}_{a\,b}$$

is defined and has good reduction over F_2 by [CMc, Prop 5.2].

Now suppose that $n=3$ and fix a supersingular curve, $A/\mathbb{F}_p$, with $j(A) \neq 0$ or 1728. By [CMc, Prop 4.2] and Theorem 5.5, it suffices to verify the above conditions for the subspaces which cover $W_A(p^3)$ for one such A. For convenience, we briefly recall the definitions of these subspaces. Initially, we cover $W_A(p^3)$ with three subspaces: $V_1(A)$, $V_2(A)$, and $U(A)$. Each one is $\pi_{1\,1}^{-1}$ of some sub-annulus of $W_A(p)$, and they are chosen so that $V_i(A)$ is a neighborhood of $\mathbf{E}_{i\,A}$ while $U(A)$ is a neighborhood of $\mathbf{Z}_A$. Now, in order to deal with the singular residue classes of $\mathbf{Z}_A$, we then refine the cover in the following way. Let $\mathcal{S} := \mathcal{S}(A)$ be the set of singular residue classes of $\mathbf{Z}_A$, and let $\mathbf{X}_S$ be the underlying affinoid of any $S \in \mathcal{S}$. Then we basically remove every $\mathbf{X}_S$ from $U(A)$ to get a new neighborhood, $\hat{U}(A)$, of $\mathbf{Z}_A$. Thus the subspaces in $\mathcal{C}_0(p^3)$ which cover $W_A(p^3)$ are given by:

$$\big\{V_1(A), V_2(A), \hat{U}(A)\big\} \cup \mathcal{S}(A).$$

Now, much of the proof of [CMc, Thm 9.2] is still valid, as stated, over F_3. For example, by Proposition 8.7 of [CMc] and Proposition 5.3 the elements in $\mathcal{S}(A)$ are basic wide opens over F_3. Also, $V_i(A)$ and $U(A)$ are at least wide opens over F_3, because they are residue classes of affinoids which are defined over F_3 (exactly as in the proof over $\mathbb{C}_p$). So the only things which we have to justify are that the affinoids, $\mathbf{Z}_A$, $\mathbf{E}_{1\,A}$, and $\mathbf{E}_{2\,A}$ have good reduction over F_3, and that $V_i(A) \cap U(A)$ is an annulus over F_3. This is where we use Krir.

By Krir's result we know that the affinoids $\mathbf{Z}_A$, $\mathbf{E}_{1\,A}$ and $\mathbf{E}_{2\,A}$ have good reduction over M_3, and that $V_i(A) \cap U(A)$ is an annulus over M_3. Then it follows from Proposition 3.14 of [CMc] that $V_i(A) \cap U(A)$ is an annulus over F_3. Also, $\mathbf{Z}_A$, $\mathbf{E}_{1\,A}$, and $\mathbf{E}_{2\,A}$ have good reduction over F_3 because any reduced affinoid which acquires good reduction over an unramified extension must have good reduction. Therefore our cover can be defined and is semi-stable over F_3, and hence it corresponds by [CMc, Prop 2.7] to a semi-stable model for the curve over F_3.

6 Action of Inertia

If Y/K is a curve, and $\mathcal{Y}$ its stable model over $\mathbb{C}_p$, there is a homomorphism w_Y from

$$I_K := \mathrm{Aut}_{cont}(\mathbb{C}_p/K^{nr}) \to \mathrm{Aut}(\overline{\mathcal{Y}}).$$

It is characterized by the fact that for each $P \in Y(\mathbb{C}_p)$ and $\sigma \in I_K$,

$$\overline{P^\sigma} = w_Y(\sigma)(\overline{P}). \tag{1}$$

We have something similar if $\mathbf{Y}$ is a reduced affinoid over K. Namely, we have a homomorphism $w_Y \colon I_K \to \mathrm{Aut}(\overline{\mathbf{Y}}_{\mathbb{C}_p})$ characterized by (1). This follows from the fact that I_K preserves $(\mathbf{Y}_{\mathbb{C}_p})^0$ (power bounded elements of $A(\mathbf{Y}_{\mathbb{C}_p})$) and $A(\mathbf{Y}_{\mathbb{C}_p})^v$ (topologically nilpotent elements of $A(\mathbf{Y}_{\mathbb{C}_p})$). Moreover, inertia action behaves well with respect to morphisms in the following sense.

Lemma 6.1. *If $f \colon X \to Y$ is morphism of reduced affinoids over K and $\sigma \in I_K$, then $w_Y(\sigma) \circ \bar{f} = \bar{f} \circ w_X(\sigma)$.*

For convenience, we let $I = I_{\mathbb{Q}_p}$ and let w be the inertia action (over $\mathbb{Q}_p$) on

$$\prod_{n \geq 1} \mathrm{Aut}(\overline{\mathcal{X}_0(p^n)}).$$

Also, let m_n denote the intersection of all extensions of K^{nr} over which $X_0(p^n)$ has semi-stable reduction. It is known that m_n is the minimal such extension. Clearly $m_n \subseteq M_n$ but Krir says the extension M_n "n'est certainement pas minimale." In the case of $X_0(81)$, this is confirmed in [M2, §4], where a stable model for $X_0(81)$ is defined over an extension of $\mathbb{Q}_3^{nr}$ of degree 36 while Krir's field has ramification index $8 \cdot 3^4$. From our calculation of the inertia action, however, it will follow that $m_n = M_n$ for $n \leq 3$.

6.1 Inertial action on the ordinary components

For $a, b \geq 0$, let $X^{\pm}_{a\,b}$ denote the reduction of the ordinary affinoid, $(\mathbf{X}^{\pm}_{a\,b})_{\mathbb{C}_p}$, in the sense of Remark 2.3. Then since $\mathbf{X}_{a\,b}$ is defined over $\mathbb{Q}_p$, $w(\sigma)$ must preserve $X_{a\,0}$, $X_{0\,b}$ and $X_{a\,b} = X^+_{a\,b} \coprod X^-_{a\,b}$ (for $ab \neq 0$). Also, as explained in [C1, §1] (or the previous section on Heegner points), if $a \geq b$, $\mathbf{X}_{a\,b}$ is naturally isomorphic to $\mathbf{X}_{b\,a}$ and to $\mathbf{X}_{b\,b}$. Therefore, by Lemma 6.1, it suffices to compute the inertial action on $X_{b\,b}$.

So recall first that there is an isomorphism between $X^{\beta}_{b\,b}$ and $Ig(p^b)$ which can be constructed as follows. First we choose a primitive p^b-th root of unity, ζ, which represents β in the sense that whenever $(E,\mathcal{P}) \in \mathbf{X}^{\beta}_{b\,b}$ and P generates $K_b(E)$ we have $\mathcal{P}(P,P) = \zeta^{k^2}$ for some $k \in (\mathbb{Z}/p^b\mathbb{Z})^*$ (this is explained on page 5 of [C1]). Then we can define an embedding, $\alpha_\zeta : \mathbf{X}^{\beta}_{b\,b} \to X_1(p^b)$, given by $\alpha_\zeta(E,\mathcal{P}) = (E, p^bQ)$, where $Q \in E[p^{2b}]$ such that there exists $P \in K_b(E)$ with

$$e_{p^{2b}}(P,Q) = \mathcal{P}(P,P) = \zeta.$$

This passes to an isomorphism, $X^{\beta}_{b\,b} \to Ig(p^b)$.

Now, let d be a quadratic non-residue. Identify $\mathbf{X}^{+}_{b\,b}$ with $\mathbf{X}^{-}_{b,b}$ by $(E,\mathcal{P}) \to (E,\mathcal{P}^d)$, and correspondingly $X_{b\,b}$ with $Ig(p^b) \times \{\pm 1\}$. Suppose that $\sigma \in I$ and $\sigma(\zeta) = \zeta^{d^i t^2}$, where $i \in \{0,1\}$ and $t \in (\mathbb{Z}/p^b\mathbb{Z})^*$. Then we have $\sigma(E,\mathcal{P}) = (E^\sigma, \mathcal{P}^\sigma)$, where

$$\mathcal{P}^\sigma(\sigma(A),\sigma(B)) = \sigma(\mathcal{P}(A,B)).$$

So if $\mathcal{P}(P,P) = \zeta$, it follows that

$$e_{p^{2b}}(\sigma(P)/t, \sigma(Q)/T) = \mathcal{P}^\sigma(\sigma(P)/t, \sigma(P)/t) = \zeta^{d^i},$$

where $T \in \mathbb{Z}/p^{2b}\mathbb{Z}$ and $T \equiv t \pmod{p^b}$. Identify (the obvious subgroup of) $\mathrm{Aut}(Ig(p^n))$ with $(\mathbb{Z}/p^n\mathbb{Z})^*$. Then we see that $w(\sigma)$ acts on $X_{b\,b}$ as follows.

Proposition 6.2. *The inertial action on the ordinary components of $X_0(p^n)$ is given by*

$$w(\sigma)|_{X_{b\,b}} = (t^{-1}, (-1)^i).$$

Corollary 6.3. *The field $\mathbb{Q}_p^{nr}(\mu_{p^{[n/2]}})$ is contained in m_n.*

6.2 Action of Inertia on $\overline{\mathcal{X}_0(p^2)}$

Suppose A is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Inside the corresponding residue class, $W_A(p^2) \subseteq X_0(p^2)$, we have an affinoid $\mathbf{Y}_A$ defined over $W(\mathbb{F}_{p^2}) \otimes \mathbb{Q}_p$ such that $Y_A := \overline{\mathbf{Y}_A \otimes \mathbb{C}_p}$ is the set of non-singular points in a component of the stable reduction of $\mathcal{X}_0(p^2)$. Now we determine the action of I on Y_A.

First assume that A is defined over $\mathbb{F}_p$ and that $j(A) \neq 0$ or 1728 (general case will follow from Lemma 6.1). Let κ be as in Theorem 2.2. We know there are series $F(T), G(T) \in T\mathbb{Z}_p[[T]]$ such that $\mathbf{Y}_A$ is the affinoid

$$\mathrm{Max}\ (\mathbb{Q}_p\langle a, a^{-1}, b, b^{-1}, x, y\rangle / M)$$

where M is the ideal generated by $\kappa^p a = x^{p+1}$, $\kappa^p b = y^{p+1}$ and

$$(F(x) + G(\kappa/x) - F(y) - G(\kappa/y)).$$

Suppose $\alpha^{p+1} = \kappa$. Then if $K = \mathbb{Q}_p(\alpha)$, $(\mathbf{Y}_A)_K$ is

$$\text{Max}\ \big(K\langle u, v, u^{-1}, v^{-1}\rangle/(F(\alpha^p/u) + G(\kappa u/\alpha^p) - F(\alpha^p/v) - G(\kappa v/\alpha^p))\big),$$

where $u = \alpha^p/x$ and $v = \alpha^p/y$. It follows that Y_A has the equation,

$$uv(v-u)^{p-1} = 1,$$

or $s^{p+1} = (r^2-1)/4$, if we let $s = 1/(v-u)$ and $r = (u+v)/(v-u)$. Now, on one hand we have $\overline{\sigma(u(P))} = \overline{u(P)}$. On the other, if $\sigma(\alpha) = \zeta\alpha$ for a $p+1$-st root of unity, ζ, we have $\sigma(u(P)) = \zeta^p u(\sigma(P))$. Thus, on Y_A, $w(\sigma)$ is the automorphism $(u, v) \to (\zeta u, \zeta v)$, or equivalently $(r, s) \to (r, \zeta^{-1}s)$.

Since we have a finite morphism from $\mathbf{Y}_A$ to $\mathbf{Y}_{A'}$ over $W(\bar{\mathbb{F}}_p) \otimes \mathbb{Q}$ for arbitrary supersingular A' (an isomorphism when $j(A') \neq 0$ or 1728) we know by Lemma 6.1 the action of I on $Y_{A'}$ for all A' as long as $p \geq 13$. In general, Y_A has the equation

$$s^{(p+1)/i(A)} = (r^2-1)/4$$

and $w(\sigma)$ is the automorphism $(r, s) \to (r, \zeta^{-i(A)}s)$. This also determines the action on $E_{i\,A}$, $i \in \{1, 2\}$, since as explained in Remark 9.3 of [CMc] we have finite degree p morphisms $\mathbf{E}_{1\,A} \to \mathbf{Y}_A$ and $\mathbf{E}_{2\,A} \to \mathbf{Y}_{A^{Frob}}$ with purely inseparable reduction.

Remark 6.4. *It follows from the above and Corollary 6.3 that $K^{nr}(\mu_p, \alpha) \subseteq m_2$. Therefore, since*

$$Gal(K^{nr}(\mu_p, \alpha)/K^{nr}) \cong \mathcal{O}_K^*/\{a \in \mathcal{O}_K^* \colon a^2 \in 1 + \sqrt{p}\mathcal{O}_K\},$$

we see that $M_2 = m_2$.

6.3 Action of Inertia on $\overline{\mathcal{X}_0(p^3)}$

Suppose A is a supersingular elliptic curve over $\mathbb{F}_p$ with $B = \text{End}(\hat{A})$. Suppose $\rho \in B'$ and x is a fixed point of $\overline{w}_\rho$. Then we know w_ρ has a unique fixed point $\tilde{x} := (F, \iota, C)$ in $\mathbf{SD}(\mathbb{C}_p)$ above x. Let C_x be the smooth locus of the corresponding component of the stable reduction of $X_0(p^3)$ (which is affine and hyper-elliptic, with equation $y^2 = x^p - x$). By Proposition 7.4 of [CMc] the fixed points $\mathcal{F}_x$ of the hyper-elliptic involution τ_x of C_x are naturally in 1-1 correspondence with the p non-canonical subgroups of $F[p]$. So $\text{Aut}(F)$ acts on $\mathcal{F}_x$.

If L is a finite extension of $\mathbb{Q}_p$, let Art_L denote the Artin map from L^* to $\text{Gal}(L^{ab}/L)$. Let $D \in \mathbb{Z}^+$ be a quadratic non-residue mod p and $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$.

Theorem 6.5. *Let N_F denote the norm from K^* to $\mathbb{Q}_p \otimes EndF$. If $b \in \mathcal{O}_K^*$ and $Q \in \mathcal{F}_x$, then*

$$w(Art_K(b))Q = N_F(b^{-1})Q.$$

This makes sense because $\operatorname{End} F$ maps naturally into K. Also, if M_3 is the class field over K of the subgroup of K^* given by $(\sqrt{p})^{\mathbb{Z}}\mu_{p^2-1}(1+p\mathcal{O}_K)$, then the non-canonical subgroups of $F[p]$ are defined over M_3 by Proposition 5.3.

Proposition 6.6. *Suppose K is an imaginary quadratic field and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. If E is an elliptic curve with good reduction over the ring of integers R of a finite unramified extension L of $K_\mathfrak{p}$ with CM in K then the formal group of E over R is a relative Lubin-Tate group as defined by de Shalit in [dS2].*

Lemma 6.7. *Suppose E and L are as above and σ is the Frobenius automorphism of $L/K_\mathfrak{p}$. Then there is an isomorphism of $E' := E/\ker(\mathfrak{p}\cap EndE)$ with E^σ so that the reduction of the natural map $\alpha\colon E \to E'$ is Frobenius.*

Proof. This follows from [S, Thm 5.4]. Indeed, identify $\mathbb{C}$ with $\mathbb{C}_\mathfrak{p}$, and take σ to be an automorphism of $\mathbb{C}$ which restricts to $[s, K]$ on K^{ab} where $s_\mathfrak{l} = 1$ for $\mathfrak{l} \neq \mathfrak{p}$ and $(s_\mathfrak{p}) = \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$. Then Shimura's theorem implies that there exists an isomorphism, $\xi\colon E' \xrightarrow{\sim} E^\sigma$, such that if P is a torsion point on E of order prime to $\mathfrak{p}$, $\xi(\alpha(P)) = P^\sigma$. Because σ is a lifting of Frobenius and the points of order prime to $\mathfrak{p}$ reduce to infinitely many distinct points of $E \mod \mathfrak{p}$, the lemma follows. □

Proof. (of proposition) Let $\beta\colon E \to E^\sigma$ be the isogeny of the above lemma. If T is a parameter at the origin on E, let $f(T) = \beta^* T^\sigma$ and $f(T) = \pi' T + \cdots$. Then $f \in \mathcal{F}_{N_{L/K}(\pi')}$ (notation as in [dS2]), and if p_1 and p_2 are the natural projections of $E \times E$ onto E, with $X = p_1^* T$ and $Y = p_2^* T$, then $\hat{E}(X, Y) = F_f(X, Y)$. □

Proposition 6.8. *If E/R has fake CM, then $\hat{E}$ is a relative Lubin-Tate group.*

Proof. Suppose $S \in \mathcal{R}$, $E = (F, \alpha)$ and $\operatorname{End}_R F \cong S$. Then, by Theorem 4.1, we know $\exists \rho \in B^*$, such that $(F, \rho\alpha)$ has CM. □

The theorem now follows from (6.4) of [Iw].

Corollary 6.9. *$M_3 = m_3$.*

Proof. It follows from Corollary 6.3 and the remarks at the end of §6.2 that $M_2 = K^{nr}(\mu_p, p^{1/(p+1)}) \subseteq m_3$. (In general, it follows from Lemma 2 and Theorem 6 of [BLR, §6] that $m_n \subseteq m_{n+1}$.) The theorem implies that $(1 + \sqrt{p}\mathcal{O}_K)/(1 + p\mathcal{O}_K)$ injects into $\mathrm{Gal}(m_3/K)$ via the Artin map. Indeed, if $K_1 = \mathbb{Q}_p(\sqrt{p})$ and $K_2 = \mathbb{Q}_p(\sqrt{pD})$, the map $(N^K_{K_1}, N^K_{K_2})$ from $(1+\sqrt{p}\mathcal{O}_K)/(1+p\mathcal{O}_K)$ to

$$(1 + \sqrt{p}\mathcal{O}_{K_1})/(1 + p\mathcal{O}_{K_1}) \times (1 + \sqrt{pD}\mathcal{O}_{K_2})/(1 + p\mathcal{O}_{K_2})$$

is an isomorphism. □

Remark 6.10. *This implies the existence of a weight 2 newform on $X_0(p^3)$ whose corresponding representation is wildly ramified at p, which has been independently verified by Jared Weinstein.*

Let $\mathcal{D}_x$ be the wide open residue class above x in $\mathbf{SD}_A$ (recall that x is a fixed point of $\overline{w}_\rho$) and $\tilde{\mathcal{D}}_x$ the residue class above $\mathcal{D}_x$ in $\mathbf{Z}_A$. Let $s\colon \mathcal{D}_x \to X_1(p)$ be a section of $X_1(p) \to X_0(p)$ on the image of $\mathcal{D}_x$ as in Lemma 8.6 of [CMc]. For $\zeta \in \mu_p$ we defined an automorphism $\tilde{S}_{s,\zeta}$ of $\tilde{\mathcal{D}}_x$. For $b \in \mathcal{O}_K^*$, let $\nu(b) = 0$ if b is a square and 1 otherwise.

Corollary 6.11. *Suppose $\tilde{x} = (E, C)$. Then there exists an $n_x \in \{0,1\}$ such that for $b \in \mathcal{O}_K^*$*

$$w(Art_K(b))\big|_{C_x} = \overline{\tilde{S}_{s,e_1(P,Q)}}\tau_x^{\nu(b)n_x},$$

where $s(E,C) = (E,P)$, $Q \in E[p]\backslash C$, $e_1(\ ,\ )$ is the Weil pairing on $E[p]$ and $(P+Q) = N_F(b^{-1})(Q)$.

This follows from the theorem and the following lemma whose proof we leave as an exercise for the reader.

Lemma 6.12. *The automorphism group of the affine curve $y^2 = x^p - x$ has order $2(p-1)p$ and is generated by $\alpha : (x,y) \mapsto (x+1, y)$ and $\beta_b : (x,y) \mapsto (ax, by)$, where $a \in \mathbb{F}_p^*$ and $b^2 = a$. These satisfy $\alpha^p = \beta_b^{2(p-1)} = 1$ and $\beta_b \alpha \beta_b^{-1} = \alpha^a$. In particular, there is only one p-Sylow subgroup, and its centralizer is Abelian and generated by α and β_{-1}.*

We will show that $n_x = 1$. Suppose $\sigma \in I$ and $\sigma(\sqrt{p}) = -\sqrt{p}$. Then $w(\sigma)$ on the bridging component above A, which has the equation

$$X^{(p+1)/i(A)} + X^{-(p+1)/i(A)} = Z^p,$$

is $X \to (-1)^{i(A)}X$. When $j(A) \neq 0$ or 1728, this follows from Equation (4) of [CMc, §8]. The general case then follows from Lemma 6.1. As in the proof of Proposition 8.3 of [CMc], the involutions $\overline{\tilde{w}}_\rho$ are

$$(X, Z) \to (\zeta/X, Z),$$

where ζ runs over the $(p+1)/i(A)$-th roots of unity (X^{-p} may be identified with a parameter U on $\mathbf{SD}_A$ so that the involutions $\overline{w}_\rho$ are $U \to \zeta/U$). The fixed points of $\overline{w}_\rho$ on $\overline{\mathbf{SD}}_A$ are the solutions x of $U(x)^2 \equiv \zeta$. We now label the fixed points of the involutions $\overline{w}_\rho$ by the $2(p+1)/i(A)$-th roots of unity. So for each such root of unity ξ, there is a component C_ξ of $\overline{\mathcal{X}_0(p^3)}$. It follows from the above that $w(\sigma)$ restricts to an isomorphism from C_ξ to $C_{(-1)^{i(A)}\xi}$.

The group B^* acts on the part of stable model over A. If $\alpha \in B^*$, let $h(\alpha)$ be the corresponding automorphism of that part of the reduction. If $\sigma \in I$, because the action of B^* is defined over $\mathbb{Q}_p^{nr}$ (and by Lemma 6.1), we have

$$w(\sigma) \circ h(\alpha) = h(\alpha) \circ w(\sigma). \tag{2}$$

Using Lemma 3.6, we see that if $\alpha \in B'$ and $\alpha^2 \in \mathbb{Z}_p^*$, then

$$0 = \alpha^2 - (\alpha')^2 = (\alpha - \alpha')(\alpha + \alpha'),$$

and thus $\alpha = \pm\alpha'$. In particular, we have $\alpha\tilde{x} = \alpha'\tilde{x}$. So

$$w_\rho(\alpha\tilde{x}) = \rho w(\alpha'\tilde{x}) = \rho\alpha w(\tilde{x}),$$

which equals $\alpha\tilde{x}$ if $\alpha\rho = \rho\alpha$ and doesn't equal $\tilde{x}$ if $\alpha \notin \mathrm{Aut}(A)\mathbb{Z}_p^*(1+jB)$. (So for example, if $\rho \in \mathbb{Z}_p[i]$ and $\alpha = i$ and $j(A) \neq 1728$.) Suppose this to be the case (i.e. α satisfies these conditions). Then if $\tilde{x} \sim (F, \iota, C)$, the other fixed point of w_ρ is $\alpha\tilde{x} \sim (F, \alpha\iota, C)$. (This implies Corollary 3.10 in this case.) Let $x' = \overline{\alpha x}$. Then $h(\alpha)$ takes C_x to $C_{x'}$ and vice-versa.

Let $X_\xi = C_\xi \coprod C_{-\xi}$. For $\tau \in I$, identifying C_ξ with $C_{-\xi}$ via $h(\alpha)$ and using (2), we can write

$$w(\tau)|_{X_\xi} = (a(\tau), s(\tau)) \in \mathrm{Aut}(C_\xi) \times \{\pm 1\}$$

where $s(\tau) = \tau(\sqrt{p})/\sqrt{p}$. If $\tau = \mathrm{Art}_K(v)$, it follows that $s(\tau) = 1$. Suppose $s(\sigma) = -1$. Then on X_ξ, on one hand we have

$$w(\sigma)w(\tau)w(\sigma^{-1}) = w(\sigma\tau\sigma^{-1}) = (a(\tau^{-1}), 1),$$

and on the other we have

$$w(\sigma)w(\tau)w(\sigma^{-1}) = (a(\sigma)a(\tau)a(\sigma^{-1}), 1).$$

It follows that $a(\sigma)$ is not in the commutative subgroup (α, β_{-1}) of $\mathrm{Aut}(y^2 = x^p - x)$. This implies $a(\sigma)^2 \notin (\alpha)$ so $n_x = 1$. Thus, in particular, there exists σ such that $s(\sigma) = -1$, $a(\sigma) = \beta_\epsilon$, where $\epsilon^2 = -1$.

Suppose now that $j(A) = 1728$. Let ξ be a $(p+1)/2$-th root of unity and $X = C_\xi$. It follows that if $\sigma \in I$, $w(\sigma)(X) = X$. Let $L = \mathrm{End}\, F \otimes \mathbb{Q}_p$. We know X is a double cover of $\mathbf{P}^1$ and its branch points correspond to non-canonical subgroups of $F[p]$. Moreover, if Q is such a subgroup and $b \in \mathcal{O}_L^*$, we have

$$w(\mathrm{Art}_L(b))Q = b^{-1}Q.$$

In particular, $w(\mathrm{Art}_L(\mathbb{Z}_p^*(1+p\mathcal{O}_L)))$ is the identity. Now suppose that $\sigma|_L \neq id$. Then

$$\sigma\mathrm{Art}_L(b) = \mathrm{Art}_L(\bar{b})\sigma.$$

So if $\tau = \mathrm{Art}_L(b)$, then

$$w(\sigma)w(\tau)w(\sigma)^{-1} = w(\tau)^{-1}.$$

It follows from the theorem and Lemma 6.12 that if the order of $w(\sigma)$ is prime to p, $w(\sigma^2) = w(\sigma)^2 = \tau_x$ and thus $n_x = 1$.

7 Stable Model of $X_0(p^3)$ when $p < 13$

Recall from Section 2 that the argument which we used in [CMc] to compute the stable model of $X_0(p^3)$ does not only apply when $p < 13$. The reason for this is that in these cases there is no supersingular region where one can apply analysis of de Shalit, as restated in Theorem 2.2, which approximates the forgetful map from $X_0(p)$ to $X(1)$. In this section, we recall in greater detail how the theorem is used to construct components in the supersingular regions of $X_0(p^2)$ and $X_0(p^3)$ when $p \geq 13$. We then use explicit equations for $X_0(p)$ when $p = 5$, 7, and 11, to derive formulas analogous to Theorem 2.2, and subsequently construct the analogous stable reduction components. This should serve not only to extend the result of [CMc] to $p > 3$, but also to make the construction more understandable and concrete.

7.1 Explicit Analysis of a "Good" Supersingular Region

Suppose that $p > 13$, and hence by the result of Howe that there is a supersingular $A/\mathbb{F}_p$ with $j(A) \neq 0, 1728$. All of the information from Theorem 2.2 which we need to do the explicit analysis of [CMc] can be summarized as follows. First of all, we have parameters, t and s, on $W_A(p)$ and $W_A(1)$ (respectively), which identify these regions with the annulus, $0 < v(t) < 1$, and the disk, $v(s) > 0$. Moreover, in terms of these parameters, the maps π_f and w_1 satisfy

$$w_1(t) = \frac{\kappa}{t} \qquad \text{and} \qquad s = \pi_f(t) \equiv t + \left(\frac{\kappa}{t}\right)^p \pmod{p},$$

for some $\kappa \in W(\mathbb{F}_{p^2})$ with $v(\kappa) = 1$. Finally, the three special circles inside $W_A(p)$, namely $\mathbf{TS}_A$, $\mathbf{SD}_A$, and $\mathbf{C}_A$, are described by $v(t) = \frac{p}{p+1}$, $v(t) = \frac{1}{2}$, and $v(t) = 1 - \frac{1}{2p}$ (respectively).

Using the above information, we now recall briefly how to explicitly calculate the reduction of the affinoid, $\mathbf{Y}_A := \pi_\nu^{-1}(\mathbf{TS}_A) \subseteq W_A(p^2)$. First of all, we show in [CMc, Lemma 5.1] that $\mathbf{Y}_A$ is isomorphic to the rigid space:

$$T_A := \{\ (x, y) \in \mathbf{TS}_A \times \mathbf{TS}_A \mid x \neq y,\ \pi_f(x) = \pi_f(y)\ \}.$$

Then we take $u, v = \alpha^p/t$ as parameters on two copies of $\mathbf{TS}_A$, for any α with $v(\alpha) = \frac{1}{p+1}$. With these parameters, the condition that $\pi_f(x) = \pi_f(y)$ leads to the following congruence.

$$u^{-1} - v^{-1} \equiv (v^p - u^p)(\kappa/\alpha^{p+1})^p \pmod{\alpha}.$$

By making the change of variables $s = 1/(v - u)$ and $r = (v + u)/(v - u)$, we disregard the $u = v$ component and arrive at an isomorphism between $\overline{\mathbf{Y}}_A$ and an affine curve of the form $s^{p+1} = c(r^2 - 1)$. Note that this equation also ends up describing the reductions of the affinoids, $\mathbf{E}_{1A}, \mathbf{E}_{2A} \subseteq W_A(p^3)$, which lie over $\mathbf{Y}_A$ via π_f and π_ν (see [CMc, Remark 9.3]).

Similarly, we compute the reduction of $\mathbf{Z}_A := \pi_{11}^{-1}(\mathbf{SD}_A) \subseteq W_A(p^3)$ by first identifying it with the rigid space:

$$S_A := \{\ (x, y) \in \mathbf{C}_A \times \mathbf{C}_A \mid \tau_f(x) = w_1 \circ \tau_f(y)\ \}$$

(this is done in [CMc, Prop 7.1]). Recall that $\tau_f : \mathbf{C}_A \to \mathbf{SD}_A$ is the map which takes (E, C) to $(E, H_1(E))$, and hence that $\pi_f \circ \tau_f = \pi_f$. Therefore, in terms of the parameter t from above, it is easy to show that

$$\tau_f(t) \equiv t + (\kappa/t)^p \pmod{p}.$$

Now we may proceed as before, taking $U = t/\sqrt{\kappa}$ as a parameter on $\mathbf{SD}_A$ (note that $w_1(U) = 1/U$), and taking $X, Y = t/\alpha$ as parameters on two copies of $\mathbf{C}_A$, for any α with $v(\alpha) = 1 - \frac{1}{2p}$. With a careful choice of α (see [CMc, Prop 8.2]), the definition of S_A translates into the following congruence.

$$(X^{-p} + \alpha X/\sqrt{\kappa})(Y^{-p} + \alpha Y/\sqrt{\kappa}) \equiv 1 \pmod{\sqrt{p}}$$

Finally, after a second change of variables of the form, $Z = c(XY - 1)$, we obtain the following equation for $\overline{\mathbf{Z}}_A$.

$$X^{p+1} + X^{-(p+1)} = Z^p$$

Once again, when $p < 13$, the preceding calculations do not apply because there is no such A. So for the specific primes, $p = 5$, 7, and 11, we will now derive a formula which is analogous to Theorem 2.2 for each supersingular region, and then use it to compute the reductions of $\mathbf{Y}_A$ and $\mathbf{Z}_A$ (as above). In each case, we do arrive at equations which are consistent with Theorem 2.5. Our claim is that the rest of the argument of [CMc] (as summarized in Section 2) is completely analogous for these primes, and need not be repeated. As a final note, we do not address $X_0(8)$ and $X_0(27)$ primarily because both have good reduction. Additionally, complications arise from the fact that $j = 0$ and $j = 1728$ lie in the same residue disk of $X(1)$ in both cases.

7.2 $X_0(5^3)$

Borrowing directly from [M1, §4], we can choose a parameter on the genus 0 curve, $X_0(5)$, by taking $t = \eta_1^6/\eta_5^6$. The only supersingular j-invariant is $j = 0$, and the corresponding annulus is described by $0 < v(t) < 3$. Furthermore, from [M1, Table 3], the formulas for the forgetful map and Atkin-Lehner involution are then given by

$$\pi_f^* j = \frac{(t^2 + 2 \cdot 5^3 t + 5^5)^3}{t^5} \qquad \text{and} \qquad w_1^* t = 125/t.$$

The circles $\mathbf{SD}$ and $\mathbf{C}$ are described by $v(t) = 1.5$ and $v(t) = 2.7$ (respectively), and the too-supersingular circle, $\mathbf{TS}$, is where $v(t) = 2.5$.

First we compute the reduction of the affinoid, $\mathbf{Y} := \pi_\nu^{-1}(\mathbf{TS}) \subseteq X_0(25)$, by embedding it into $\mathbf{TS} \times \mathbf{TS}$ as above. For parameters on two copies of $\mathbf{TS}$, we may choose $X, Y = t/(25\sqrt{5})$. Then plugging these parameters into the equation, $\pi_f(x) = \pi_f(y)$, we quickly arrive at the congruence:

$$(X^2 + 1)^3/X^5 \equiv (Y^2 + 1)^3/Y^5 \pmod{\sqrt{5}}.$$

From the definition of T_A, we are interested only in the component where $X \neq Y$, and by letting $X = s/(r-1)^3$ and $Y = s/(r+1)^3$ we see that this is isomorphic to the affine curve:

$$s^2 = r^2 - 1. \tag{3}$$

Now we compute the reduction of $\mathbf{Z} := \pi_{1\,1}^{-1}(\mathbf{SD}) \subseteq X_0(125)$ by means of the embedding into $\mathbf{C} \times \mathbf{C}$. We need an approximation for $\tau_f : \mathbf{C} \to \mathbf{SD}$, and from the above formula for π_f, it is easy to show that

$$\tau_f(t) \equiv \frac{5^{15}}{t^5} + \frac{3 \cdot 5^{10}}{t^3} \pmod{5^2}.$$

As in [CMc, §8.1], we need to work over a larger extension of $\mathbb{Z}_5$ to define and compute the reduction of $\mathbf{Z}$. In particular, it suffices to work over $R := \mathbb{Z}_5[\beta, \sqrt{5}]$, where $\beta \in \mathbb{C}_5$ is chosen so that $\beta^{25} \equiv 5 \pmod{5\sqrt{5}}$. For parameters on $\mathbf{SD}$ and (both copies of) $\mathbf{C}$, we then choose the functions $U = t/(5\sqrt{5})$ and $X, Y = t/(25\beta^5\sqrt{5})$. Using these parameters and our formula for τ_f, the equation $\tau_f(x) = w_1 \circ \tau_f(y)$ then leads to the following congruence.

$$\left(\frac{1}{X^5} + \frac{3\beta^{10}}{X^3}\right)\left(\frac{1}{Y^5} + \frac{3\beta^{10}}{Y^3}\right) \equiv 1 \pmod{\sqrt{5}}$$

After making the substitution, $Z = (XY-1)/(3\beta^2)$, we arrive at our final equation for $\overline{\mathbf{Z}}$.

$$X^2 + X^{-2} = Z^5 \tag{4}$$

Remark 7.1. *Note that Equations* (3) *and* (4)*, describing* $\overline{\mathbf{Y}}$ *and* $\overline{\mathbf{Z}}$*, are consistent with Theorem 2.5, since* $p = 5$ *and* $i(A) = 3$ *in this case.*

7.3 $X_0(7^3)$

This is very similar to the previous example, as $X_0(7)$ also has genus 0 and only one supersingular annulus corresponding to $j = 1728$. If we take $t = \eta_1^4/\eta_7^4$ as a parameter (see [M1, §2]), the supersingular annulus is the region described by $0 < v(t) < 2$, and the formulas for the forgetful map and Atkin-Lehner involution are as follows.

$$\pi_f^*(j - 1728) = \frac{(t^4 - 10 \cdot 7^2 t^3 - 9 \cdot 7^4 t^2 - 2 \cdot 7^6 t - 7^7)^2}{t^7} \qquad w_1^* t = \frac{49}{t}$$

The circles, $\mathbf{SD}$ and $\mathbf{C}$, are now given by $v(t) = 1$ and $v(t) = 13/7$ (respectively), and $\mathbf{TS}$ is the circle where $v(t) = 7/4$.

We begin by embedding $\mathbf{Y} := \pi_\nu^{-1}(\mathbf{TS}) \subseteq X_0(49)$ into $\mathbf{TS} \times \mathbf{TS}$, taking $X, Y = \alpha t/49$ as parameters on both copies of $\mathbf{TS}$, where $\alpha^4 = -7$. With these parameters, the equation $\pi_f(x) = \pi_f(y)$ yields the congruence:

$$(X^4 + 1)^2/X^7 \equiv (Y^4 + 1)^2/Y^7 \pmod{\alpha}.$$

Then the substitution, $X = s/(r-1)^2$ and $Y = s/(r+1)^2$, defines an isomorphism between the component with $X \neq Y$ and the genus 1 affine curve:

$$s^4 = r^2 - 1. \tag{5}$$

Likewise we compute the reduction of $\mathbf{Z}$ by embedding it into $\mathbf{C} \times \mathbf{C}$. This time the approximation formula for $\tau_f : \mathbf{C} \to \mathbf{SD}$, which we derive from the formula for π_f, is as follows.

$$\tau_f(t) \equiv \frac{7^{14}}{t^7} - \frac{2 \cdot 7^7}{t^3} \pmod{7\sqrt{7}}$$

Working over the extension given by $R = \mathbb{Z}_7[\beta]$ with $\beta^{49} \equiv 7 \pmod{7\sqrt{7}}$, we take $X, Y = \beta^7 t/49$ as parameters on two copies of $\mathbf{C}$. We also take $U = t/7$ as our parameter on $\mathbf{SD}$. Then the equation $\tau_f(x) = w_1 \circ \tau_f(y)$ gives us the congruence:

$$\left(\frac{1}{X^7} - \frac{2\beta^{21}}{X^3}\right)\left(\frac{1}{Y^7} - \frac{2\beta^{21}}{Y^3}\right) \equiv 1 \pmod{\sqrt{7}}.$$

To complete the calculation, we make the substitution, $Z = (1 - XY)/(2\beta^3)$, which results in our final equation for $\overline{\mathbf{Z}}$.

$$X^4 + X^{-4} = Z^7 \tag{6}$$

Remark 7.2. *Once again, note that Equations* (5) *and* (6) *are consistent with Theorem 2.5, as $p = 7$ and $i(A)$ is now* 2.

7.4 $X_0(11^3)$

When $p = 11$, $X_0(p)$ has genus 1 and two supersingular annuli corresponding to $j = 0$ and $j = 1728$. In order to work out formulas for the forgetful map on these supersingular regions, we must choose an appropriate model for the overall curve. One convenient model relates the following two functions.

$$t = \left(\frac{\eta_1}{\eta_{11}}\right)^{12} \qquad\qquad x = \frac{dt/t}{(\eta_1\eta_{11})^2}$$

The first function has divisor $5(0) - 5(\infty)$, and the second is a degree 2 function with a simple pole at each cusp. Since w_1 interchanges the two cusps, it follows that x is actually a parameter on the genus 0 quotient, $X_0(11)^+ := X_0(11)/w_1$. Therefore, t must be quadratic over x, and indeed by comparing q-expansions we have the equation:

$$t^2 + \frac{1}{5^5}(x^5 + 170x^4 + 9345x^3 + 167320x^2 - 7903458)t + 11^6 = 0.$$

This model is singular, but we can normalize by adjoining a square root of the discriminant. In particular, the following gives a nonsingular model for $X_0(11)$.

$$y = \frac{2 \cdot 5^5 t + (x^5 + 170x^4 + 9345x^3 + 167320x^2 - 7903458)}{(x+47)(x^2+89x+1424)}$$

$$y^2 = f(x) = (x-8)(x^3+76x^2-8x+188)$$

Remark 7.3. *Since x is invariant under w_1, the formulas for the Atkin-Lehner involution are given by $w_1^* t = 11^6/t$ and $w_1^* y = -y$.*

Note that there are two pairs of branch points in the degree two extension from $X_0(11)^+$ up to $X_0(11)$, and they lie in the two residue disks where $v(x-2) > 0$ and $v(x+3) > 0$. It follows that the regions lying over these residue disks are annuli. In fact, from [DR, §VI 6.16] (or the explicit calculations which follow) these are precisely the two supersingular annuli.

7.4.1 $j = 0$

Let r_1, r_2 be the two roots of $f(x)$ close to $x = -3$, and let s_1, s_2 be those close to $x = 2$. Then the following map defines an isomorphism (over $\mathbb{Q}_{11}$) between the annulus, $0 < v(z) < 3$, and the subspace of $X_0(11)$ which lies over the residue disk, $v(x-2) > 0$.

$$\begin{aligned}
x &= z + \frac{(s_1+s_2)}{2} + \frac{(s_1-s_2)^2}{16z} \equiv z + 310 - 212\left(\frac{11^3}{z}\right) \pmod{11^3} \\
y &= \left(-z + \frac{(s_1-s_2)^2}{16z}\right)\sqrt{(x(z)-r_1)(x(z)-r_2)} \\
&\approx \left(-z - 212\left(\frac{11^3}{z}\right)\right)\left(\cdots + 484\left(\frac{11^3}{z}\right)^3 + 363\left(\frac{11^3}{z}\right)^2 + \right. \\
&\qquad \left. 393\left(\frac{11^3}{z}\right) + 775 + 243z + 484z^2 + 968z^3 + \cdots\right)
\end{aligned}$$

To obtain an approximation formula for π_f over the annulus, we begin with the following explicit formula (easily verified by q-expansions).

$$\pi_f^* j = \frac{(60y + 61x^2 + 864x - 2016)^3}{5^6 t}$$

Over the whole annulus, $60y + 61x^2 + 864x - 2016$ is well approximated by $5z - 11^{11}/z^3$, in the sense that the error is always strictly smaller than the larger of these two terms. Similarly, t is always close to $-4z^2$. From this we may conclude that $v(j) > 0$ over the whole annulus (as claimed).

Now we are able to embed $\mathbf{Z} \subseteq X_0(11^3)$ into $\mathbf{C} \times \mathbf{C}$ and explicitly compute its reduction. We know that the circles, $\mathbf{SD}$ and $\mathbf{C}$, are described by $v(z) = 3/2$ and $v(z) = 63/22$ (respectively). So our formula for π_f leads to the following approximation for $\tau_f : \mathbf{C} \to \mathbf{SD}$ in terms of z.

$$\tau_f(z) \equiv \frac{-3 \cdot 11^{33}}{z^{11}} + \frac{11^{22}}{z^7} \pmod{11^2}.$$

Also, from the fact that $x(z)$ must be fixed by w_1, we see that

$$w_1(z) = \frac{(s_1 - s_2)^2}{16z} \equiv \frac{-3 \cdot 11^3}{z}.$$

At this point our analysis closely parallels that of the two previous examples. In particular, let $R = \mathbb{Z}_{11}[\sqrt{-11}, \beta]$ where $\beta \in \mathbb{C}_{11}$ satisfies $\beta^{121} \equiv -11 \pmod{11\sqrt{-11}}$, and choose the following functions as parameters on **SD** and (two copies of) **C**.

$$U = \frac{2z}{11\sqrt{-11}} \qquad X, Y = \frac{-2z}{121\beta^{44}\sqrt{-11}}$$

In terms of these new parameters, the relation $\tau_f(x) = w_1 \circ \tau_f(y)$ leads to the following congruence.

$$\left(\frac{1}{X^{11}} + \frac{3\beta^{55}}{X^7}\right)\left(\frac{1}{Y^{11}} + \frac{3\beta^{55}}{Y^7}\right) \equiv 1 \pmod{\sqrt{-11}}$$

Finally, with the substitution, $Z = (XY - 1)/(3\beta^5)$, we obtain the desired equation for the reduction of **Z** over R.

$$X^4 + X^{-4} = Z^{11}$$

Similarly, the equation for the $(j = 0)$ supersingular component of $X_0(11^2)$ follows directly from the embedding of **Y** into **TS** × **TS** (where **TS** is now the circle, $v(z) = 11/4$). The approximating formula for π_f on that circle is

$$j = \pi_f(z) \equiv \frac{(5z - 11^{11}/z^3)^3}{5^6(-4z^2)} \pmod{11^3}.$$

So now let $\alpha^2 = \sqrt{-11}$ and take as parameters on both copies of **TS** the functions $X, Y = \alpha z/(5 \cdot 11^3)$. Then the relation $\pi_f(x) = \pi_f(y)$ reduces to

$$(X^4 + 1)^3/X^{11} \equiv (Y^4 + 1)^3/Y^{11} \pmod{\alpha}.$$

The irreducible component of this curve where $X \neq Y$ is then isomorphic to the genus 1 curve, $s^4 = r^2 - 1$, by the following map.

$$X = s/(r-1)^3 \qquad Y = s/(r+1)^3$$

Remark 7.4. *These equations match those of Theorem 2.5 when* $p = 11$ *and* $i(A) = 3$.

7.4.2 $j = 1728$

The supersingular annulus of $X_0(11)$ corresponding to $j = 1728$ is the region which lies over the residue disk, $v(x + 3) > 0$. To see this, we first parameterize the region using the annulus, $0 < v(z) < 2$, and the following map.

$$\begin{aligned}
x &= z + \frac{(r_1+r_2)}{2} + \frac{(r_1-r_2)^2}{16z} \equiv z + 2318 + 12356\left(\frac{11^2}{z}\right) \pmod{11^4}\\
y &= \left(-z + \tfrac{(r_1-r_2)^2}{16z}\right)\sqrt{(x(z)-s_1)(x(z)-s_2)}\\
&\approx \left(-z + 12356\left(\frac{11^2}{z}\right)\right)\left(\cdots + 5324\left(\frac{11^2}{z}\right)^3 + 3993\left(\frac{11^2}{z}\right)^2 + \right.\\
&\qquad\qquad \left. 4370\left(\frac{11^2}{z}\right) + 6001 + 11980z + 5324z^2 + 3993z^3 + \cdots\right)
\end{aligned}$$

Then we choose an explicit formula for the forgetful map which is convenient for analysis near $j = 1728$, in particular

$$\pi_f^*(j-1728) = \frac{(665x^3 + 666xy + 22680x^2 + 2592y - 120960x + 22680)^2}{5^6 t}.$$

Over the entire annulus, the cubic function in the numerator is well approximated (in the above sense) by $5z^2 - 3\cdot 11^{11}/z^4$, and t is well approximated by $-3z^3$. Therefore by counting valuations it follows that $v(j-1728) > 0$ over the entire annulus, as claimed.

As in the previous examples we now compute the equations for the bridging component of $X_0(11^3)$ and supersingular component of $X_0(11^2)$ corresponding to $j = 1728$. By approximating π_f on **C** (where $v(z) = 21/11$) and **SD** (where $v(z) = 1$), we find the following formula for τ_f in terms of z.

$$\tau_f(z) \equiv 3\left(\frac{11^2}{z}\right)^{11} + 11\left(\frac{11^2}{z}\right)^5 \pmod{11\sqrt{11}}$$

After an appropriate choice of parameters on **C** and **SD**, this leads to the equation,

$$X^6 + X^{-6} = Z^{11},$$

which describes the bridging component. Then on the too-supersingular circle, where $v(z) = 11/6$, we approximate π_f by

$$j - 1728 = \pi_f(z) \equiv \frac{(5z^2 - 3\cdot 11^{11}/z^4)^2}{5^6(-3z^3)} \pmod{11^2}.$$

After making an appropriate change of variables, this leads to the equation which one should expect for $\overline{\mathbf{Y}}$:

$$s^6 = r^2 - 1.$$

8 Stable Model of $X_0(Np^3)$

Intuitively, one might expect the stable model of $X_0(Np^3)$ (when $(N,p) = 1$) to follow fairly directly from the stable model of $X_0(p^3)$. Indeed, $X_0(Np^3)$ is birational to $X_0(p^3) \times_{X(1)} X_0(N)$, and $X_0(N)$ has good reduction. Using semi-stable maps (as in [C2]) to make this line of reasoning precise, we are able to show the following (compare with Theorem 2.5).

Theorem 8.1. *The stable reduction of $X_0(Np^3)$ has six ordinary components: two isomorphic to $X_0(N)$ and four isomorphic to (the normalization of) $Ig(p)\times X_0(N)$. Also, for each supersingular point P of $X_0(N)$, there is a "necklace" of components whose graph is given below in Figure 2. Set $i(P) = 2$ or 3 if P is elliptic and $j(P) = 1728$ or 0 (respectively). Set $i(P) = 1$ otherwise. Then $E_{2,P}$ and $E_{1,P}$ are isomorphic to $y^2 = x^{(p+1)/i(P)} + 1$, while Z_P is crossed by $2(p+1)/i(P)$ components isomorphic to $y^2 = x^p - x$.*

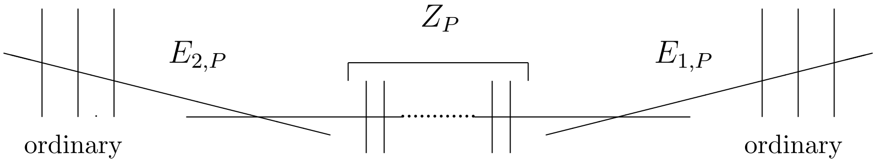


Figure 2: Partial Graph of the Stable Reduction of $X_0(Np^3)$

Corollary 8.2. *The stable reduction of the p-new part of the Jacobian of $X_0(Np^3)$ has $c_N(p^2-1)/6$ copies of the Jacobian of $y^2 = x^p - x$, where $c_N = [\Gamma : \Gamma_0(N)]$.*

8.1 Semi-stable Maps

We begin by giving the definition of semi-stable map, and by proving the lemma which will form the blueprint for our overall construction.

Definition 8.3. *Let $K \subseteq \mathbb{C}_p$ be a complete subfield with ring of integers R. Then $f : X \to Y$ is a semi-stable map over R, if X/R and Y/R are semi-stable (as in [CMc, Definition 2.6]) and f is finite. In this case we say that f extends the restriction map, $f_K : X_K \to Y_K$, on generic fibers.*

Lemma 8.4. *Let $f : X \to Z$ and $g : Y \to Z$ be semi-stable maps over R. Suppose that the following conditions hold.*
(i) $\bar{X}$ and $\bar{Y}$ have (only) smooth components.
(ii) f and g take singular points to singular points (and vice-versa).
(iii) For each pair, (x_i, y_i), of singular points in $\bar{X}$ and $\bar{Y}$ with $f(x_i) = g(y_i)$, $A_{x_i} \times A_{y_i}$ is the disjoint union of annuli (over K), where $A_P = red^{-1}(P)$.

(iv) For each pair, (X_i, Y_i), of components of $\bar{X}$ and $\bar{Y}$ with $f(X_i) = g(Y_i)$, $X_i \times Y_i$ is irreducible, and smooth away from all the points from (iii).
Then $f \times g : X \times Y \to Z$ is a semi-stable map (over R), and in particular $X \times Y$ is semi-stable.

Proof. Choose any pair (X_i, Y_i) of irreducible components of $\bar{X}$ and $\bar{Y}$ with $f(X_i) = g(Y_i)$. Let $W_i = \mathrm{red}^{-1}(X_i) \times \mathrm{red}^{-1}(Y_i)$ and $A_i = \mathrm{red}^{-1}(X_i^{\mathrm{ns}}) \times \mathrm{red}^{-1}(Y_i^{\mathrm{ns}})$. Then (i)-(iv) guarantee that each W_i is a basic wide open (as in [CMc, §2]. Furthermore, the W_i's forms a semi-stable covering of $X_K \times Y_K$, and then it follows from [CMc, Prop 2.7] that $X \times Y$ is semi-stable. Finiteness of $f \times g$ is immediate. □

Remark 8.5. *We will apply Lemma 8.4 to semi-stable extensions of the forgetful maps from $X_0(p^3)$ and $X_0(N)$ to $X(1)$, but with one caveat. Technically, condition (iv) will fail at all points of the form $(P, Q) \in X_0(p^3) \times X_0(N)$ where P and Q lie over $j = 0$ (or $j = 1728$) and both ramify. This issue can basically be ignored, however, as these singularities are resolved in $X_0(Np^3)$.*

8.2 Semi-stable Extensions of the Forgetful Map

We begin by constructing a semi-stable map which extends $\pi_f : X_0(p^3) \to X(1)$ (as in the main theorem of [C2]). This can be done by starting with the stable models for $X_0(p^3)$ and $X(1)$ (say, $\mathrm{Spec}(\mathbb{Z}_p[j])$) and performing a series of blow-ups. At each step, we choose a component of $X_0(p^3)$ which has finite image in $X(1)$. There is a unique minimal way to blow-up our models for $X(1)$ and $X_0(p^3)$ so that this component no longer has finite image and so that π_f still extends. After finitely many steps, the process terminates and we have our semi-stable map. A partial picture of this map (showing one supersingular region only) is given below in Figure 3, and the components in the final models for $X_0(p^3)$ and $X(1)$ can be described in words as follows.

First of all, the ordinary regions of $X_0(p^3)$ and $X(1)$ are unchanged. In other words, the final model for $X_0(p^3)$ still has six ordinary components corresponding to the six ordinary affinoids, $\mathbf{X}^{\pm}_{a\,b}$ (defined in §2), and these all map onto the same component of $X(1)$. For each supersingular elliptic curve, A, the special fiber of $X(1)$ also contains a "necklace" of trivial components. More specifically, each necklace contains a chain of four components which correspond to the circles (and disk) where $h(E) = \frac{1}{p(p+1)}$, $h(E) = \frac{1}{2p}$, $h(E) = \frac{1}{p+1}$, and $h(E) \geq \frac{p}{p+1}$ (as in §2.1). Intersecting the second of these we also have $2(p+1)/i(A)$ components which correspond to residue classes within that circle. The components in our final model for $X_0(p^3)$ can be given similar descriptions, i.e. we can describe the components within a fixed supersingular region by describing points of the corresponding affinoids in moduli-theoretic terms. Remember that these affinoids should map onto the ones which were just described for $X(1)$ via the forgetful map.

$$\begin{aligned}
\mathbf{E}_{2,A} &= \{\ (E,C) \mid h(E) = \tfrac{1}{p(p+1)},\ pC = K_2(E)\ \} \\
\mathbf{Z}_A &= \{\ (E,C) \mid h(E) = \tfrac{1}{2p},\ pC = K_2(E)\ \} \\
&\qquad \text{(with its } 2(p+1)/i(A) \text{ nontrivial residue classes)} \\
\mathbf{E}_{1,A} &= \{\ (E,C) \mid h(E) = \tfrac{1}{p+1},\ p^2C = K_1(E)\ \} \\
W^{\pm}_{1,2} &\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{2p},\ |C \cap K_2(E)| = p\ \} \\
&\qquad \text{(also blow-up } 2(p+1)/i(A) \text{ residue classes)} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{p(p+1)},\ |C \cap K_2(E)| = p\ \} \\
W_{0,3} &\supseteq \{\ (E,C) \mid h(E) = \tfrac{p}{p+1}\ \} \text{ (so } E \text{ is too-ss)} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{p+1},\ |C \cap K_1(E)| = 1\ \} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{2p},\ |C \cap K_2(E)| = 1\ \} \\
&\qquad \text{(also blow-up } 2(p+1)/i(A) \text{ residue classes)} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{p(p+1)},\ |C \cap K_2(E)| = 1\ \}
\end{aligned}$$

Remark 8.6. *Recall that $W^{\pm}_{a\,b}$ is a wide open neighborhood of the ordinary affinoid, $\mathbf{X}^{\pm}_{a\,b}$, which extends into the supersingular locus (see [CMc, §3.2]).*

In order to apply Lemma 8.4, we also need to construct a semi-stable map extending $\pi_f : X_0(N) \to X(1)$ (involving the same model for $X(1)$). Basically, we start with the good reduction model for $\pi_f : X_0(N) \to X(1)$. Then every time we blow-up $X(1)$ (as above), this forces a blow-up of $X_0(N)$ so that π_f still extends. Again the ordinary locus of $X_0(N)$ is unchanged. To understand the supersingular regions, consider $\pi_f : X_0(N) \to X(1)$ first as a map of smooth curves over $\overline{\mathbb{F}}_p$, and let P be a point of $X_0(N)$ such that $\pi_f(P)$ is supersingular. If P does not ramify, π_f must restrict to an isomorphism on the corresponding residue class of $X_0(N)$. The only other option is that either $e(P) = 3$ and $j(\pi_f(P)) = 0$, or $e(P) = 2$ and $j(\pi_f(P)) = 1728$. There are two key points to make in either case. First of all, the corresponding residue class of $X_0(N)$ (over $\mathbb{C}_p$) is an extension of a disk which is ramified (totally) at exactly one point (degree 2 if $j = 1728$, degree 3 if $j = 0$). Hence, the extension can be generated analytically by adjoining either $\sqrt{j - 1728}$ or $\sqrt[3]{j}$. Secondly, when $j = 0$ or 1728 is supersingular, it is necessarily too-supersingular. Hence it reduces to a smooth point on the innermost component of its residue class in our final model for $X(1)$. Therefore, like its image in $X(1)$, the residue class of $X_0(N)$ corresponding to such a P contains a chain of 4 components on which π_f is given locally by $t \to t^2$ or $t \to t^3$. The "bridging component" then intersects $2(p+1)$ copies of $\mathbf{P}^1$, which map $2:1$ or $3:1$ onto analogous components of $X(1)$.

To summarize the semi-stable extensions of both forgetful maps to $X(1)$, a picture of the special fibers is now given below in Figure 3. Once again, the graph shows the entire ordinary locus, but only one supersingular region for each curve.

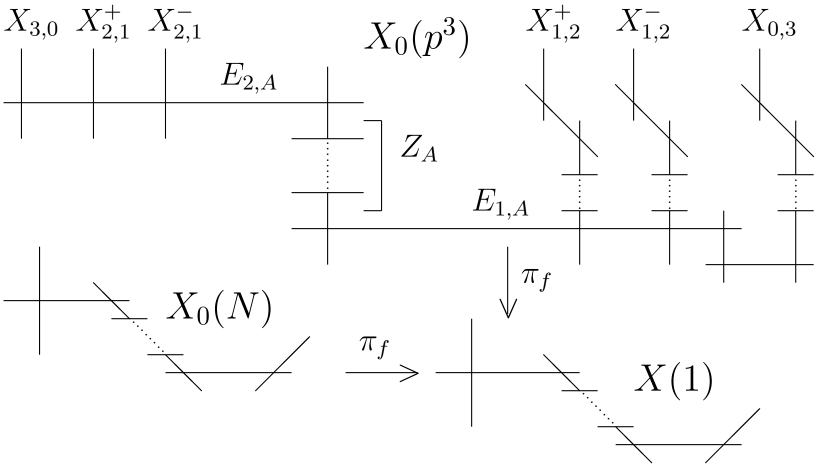


Figure 3: Partial Graph of Semi-Stable Maps from $X_0(p^3)$ and $X_0(N)$ to $X(1)$

8.3 Crossing the Semi-Stable Maps

At this point the proof comes down to verifying the hypotheses of Lemma 8.4 and computing the products of irreducible components with common image. The first two hypotheses follow immediately from the construction. To verify condition (iii), we first observe that $\pi_f : X_0(N) \to X(1)$ can only ramify over $j = 0$, 1728, or ∞, all of which have smooth reduction on our model for $X(1)$. Furthermore, each supersingular residue class of $X_0(N)$ maps with total degree at most 3. Therefore, for any pair of double points, (x, y) (as in the lemma), the corresponding product of annuli, $A_x \times A_y$, is an unramified extension of some annulus of $X_0(p^3)$ with degree less than p. Hence it can only be the disjoint union of annuli by [CMc, Lemma 3.3].

Now we compute the products of the irreducible components, starting with the ordinary locus. When we cross $X_0(N)$ with the reduction of $X_{3,0}$, we are essentially crossing with $\mathbf{P}^1$ trivially (as π_f has degree 1 on $X_{3,0}$). So we simply get a copy of $X_0(N)$. When we cross $X_0(N)$ with the reduction of $X_{2,1}^{\pm}$, we get the curve $Ig(p) \times X_0(N)$ which is at least irreducible from [E1, Thm 2.1.2]. Recall that $Ig(p)/X(1)$ is a degree $(p-1)/2$ extension which is totally ramified over supersingular points, ramified with index 3 or 2 when $j = 0$ or 1728 is ordinary, and unramified elsewhere. Hence the only singular points of $Ig(p) \times X_0(N)$ can be ignored as a result of Remark 8.5. The remaining ordinary components can be dealt with by applying an appropriate Atkin-Lehner involution.

Next we consider a fixed supersingular region corresponding to a point P of $X_0(N)$ (as above). If $j(P) \neq 0, 1728$, or if P is an elliptic point, there's nothing to do, since $\pi_f : X_0(N) \to X(1)$ must be an isomorphism on the residue class corresponding to P. But now suppose that $j(P) = 0$ or 1728, and P is not elliptic. By [E2, 2.3.1] we can choose parameters on $E_{2,A}$ so that it has the equation,

$$y^2 = x^{\frac{p+1}{i(A)}} + 1.$$

Furthermore, the two infinite points are where $E_{2,A}$ meets $X_{3,0}$ and Z_A, and $(0, \pm 1)$ are the points where $E_{2,A}$ meets $X^{\pm}_{2,1}$. The forgetful map induces a degree p map on $E_{2,A}$ which has ramification indices of 1, $(p-1)/2$, and p at the intersections with $X_{3,0}$, $X^{\pm}_{2,1}$, and Z_A. Therefore, if t is a parameter on the image of $E_{2,A}$ in $X(1)$, with $t = 0$ and ∞ at the double points, it follows that

$$\pi_f^* t = \frac{c x^{\frac{p-1}{2}}}{(y - x^{\frac{p+1}{2i(A)}})^{i(A)}}.$$

Now, we have already seen that the extension from $X(1)$ up to $X_0(N)$ is equivalent to adjoining an $i(A)$-th root of t in this case. Hence one can show that the extension of $E_{2,A}$ can be obtained by adjoining an $i(A)$-th root of x. Subsequently, by a change of coordinates, the component lying over $E_{2,A}$ in $X_0(Np^3)$ will have the equation, $y^2 = x^{p+1} + 1$. The argument for the remaining components is very similar. For example, on the bridging component, Z_A, we may choose a parameter x such that it meets $E_{1,A}$ and $E_{2,A}$ at 0 and ∞, and such that π_f is given by $t = x^p$. Adjoining an $i(A)$-th root of t then generates the same extension as adjoining an $i(A)$-th root of x. Thus we obtain a bridging component, Z_P, as in the statement of the theorem, which is crossed by $2(p+1)$ components that lie $i(A) : 1$ over their counterparts on Z_A. At this point the remaining components can be computed in a similar manner, or dealt with by applying an appropriate Atkin-Lehner involution. Thus all the supersingular components of $X_0(Np^3)$ are as claimed, and the theorem is proved. One final remark is that when P ramifies over $j = 0$ or $j = 1728$ and is supersingular, we do technically get singularities in $X_0(N) \times X_0(p^3)$ which lie over the (smooth) reduction of $j = 0$ or 1728. These singularities can be ignored, however, by Remark 8.5.

8.4 Examples

It is now fairly straightforward to generate complete graphs with genera for the stable reduction of $X_0(Np^3)$. First we determine the supersingular values mod p, and the ramification of $\pi_f : X_0(N) \to X(1)$ over $j = 0$ and $j = 1728$. The latter can be derived from [S, Prop 1.43], which gives both the degree and number of elliptic points of each type. The components in the supersingular region then follow directly from Theorem 8.1. The only things which remain to be computed are the genera of $X_0(N)$ and $Ig(p) \times X_0(N)$.

The genus of $X_0(N)$ can be computed with [S, Prop 1.40]. Then Riemann-Hurwitz can be applied to the forgetful map from $X_0(N) \times Ig(p)$ to $X_0(N)$. By way of illustration, we now describe the stable reductions of $X_0(Np^3)$ in two examples: $X_0(3 \cdot 11^3)$ and $X_0(7 \cdot 13^3)$.

Example 1: $X_0(3 \cdot 11^3)$

Only $j = 0$ and $j = 1728$ are supersingular mod 11. In the degree 4 extension from $X_0(3) \to X(1)$, $j = 0$ splits into two points with $e = 1$ and $e = 3$, while $j = 1728$ splits into two points with $e = 2$. So we have a total of four supersingular necklaces. For the one corresponding to the unique elliptic point, there are 8 genus 5 components along the bridging component, and two outer components which meet the ordinary locus and have genus 1. The other three supersingular regions have 24 genus 5 components along the bridging component, and two outer components which also have genus 5. Now we compute the genera of the ordinary components. $X_0(3)$ has genus 0, and by Riemann-Hurwitz the genus of $Ig(11) \times X_0(3)$ is then 4. Indeed, it lies over $X_0(3)$ with degree 5, and is totally ramified over 4 points and unramified elsewhere. This implies a total genus of:

$$2(0) + 4(4) + 1[2(1) + 8(5)] + 3[2(5) + 24(5)] + (4 - 1)(6 - 1) = 463,$$

which can easily be verified with [S, Prop 1.40].

Example 2: $X_0(7 \cdot 13^3)$

The unique supersingular j-invariant for $p = 13$ is $j = 5$. Since this is neither 0 nor 1728, we simply get 8 supersingular regions which are all isomorphic to the supersingular region of $X_0(13^3)$. In particular, each necklace has 28 genus 6 components along the bridging component and then 2 more genus 6 components which meet the ordinary locus. Now we compute the genera of $X_0(7)$ and $X_0(7) \times Ig(13)$. The first has genus 0, and for the second we again apply Riemann-Hurwitz. The degree is 6, and we have total ramification over the 8 supersingular points. There are also two elliptic points of $X_0(7)$ lying over $j = 0$, each of which must split into two points with $e = 3$ in $X_0(7) \times Ig(13)$. So the genus of $Ig(13) \times X_0(7)$ is 19. That means if we add up the total genus of $X_0(7 \cdot 13^3)$ we get

$$2(0) + 4(19) + 8[2(6) + 28(6)] + (8 - 1)(6 - 1) = 1551,$$

which again can be easily verified with [S, Prop 1.40].

9 Index of Important Notation

$K(E)$, canonical subgroup of E	§2.1
$H_n(E)$, canonical subgroup of E of order p^n	
$\mathbf{X}^{\pm}_{a\,b}$, ordinary affinoids	
$Ig(p^n)$, level p^n Igusa curve	
$h(E)$, valuation of Hasse invariant of E	
$W_A(p^n)$, wide open subspace of $X_0(p^n)$ where $\bar{E} \cong A$	
$i(A) := \lvert\mathrm{Aut}(A)\rvert/2$	
$\mathbf{TS}_A$, $\mathbf{SD}_A$, too-supersingular and self-dual circles inside $W_A(p)$	
w_n, Atkin-Lehner involution on $X_0(p^n)$	
(F, A, α), Woods Hole representation of an elliptic curve	
π_f, forgetful map	
$W(\mathbb{F}_{p^n})$, Witt vectors of $\mathbb{F}_{p^n}$	
B, quaternionic order over $\mathbb{Z}_p$ isomorphic to $\mathrm{End}(\hat{A})$	
B', special subset of B^*	
Φ, Gross-Hopkins period map	
w_ρ, generalized Atkin-Lehner involution of $\mathbf{SD}_A$ for $\rho \in B'$	
$\mathbf{Y}_A$, nontrivial affinoid in $W_A(p^2)$	§2.2
π_ν, moduli-theoretic map taking (E, C) to $(E/C[p], C/C[p])$	
$\mathbf{E}_{1,A}$, $\mathbf{E}_{2,A}$, two pullbacks of $\mathbf{Y}_A$ to $X_0(p^3)$	
$\pi_{1\,1} := \pi_f \circ \pi_\nu$	
$\mathbf{Z}_A$, affinoid in $W_A(p^3)$ corresponding to "bridging component"	
$\mathbf{C}_A$, τ_f, special circle of $W_A(p)$ and map to $\mathbf{SD}_A$	
$\tilde{w}_\rho$, generalized Atkin-Lehner involution of $\mathbf{Z}_A$ for $\rho \in B'$	
$\mathcal{R}$, maximal orders in the quadratic extensions of $\mathbb{Q}_p$	§3
α_*, embedding of $\mathrm{End}(F)$ into B when (F, α) has fake CM	§3.2
$\mathcal{X}_0(p^n)$, stable model of $X_0(p^n)$	§4.1
$\mathcal{P}$, pairing on $K_a(E)$ onto μ_{p^b} which distinguishes $\mathbf{X}^{\pm}_{a\,b}$	
M_n, field found by Krir over which $J_0(p^n)$ has stable reduction	§5
F_n, field over which our stable model for $X_0(p^n)$ is defined ($n \leq 3$)	
$W^{\pm}_{a\,b}$, wide open neighborhood of $\mathbf{X}^{\pm}_{a\,b}$	§5.2
$V_i(A)$, $U(A)$, wide open neighborhoods of $\mathbf{E}_{i,A}$ and $\mathbf{Z}(A)$	
$\mathcal{S}(A)$, singular residue classes of $\mathbf{Z}_A$	
$\hat{U}(A)$, basic wide open refinement of $U(A)$	
$I = I_{\mathbb{Q}_p}$, $w = w_X$, inertia group and inertia action on $X = \mathcal{X}_0(p^n)$	§6
m_n, minimal extension of $\mathbb{Q}_p^{nr}$ over which $X_0(p^n)$ has stable reduction	
C_x, component of $\mathcal{X}_0(p^3)$ corresponding to a w_ρ fixed point	§6.3
τ_x, $\mathcal{F}_x$, hyper-elliptic involution on C_x, and its p fixed points	
$\mathcal{D}_x$, $\widetilde{\mathcal{D}}_x$, residue classes of $\mathbf{SD}_A$ and $\mathbf{Z}_A$	
$\tilde{S}_{s,\zeta}$, order p automorphism of $\widetilde{\mathcal{D}}_x$	

References

[B] K. Buzzard, *Analytic continuation of overconvergent eigenforms*, J. Amer. Math. Soc. 16 (2003), no. 1, 29–55.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21. Springer-Verlag, Berlin, 1990.

[C1] R. Coleman, *On the Components of $X_0(p^n)$*, J. Number Theory 110 (2005), no. 1, 3–21.

[C2] R. Coleman, *Stable Maps of Curves*, Kazuya Kato's fiftieth birthday, Doc. Math. (extra volume), 217–225.

[CMc] R. Coleman, K. McMurdy, *Stable Reduction of $X_0(p^3)$*, preprint available at http://math.berkeley.edu/~coleman/X_0(p^3)/Stable_Xp3.pdf

[dS1] E. de Shalit, *Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture, (Boston, 1991), 135–148, Contemp. Math. 165 (1994)

[dS2] E. de Shalit, *Relative Lubin-Tate Groups*, Proceedings of the AMS 95 (1985), no. 1,1–4.

[DR] P. Deligne, M. Rapoport, *Schemas de modules de courbes elliptiques*, Lecture Notes in Math. 349 (1973), 143–316.

[DM] ___________, D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. 36 (1969), 75–109.

[E1] B. Edixhoven, *Minimal resolution and stable reduction of $X_0(N)$*, Ann. Inst. Fourier (Grenoble) 40 (1990), no. 1, 31–67.

[E2] ___________, *Stable models of modular curves and applicatons*, Thèse de doctorat à l'université d'Utrecht, juin 1989. Available at http://www.math.leidenuniv.nl/~edix/public_html_rennes/publications/prschr.html

[G] B. Gross, *On canonical and quasi-canonical liftings*, Invent. Math. 84 (1986), no. 2, 321–326.

[GH] ___________, M. Hopkins, *Equivariant vector bundles on the Lubin-Tate moduli space*, Topology and representation theory (Evanston, IL, 1992), 23–88, Contemp. Math., 158 (1994).

[Ig] J-i Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan 20 (1968), 96–106.

[Iw] K. Iwasawa, *Local class field theory*, Oxford Science Publications. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1986. viii+155 pp

[K] M. Krir, *Degré d'une extension de Q_p^{nr} sur laquelle $J_0(N)$ est semi-stable*, Ann. Inst. Fourier (Grenoble) 46 (1996), no. 2, 279–291.

[M1] K. McMurdy, *Explicit parameterizations of ordinary and supersingular regions of $X_0(p^n)$*, Modular curves and abelian varieties (Barcelona, 2002), 165–179, Prog. Math. 224 (2004).

[M2] ____________, *Stable Reduction of $X_0(81)$*, preprint available.

[R] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{Q}/Q)$ *arising from modular forms*, Invent. Math. 100 (1990), no. 2, 431–476.

[S] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princteon, N.J., 1971.

[T] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144.

[WH] J. Lubin, J.-P. Serre, J. Tate, *Elliptic curves and formal groups*, Lecture notes from the Summer Institute on Algebraic Geometry (Woods Hole, MA, 1964), available at
http://www.ma.utexas.edu/users/voloch/lst.html

Ken McMurdy
Department of Mathematics
Rose-Hulman Institute of Technology
USA
mcmurdy@rose-hulman.edu

Robert Coleman
Department of Mathematics
U. C. Berkeley
USA
coleman@math.berkeley.edu

Λ-Adic Euler Characteristics of Elliptic Curves

To John Coates on the occasion of his sixtieth birthday

Daniel Delbourgo

Received: July 11, 2005
Revised: February 17, 2006

Abstract. Let $E_{/\mathbb{Q}}$ be a modular elliptic curve, and $p > 3$ a good ordinary or semistable prime.

Under mild hypotheses, we prove an exact formula for the μ-invariant associated to the weight-deformation of the Tate module of E. For example, at ordinary primes in the range $3 < p < 100$, the result implies the triviality of the μ-invariant of $X_0(11)$.

2000 Mathematics Subject Classification: 11G40; also 11F33, 11R23, 11G05

0. Introduction

A central aim in arithmetic geometry is to relate global invariants of a variety, with the behaviour of its L-function. For elliptic curves defined over a number field, these are the numerical predictions made by Birch and Swinnerton-Dyer in the 1960's. A decade or so later, John Coates pioneered the techniques of Iwasawa's new theory, to tackle their conjecture prime by prime. Together with Andrew Wiles, he obtained the first concrete results for elliptic curves admitting complex multiplication.

Let p be a prime number, and F_∞ a p-adic Lie extension of a number field F. From the standpoint of Galois representations, one views the Iwasawa theory of an elliptic curve E defined over F, as being the study of the p^∞-Selmer group

$$\mathrm{Sel}_{F_\infty}(E) \quad \subset \quad H^1\Big(\mathrm{Gal}(\overline{F}/F),\ \mathbb{A}_{F_\infty}\Big)\ .$$

Here $\mathbb{A}_{F_\infty} = \mathrm{Hom}_{\mathrm{cont}}\Big(\mathrm{Ta}_p(E)[[\mathrm{Gal}(F_\infty/F)]],\ \mathbb{Q}/\mathbb{Z}\Big)$ denotes the Pontrjagin dual to the $\mathrm{Gal}(F_\infty/F)$-deformation of the Tate module. The field F_∞ is often taken to be the cyclotomic $\mathbb{Z}_p$-extension of F, or sometimes the anti-cyclotomic extension. Hopefully a more complete picture becomes available over $F_\infty = F\big(E[p^\infty]\big)$, the field obtained by adjoining all p-power division points on E. If E has no complex multiplication, then $\mathrm{Gal}\big(F_\infty/F\big)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ by a theorem of Serre, which means the underlying Iwasawa algebras are no longer commutative.

In this article we study a special kind of Selmer group, namely the one which is associated to a Hida deformation of $\mathrm{Ta}_p(E)$. This object is defined by imposing the local condition that every 1-cocycle lies within a compatible family of points, living on the pro-jacobian of $\hat{X} = \varprojlim_r X_1(Np^r)$. There is a natural action of the diamond operators on the universal nearly-ordinary representation, which extends to a continuous action of $\Lambda = \mathbb{Z}_p[[1+p\mathbb{Z}_p]]$ on our big Selmer group. By the structure theory of Λ-modules, we can define an analogue of the μ-invariant for a weight deformation, μ^{wt} say. One can also deform both the Tate-Shafarevich group and the Tamagawa factors $[E(F_\nu) : E_0(F_\nu)]$, as sheaves over weight-space. Conjecturally the deformation of Ш should be mirrored by the behaviour of the *improved* p-adic L-function in [GS, Prop 5.8], which interpolates the L-values of the Hida family at the point $s = 1$. The Λ-adic Tamagawa factors $\mathrm{Tam}_{\Lambda,l}$ are related to the arithmetic of $F_\infty = F\big(E[p^\infty]\big)$, as follows.

For simplicity suppose that E is defined over $F = \mathbb{Q}$, and is without complex multiplication. Let $p \geq 5$ be a prime where E has good ordinary reduction, and assume there are no rational cyclic p-isogenies between E and any other elliptic curve. Both Howson and Venjakob have proposed a definition for a μ-invariant associated to the full GL_2-extension. Presumably, this invariant should represent the power of p occurring in the leading term of a hypothetical p-adic L-function, interpolating critical L-values of E at twists by Artin representations factoring through $\mathrm{Gal}(F_\infty/\mathbb{Q})$.

Recall that for a discrete p-primary $\mathrm{Gal}(F_\infty/\mathbb{Q})$-module M, its $\mathrm{Gal}(F_\infty/\mathbb{Q})$-Euler characteristic is the product

$$\chi\Big(\mathrm{Gal}(F_\infty/\mathbb{Q}),\ M\Big) \ := \ \prod_{j=0}^{\infty} \Big(\# H^j\big(F_\infty/\mathbb{Q}, M\big)\Big)^{(-1)^j}.$$

Under the twin assumptions that $L(E,1) \neq 0$ and $\mathrm{Sel}_{F_\infty}(E)$ is cotorsion over the non-abelian Iwasawa algebra, Coates and Howson [CH, Th 1.1] proved that

$$\chi\Big(\mathrm{Gal}(F_\infty/\mathbb{Q}),\ \mathrm{Sel}_{F_\infty}(E)\Big) \ = \prod_{\text{bad primes } l} \big|L_l(E,1)\big|_p \ \times \ \Big(\#\widetilde{E}(\mathbb{F}_p)[p^\infty]\Big)^2$$
$$\times\ \Big(\text{the } p\text{-part of the BS,D formula}\Big).$$

Let μ^{GL_2} denote the power of p occurring above. It's straightforward to combine the main result of this paper (Theorem 1.4) with their Euler characteristic calculation, yielding the upper bound

$$\mu^{\mathrm{wt}} \quad \leq \quad \mu^{\mathrm{GL}_2} \ + \sum_{\text{bad primes } l} \left\{ \mathrm{ord}_p\big(L_l(E,1)\big) - \mathrm{ord}_p\big(\mathrm{Tam}_{\Lambda,l}\big) \right\} .$$

In other words, the arithmetic of the weight-deformation is controlled in the p-adic Lie extension. This is certainly consistent with the commonly held belief, that the Greenberg-Stevens p-adic L divides the projection (to the Iwasawa algebra of the maximal torus) of some 'non-abelian L-function' living in $\mathbb{Z}_p\Big[\Big[\mathrm{Gal}\big(\mathbb{Q}\big(E[p^\infty]\big)/\mathbb{Q}\big)\Big]\Big]$. The non-commutative aspects currently remain shrouded in mystery, however.

Finally, we point out that many elliptic curves E possess Λ-adic Tamagawa factors, which differ from the p-primary component of the standard factor $\mathrm{Tam}(E)$. P. Smith has estimated this phenomenon occurs infrequently – a list of such curves up to conductor $< 10,000$ has been tabulated in [Sm, App'x A].

Acknowledgement: We dedicate this paper to John Coates on his sixtieth birthday. The author thanks him heartily for much friendly advice, and greatly appreciates his constant support over the last decade.

1. Statement of the Results

Let E be an elliptic curve defined over the rationals. We lose nothing at all by supposing that E be a strong Weil curve of conductor N_E, and denote by $\pm\phi$ the non-constant morphism of curves $\phi : X_0(N_E) \twoheadrightarrow E$ minimal amongst all $X_0(N_E)$-parametrisations. In particular, there exists a normalised eigenform $f_E \in \mathcal{S}_2^{\mathrm{new}}\big(\Gamma_0(N_E)\big)$ satisfying $\phi^*\omega_E \ = c_E^{\mathrm{Man}} f_E(q)dq/q$, where ω_E denotes a Néron differential on E and c_E^{Man} is the Manin constant for ϕ.

Fix a prime number $p \geq 5$, and let's write $N = p^{-\mathrm{ord}_p N_E} N_E$ for the tame level. We shall assume E has either good ordinary or multiplicative reduction over $\mathbb{Q}_p$,

hence $\mathbf{f}_2 := \begin{cases} f_E(q) - \beta_p f_E(q^p) & \text{if } p \nmid N_E \\ f_E(q) & \text{if } p \| N_E \end{cases}$ will be the p-stabilisation of f_E at p.

Hypothesis($\mathcal{R}_E$). $\mathbf{f}_2$ *is the unique* p*-stabilised newform in* $\mathcal{S}_2^{\mathrm{ord}}\big(\Gamma_0(Np)\big)$.

Throughout $\Lambda = \mathbb{Z}_p[[\Gamma]]$ denotes the completed group algebra of $\Gamma = 1 + p\mathbb{Z}_p$, and $\mathcal{L} = \mathrm{Frac}(\Lambda)$ its field of fractions. There are non-canonical isomorphisms $\Lambda \cong \mathbb{Z}_p[[X]]$ given by sending a topological generator $u_0 \in \Gamma$ to the element $1 + X$. In fact the $\mathbb{Z}_p$-linear extension of the map $\sigma_k : u_0 \mapsto u_0^{k-2}$ transforms Λ into the Iwasawa functions $\mathcal{A}_{\mathbb{Z}_p} = \mathbb{Z}_p\langle\langle k \rangle\rangle$, convergent everywhere on the closed unit disk.

Under the above hypothesis, there exists a unique Λ-adic eigenform $\mathbf{f} \in \Lambda[[q]]$ lifting the cusp form $\mathbf{f}_2$ at weight two; furthermore

$$\mathbf{f}_k \ := \ \sum_{n=1}^{\infty} \sigma_k\big(a_n(\mathbf{f})\big) q^n \ \in \ \mathcal{S}_k^{\mathrm{ord}}\big(\Gamma_1(Np^r)\big)$$

is a p-stabilised eigenform of weight k and character ω^{2-k}, for all integers $k \geq 2$. Hida and Mazur-Wiles [H1,H2,MW] attached a continuous Galois representation

$$\rho_\infty : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\Lambda) \ = \ \mathrm{Aut}_\Lambda(\mathbb{T}_\infty)$$

interpolating Deligne's p-adic representations for every eigenform in the family. The rank two lattice $\mathbb{T}_\infty$ is always free over Λ, unramified outside of Np, and the characteristic polynomial of $\rho_\infty\big(\mathrm{Frob}_l\big)$ will be $1 - a_l(\mathbf{f})x + l\big\langle l \big\rangle x^2$ for primes $l \nmid Np$. If we restrict to a decomposition group above p,

$$\rho_\infty \otimes_\Lambda \mathcal{A}_{\mathbb{Z}_p}\Bigg|_{G_{\mathbb{Q}_p}} \sim \begin{pmatrix} \chi_{\mathrm{cy}} < \chi_{\mathrm{cy}} >^{k-2} \phi_k^{-1} & * \\ 0 & \phi_k \end{pmatrix} \quad \text{where } \phi_k : G_{\mathbb{Q}_p}/I_p \to \mathbb{Z}_p^\times$$

is the unramified character sending Frob_p to the eigenvalue of U_p at weight k.

Question. *Can one make a Tamagawa number conjecture for the Λ-adic form $\mathbf{f}$, which specialises at arithmetic primes to each Bloch-Kato conjecture?*

The answer turns out to be a cautious 'Yes', provided one is willing to work with p-primary components of the usual suspects. In this article, we shall explain the specialisation to weight two (i.e. elliptic curves) subject to a couple of simplifying assumptions. The general case will be treated in a forthcoming work, and includes the situation where the nearly-ordinary deformation ring $\mathcal{R}_E$ is a non-trivial finite, flat extension of Λ. Let's begin by associating local points to ρ_∞...

For each pair of integers $m, r \in \mathbb{N}$, the multiplication by p^m endomorphism on the p-divisible group $J_r = \mathrm{jac}\ X_1(Np^r)$ induces a tautological exact sequence $0 \to J_r[p^m] \to J_r \overset{\times p^m}{\to} J_r \to 0$. Upon taking Galois invariants, we obtain a long exact sequence in $G_{\mathbb{Q}_p}$-cohomology

$$\begin{aligned} 0 \to J_r(\mathbb{Q}_p)[p^m] \to J_r(\mathbb{Q}_p) &\overset{\times p^m}{\to} J_r(\mathbb{Q}_p) \\ &\overset{\partial_{r,m}}{\to} H^1(\mathbb{Q}_p, J_r[p^m]) \to H^1(\mathbb{Q}_p, J_r)[p^m] \to 0. \end{aligned}$$

The boundary map $\partial_{r,m}$ injects $J_r(\mathbb{Q}_p)/p^m$ into $H^1(\mathbb{Q}_p, J_r[p^m])$, so applying the functors $\varprojlim_m$ and $\varprojlim_r$ yields a level-compatible Kummer map

$$\varprojlim_{r,m} \partial_{r,m} : J_\infty(\mathbb{Q}_p)\widehat{\otimes}\mathbb{Z}_p \ \hookrightarrow \ H^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(J_\infty)\big) \quad \text{which is Hecke-equivariant;}$$

here J_∞ denotes the limit $\varprojlim_r \text{jac}\ X_1(Np^r)$ induced from $X_1(Np^{r+1}) \overset{\pi_p}{\twoheadrightarrow} X_1(Np^r)$.

For a compact Λ-module M, we define its twisted dual $A_M := \text{Hom}_{\text{cont}}\big(M, \mu_{p^\infty}\big)$. Recall that Hida [H1] cuts $\mathbb{T}_\infty$ out of the massive Galois representation $\text{Ta}_p(J_\infty)$ using idempotents $\mathbf{e}_{\text{ord}} = \lim_{n\to\infty} U_p^{n!}$ and $\mathbf{e}_{\text{prim}}$ living in the abstract Hecke algebra (the latter is the projector to the p-normalised primitive part, and in general exists only after extending scalars to $\mathcal{L}$).

Definition 1.1. *(a) We define $X(\mathbb{Q}_p)$ to be the pre-image of the local points*

$$\mathbf{e}_{\text{prim}}\cdot\left(\left(\mathbf{e}_{\text{ord}}\cdot\varprojlim_{r,m}\partial_{r,m}\Big(J_\infty(\mathbb{Q}_p)\widehat{\otimes}\mathbb{Z}_p\Big)\right)\otimes_\Lambda \mathcal{L}\right)$$

under the canonical homomorphism $H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \xrightarrow{-\otimes 1} H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \otimes_\Lambda \mathcal{L}$.

(b) We define the dual group $X^D(\mathbb{Q}_p)$ to be the orthogonal complement

$$\Big\{\mathbf{x} \in H^1\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big) \quad \textit{such that}\ \ inv_{\mathbb{Q}_p}\big(X(\mathbb{Q}_p) \cup \mathbf{x}\big) \ = \ 0\Big\}$$

under Pontrjagin duality $H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \times H^1\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big) \to H^2\big(\mathbb{Q}_p, \mu_{p^\infty}\big) \cong \mathbb{Q}_p/\mathbb{Z}_p$.

The local condition $X(\mathbb{Q}_p)$ will be Λ-saturated inside its ambient cohomology group. These groups were studied by the author and Smith in [DS], and are intimately connected to the behaviour of big dual exponential maps for the family.

Let Σ denote a finite set containing p and primes dividing the conductor N_E. Write $\mathbb{Q}_\Sigma$ for the maximal algebraic extension of the rationals, unramified outside the set of bad places $\Sigma \cup \{\infty\}$. Our primary object of study is the big Selmer group

$$\text{Sel}_{\mathbb{Q}}(\rho_\infty) := \text{Ker}\left(H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q}, A_{\mathbb{T}_\infty}\big) \xrightarrow{\oplus\text{res}_l} \bigoplus_{l\neq p} H^1\big(\mathbb{Q}_l, A_{\mathbb{T}_\infty}\big) \oplus \frac{H^1\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big)}{X^D(\mathbb{Q}_p)}\right)$$

which is a discrete module over the local ring Λ.

For each arithmetic point in $\text{Spec}(\Lambda)^{\text{alg}}$, the Λ-adic object $\text{Sel}_{\mathbb{Q}}(\rho_\infty)$ interpolates the Bloch-Kato Selmer groups associated to the p-stabilisations $\mathbf{f}_k$ of weight $k \geq 2$. At $k = 2$ it should encode the Birch and Swinnerton-Dyer formulae, up to some easily computable fudge-factors.

Proposition 1.2. *(a) The Pontrjagin dual*

$$\widehat{Sel_{\mathbb{Q}}(\rho_\infty)} = Hom_{\mathrm{cont}}\big(Sel_{\mathbb{Q}}(\rho_\infty),\ \mathbb{Q}/\mathbb{Z}\big)$$

is a finitely-generated Λ-module;

(b) If $L(E,1) \neq 0$ then $\widehat{Sel_{\mathbb{Q}}(\rho_\infty)}$ is Λ-torsion, i.e. $Sel_{\mathbb{Q}}(\rho_\infty)$ is Λ-cotorsion.

In general, one can associate a characteristic element to $\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)$ via

$$Ш_{\mathbb{Q}}(\rho_\infty) \quad := \quad \mathrm{char}_\Lambda\Big(\mathrm{Hom}_{\mathrm{cont}}\Big(\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)_{\big/\Lambda\text{-div}}\ ,\ \mathbb{Q}/\mathbb{Z}\Big)\Big)$$

where ${}_{\big/\Lambda\text{-div}}$ indicates we have quotiented by the maximal $\mathfrak{m}_\Lambda$-divisible submodule; equivalently $Ш_{\mathbb{Q}}(\rho_\infty)$ is a generator of the characteristic ideal of $\mathrm{Tors}_\Lambda\Big(\widehat{\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)}\Big)$. If the L-function doesn't vanish at $s=1$ then by 1.2(b), the Pontrjagin dual $\widehat{\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)}$ is already pseudo-isomorphic to a compact Λ-module of the form

$$\bigoplus_{i=1}^{t} \mathbb{Z}/p^{\mu_i}\mathbb{Z} \ \oplus\ \bigoplus_{j=1}^{s} \Lambda/F_j^{e_j}\Lambda$$

where the F_j's are irreducible distinguished polynomials, and all of the $\mu_i, e_j \geq 0$. In this particular case $Ш_{\mathbb{Q}}(\rho_\infty)$ will equal $p^{\mu_1+\cdots\mu_t} \times \prod_{j=1}^{s} F_j^{e_j}$ modulo $\Lambda^\times$, and so annihilates the whole of $\widehat{\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)}$.

Definition/Lemma 1.3. *For each prime $l \neq p$ and integer weight $k \geq 2$, we set*

$$Tam_l(\rho_\infty; k) \quad := \quad \#Tors_\Lambda\Big(H^1\big(I_l, \mathbb{T}_\infty\big)\Big)^{\mathrm{Frob}_l=1} \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p \quad \in \quad p^{\mathbb{N}\cup\{0\}}\ .$$

Then at weight two,

$$\prod_{l\neq p} Tam_l(\rho_\infty; 2) \quad \textit{divides the p-part of} \quad \prod_{l\neq p}\big[\mathcal{C}^{\min}(\mathbb{Q}_l) : \mathcal{C}_0^{\min}(\mathbb{Q}_l)\big]$$

where $\mathcal{C}^{\min}_{\big/\mathbb{Q}}$ refers to the $\mathbb{Q}$-isogenous elliptic curve of Stevens, for which every optimal parametrisation $X_1(Np) \twoheadrightarrow E$ admits a factorisation $X_1(Np) \to \mathcal{C}^{\min} \to E$.

These mysterious Λ-adic Tamagawa numbers control the specialisation of our big Tate-Shafarevich group Ш at arithmetic points. In particular, for the weight $k=2$ they occur in the leading term of $Ш_{\mathbb{Q}}(\rho_\infty)$ viewed as an element of $\Lambda \cong \mathbb{Z}_p[[X]]$. It was conjectured in [St] that $\mathcal{C}^{\min}$ is the same elliptic curve for which the Manin constant associated to $X_1(Np) \twoheadrightarrow \mathcal{C}^{\min}$ is ± 1. Cremona pointed out the Tamagawa factors $[\mathcal{C}^{\min}(\mathbb{Q}_l) : \mathcal{C}_0^{\min}(\mathbb{Q}_l)]$ tend to be smaller than the $[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]$'s.

To state the simplest version of our result, we shall assume the following:

Hypothesis(Frb). *Either (i)* $p \nmid N_E$ *and* $a_p(E) \neq +1$,
or (ii) $p \| N_E$ *and* $a_p(E) = -1$
or (iii) $p \| N_E$ *and* $a_p(E) = +1,\ p \nmid \mathrm{ord}_p\Big(\mathbf{q}_{\mathrm{Tate}}(\mathcal{C}^{\min})\Big)$.

Note that in case (iii), the condition that p does not divide the valuation of the Tate period $\mathbf{q}_{\mathrm{Tate}}(\mathcal{C}^{\min})$ ensures the p-part of $[\mathcal{C}^{\min}(\mathbb{Q}_p) : \mathcal{C}_0^{\min}(\mathbb{Q}_p)]$ is trivial.

Theorem 1.4. *Assume both* $(\mathcal{R}_E)$ *and (Frb) hold. If* $L(E,1) \neq 0$, *then*

$$\sigma_2\Big(Ш_{\mathbb{Q}}(\rho_\infty)\Big) \equiv \mathcal{L}_p^{\mathrm{wt}}(E) \times [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)] \prod_{l \neq p} \frac{[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]}{\mathrm{Tam}_l(\rho_\infty; 2)} \times \frac{\#Ш_{\mathbb{Q}}(E)}{\#E(\mathbb{Q})^2}$$

modulo $\mathbb{Z}_p^\times$, *where the* $\mathcal{L}^{\mathrm{wt}}$*-invariant at weight two is defined to be*

$$\mathcal{L}_p^{\mathrm{wt}}(E) := \frac{\int_{E(\mathbb{R})} \omega_E}{\int_{\mathcal{C}^{\min}(\mathbb{R})} \omega_{\mathcal{C}^{\min}}} \times \frac{\#\mathcal{C}^{\min}(\mathbb{Q})}{\#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma} .$$

In particular, the Γ*-coinvariants of* $A_{\mathbb{T}_\infty}(\mathbb{Q}) = H^0\big(\mathbb{Q}_\Sigma/\mathbb{Q}, A_{\mathbb{T}_\infty}\big)$ *are always finite, and the denominator* $\#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma$ *divides into* $\#\mathcal{C}^{\min}(\mathbb{Q})[p^\infty]$.

This equation is a special case of a more general Tamagawa number formalism. Whilst none of the assumptions $(\mathcal{R}_E)$, (Frb) and $L(E,1) \neq 0$ are actually necessary, the full result requires a weight-regulator term, the relative covolume of $X(\mathbb{Q}_p)$ and various other additional factors – we won't consider these complications here.

Example 1.5. Consider the modular curve $E = X_0(11)$ given by the equation

$$E : y^2 + y = x^3 - x^2 - 10x - 20 .$$

The Tamagawa number of E at the bad prime 11 equals 5, whereas elsewhere the curve has good reduction. Let's break up the calculation into three parts: (a) Avoiding the supersingular prime numbers 19 and 29, one checks for every good ordinary prime $7 \leq p \leq 97$ that both of the hypotheses $(\mathcal{R}_E)$ and (Frb) hold true (to check the former, we verified that there are no congruences modulo p between f_E and any newform at level $11p$). Now by Theorem 1.4,

$$\sigma_2\Big(Ш_{\mathbb{Q}}(\rho_\infty)\Big) \equiv \frac{\mathcal{L}_p^{\mathrm{wt}}(E) \times 5 \times \#Ш_{\mathbb{Q}}(E)}{\mathrm{Tam}_{11}(\rho_\infty; 2) \times 5^2} \equiv 1 \quad \text{modulo } \mathbb{Z}_p^\times$$

since the $\mathcal{L}_p^{\mathrm{wt}}$-invariant is a p-adic unit, and the size of $Ш_{\mathbb{Q}}(E)$ is equal to one.

(b) At the prime $p = 11$ the elliptic curve E has split multiplicative reduction. The optimal curve $\mathcal{C}^{\min}$ is $X_1(11)$ whose Tamagawa number is trivial, hence so is $\mathrm{Tam}_{11}(\rho_\infty;2)$. Our theorem implies $\sigma_2\Big(\text{Ш}_{\mathbb{Q}}(\rho_\infty)\Big)$ must then be an 11-adic unit.

(c) When $p = 5$ the curve E fails to satisfy (Frb) as the Hecke eigenvalue $a_5(E) = 1$. Nevertheless the deformation ring $\mathcal{R}_E \cong \Lambda$, and E has good ordinary reduction. Applying similar arguments to the proof of 1.4, one can show that

$$\Big|\sigma_2\Big(\text{Ш}_{\mathbb{Q}}(\rho_\infty)\Big)\Big|_5^{-1} \quad \text{divides} \quad \frac{\#\widetilde{X_1(11)}(\mathbb{F}_5)[5^\infty] \ \times \ \#\text{Ш}_{\mathbb{Q}}\big(X_1(11)\big)[5^\infty]}{\#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma \ \times \ \#X_1(11)(\mathbb{Q})[5^\infty]}\ .$$

The right-hand side equals one, since $X_1(11)(\mathbb{Q})$ and the reduced curve $\widetilde{X_1(11)}(\mathbb{F}_5)$ possess a non-trivial 5-torsion point. As the left-hand side is 5-integral, clearly $\#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma = 1$ and it follows that $\sigma_2\Big(\text{Ш}_{\mathbb{Q}}(\rho_\infty)\Big)$ is a 5-adic unit.

Corollary 1.6. *For all prime numbers p such that $5 \leq p \leq 97$ and $a_p\big(X_0(11)\big) \neq 0$,*
the μ^{wt}-invariant associated to the Hida deformation of $\mathrm{Sel}_{\mathbb{Q}}\big(X_0(11)\big)[p^\infty]$ is zero.

In fact the μ^{wt}-invariant is probably zero at all primes p for which $X_0(11)$ has good ordinary reduction, but we need a more general formula than 1.4 to prove this.

2. Outline of the Proof of Theorem 1.4

We begin with some general comments.

The rank two module $\mathbb{T}_\infty \otimes_{\Lambda,\sigma_2} \mathbb{Z}_p$ is isomorphic to the dual of $H^1_{\text{ét}}\big(\overline{E},\mathbb{Z}_p\big)$, in general only after tensoring by $\mathbb{Q}_p$. Consider instead the arithmetic pro-variety $\hat{X} = \varprojlim_{r\geq 1} X_1(Np^r)$ endowed with its canonical $\mathbb{Q}$-structure. The specialisation $(\sigma_2)_* : \mathbb{T}_\infty \twoheadrightarrow \big(\mathbb{T}_\infty\big)_\Gamma \hookrightarrow \mathrm{Ta}_p\Big(\mathrm{jac}\ X_1(Np)\Big)$ is clearly induced from $\hat{X} \overset{\mathrm{proj}}{\longrightarrow} X_1(Np)$. It follows from [St, Th 1.9] that $\mathbb{T}_\infty \otimes_{\Lambda,\sigma_2} \mathbb{Z}_p \cong \mathrm{Ta}_p(\mathcal{C}^{\min})$ on an integral level, where $\mathcal{C}^{\min}$ denotes the same elliptic curve occurring as a subvariety of jac $X_1(Np)$, alluded to earlier in 1.3.

Taking twisted duals of $0 \to \mathbb{T}_\infty \overset{u_0-1}{\to} \mathbb{T}_\infty \to \mathrm{Ta}_p(\mathcal{C}^{\min}) \to 0$, we obtain a corresponding short exact sequence

$$0 \ \to\ \mathrm{Hom}_{\mathrm{cont}}\Big(\mathrm{Ta}_p(\mathcal{C}^{\min}), \mu_{p^\infty}\Big) \ \to\ A_{\mathbb{T}_\infty} \ \overset{u_0-1}{\to}\ A_{\mathbb{T}_\infty} \ \to\ 0$$

of discrete Λ-modules. The Weil pairing on the optimal curve $\mathcal{C}^{\min}$ implies that $\mathrm{Hom}_{\mathrm{cont}}\Big(\mathrm{Ta}_p(\mathcal{C}^{\min}), \mu_{p^\infty}\Big) \cong \mathcal{C}^{\min}[p^\infty]$. We thus deduce that $\mathrm{Ta}_p(\mathcal{C}^{\min}) \not\cong \mathrm{Ta}_p(E)$ if and only if there exists a cyclic p^n-isogeny defined over $\mathbb{Q}$, between the two elliptic curves E and $\mathcal{C}^{\min}$ (note this can only happen when the prime p is very small).

Let G denote either $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$, or a decomposition group $\mathrm{Gal}(\overline{\mathbb{Q}_l}/\mathbb{Q}_l)$ at some prime number l. For indices $j = 0, 1, 2$ there are induced exact sequences

$$0 \to H^j\big(G, A_{\mathbb{T}_\infty}\big) \otimes_{\Lambda,\sigma_2} \mathbb{Z}_p \to H^{j+1}\big(G, \mathcal{C}^{\min}[p^\infty]\big) \to H^{j+1}\big(G, A_{\mathbb{T}_\infty}\big)^\Gamma \to 0$$

and in continuous cohomology,

$$0 \to H^j\big(G, \mathbb{T}_\infty\big) \otimes_{\Lambda,\sigma_2} \mathbb{Z}_p \to H^j\big(G, \mathrm{Ta}_p(\mathcal{C}^{\min})\big) \to H^{j+1}\big(G, \mathbb{T}_\infty\big)^\Gamma \to 0\ .$$

From now on, we'll just drop the ' $_{\sigma_2}$' from the tensor product notation altogether.

Remark: Our strategy is to compare $\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)$ with the p-primary Selmer group for $\mathcal{C}^{\min}$ over the rationals. We can then use the Isogeny Theorem to exchange the optimal curve $\mathcal{C}^{\min}$ with the strong Weil curve E.

For each prime $l \neq p$, we claim there is a natural map

$$\delta_l \ :\ \frac{H^1\big(\mathbb{Q}_l, \mathcal{C}^{\min}[p^\infty]\big)}{H^1_{\mathrm{nr}}\big(\mathbb{Q}_l, \mathcal{C}^{\min}[p^\infty]\big)} \ \longrightarrow\ H^1\big(\mathbb{Q}_l, A_{\mathbb{T}_\infty}\big)^\Gamma\ ;$$

here $H^1_{\mathrm{nr}}\big(\mathbb{Q}_l, \mathcal{C}^{\min}[p^\infty]\big)$ denotes the orthogonal complement to the p-saturation of $H^1\left(\mathrm{Frob}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}\right)$ inside $H^1\big(\mathbb{Q}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)$. To see why this map exists, note that $H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big)$ is Λ-torsion, hence $H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big) \otimes_\Lambda \mathbb{Z}_p$ is p^∞-torsion and must lie in any p-saturated subgroup of $H^1\big(\mathbb{Q}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)$. Consequently the Γ-coinvariants

$$H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big)_\Gamma \ \hookrightarrow\ \text{the } p\text{-saturation of } H^1\left(\mathrm{Frob}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}\right)\ ,$$

and then dualising we obtain δ_l.

Let's now consider what happens when $l = p$. In [DS, Th 2.1] we identified the family of local points $X(\mathbb{Q}_p)$ with the cohomology subgroup

$$H^1_{\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \ :=\ \mathrm{Ker}\left(H^1_{\mathrm{cont}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \overset{(-\otimes 1)\otimes 1}{\longrightarrow} H^1_{\mathrm{cont}}\Big(\mathbb{Q}_p, \mathbb{T}_\infty \otimes \mathbb{B}_{\mathrm{dR}}\Big) \otimes_\Lambda \mathcal{L}\right)$$

where $\mathbb{B}_{\mathrm{dR}}$ denotes Iovita and Stevens' period ring. In particular, we showed that

$$X(\mathbb{Q}_p)_\Gamma \ =\ H^1_{\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \otimes_\Lambda \mathbb{Z}_p \ \hookrightarrow\ H^1_g\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big) \ \cong\ \mathcal{C}^{\min}(\mathbb{Q}_p)\widehat{\otimes}\mathbb{Z}_p$$

the latter isomorphism arising from [BK, Section 3]. Dualising the above yields

$$\delta_p \ :\ \frac{H^1\big(\mathbb{Q}_p, \mathcal{C}^{\min}[p^\infty]\big)}{\mathcal{C}^{\min}(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \ \longrightarrow\ \left(\frac{H^1\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big)}{X^D(\mathbb{Q}_p)}\right)^\Gamma$$

because $H^1_g\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)^\perp \cong \mathcal{C}^{\min}(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $X(\mathbb{Q}_p)^\perp = X^D(\mathbb{Q}_p)$.

Lemma 2.1. *For all prime numbers $l \in \Sigma$, the kernel of δ_l is a finite p-group.*

We defer the proof until the next section, but for $l \neq p$ it's straightforward. This discussion may be neatly summarised in the following commutative diagram, with left-exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_{\mathbb{Q}}(\mathcal{C}^{\min})[p^\infty] \arrow[r] \arrow[d, "\alpha"'] & H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\Big) \arrow[r, "\lambda_0"] \arrow[d, "\beta"'] & \bigoplus_{l\in\Sigma} \dfrac{H^1\big(\mathbb{Q}_l, \mathcal{C}^{\min}[p^\infty]\big)}{H^1_\star\big(\mathbb{Q}_l, \mathcal{C}^{\min}[p^\infty]\big)} \arrow[d, "\oplus\delta_l"'] \\
0 \arrow[r] & \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)^\Gamma \arrow[r] & H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\Big)^\Gamma \arrow[r, "\lambda_\infty"] & \bigoplus_{l\in\Sigma} \left(\dfrac{H^1\big(\mathbb{Q}_l, A_{\mathbb{T}_\infty}\big)}{H^1_\star\big(\mathbb{Q}_l, A_{\mathbb{T}_\infty}\big)}\right)^\Gamma .
\end{tikzcd}$$

Figure 1.

At primes $l \neq p$ the notation $H^1_\star$ represents H^1_{nr}. When $l = p$ we have written $H^1_\star\big(\mathbb{Q}_l, \mathcal{C}^{\min}[p^\infty]\big)$ for the points $\mathcal{C}^{\min}(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and analogously $H^1_\star\big(\mathbb{Q}_l, A_{\mathbb{T}_\infty}\big)$ in place of our family of local points $X^D(\mathbb{Q}_p)$.

Applying the Snake Lemma to the above, we obtain a long exact sequence

$$0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \to \mathrm{Im}(\lambda_0) \cap \left(\bigoplus_{l\in\Sigma} \mathrm{Ker}(\delta_l)\right) \to \mathrm{Coker}(\alpha) \to 0$$

as the map β is surjective. The kernel of β equals $H^0\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\big) \otimes_\Lambda \mathbb{Z}_p$ i.e., the Γ-coinvariants $H^1\Big(\Gamma,\ H^0\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\big)\Big)$. As Γ is pro-cyclic and $A_{\mathbb{T}_\infty}$ is discrete,

$$\begin{aligned}
\#H^1\Big(\Gamma,\ H^0\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\big)\Big) &\leq \#H^0\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ H^0(\Gamma, A_{\mathbb{T}_\infty})\Big) \\
&= \#H^0\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathrm{Hom}_{\mathrm{cont}}\big(\mathbb{T}_\infty \otimes_\Lambda \mathbb{Z}_p\ ,\ \mu_{p^\infty}\big)\Big) \\
&= \#H^0\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\Big) \ = \#\mathcal{C}^{\min}(\mathbb{Q})[p^\infty] .
\end{aligned}$$

In other words, the size of $\mathrm{Ker}(\beta)$ is bounded by $\#\mathcal{C}^{\min}(\mathbb{Q})[p^\infty]$. By a well-known theorem of Mazur on torsion points, the latter quantity is at most 16.

Remarks: (i) Let's recall that for any elliptic curve A over the rational numbers, its Tate-Shafarevich group can be defined by the exactness of

$$0 \to A(\mathbb{Q}) \otimes \mathbb{Q}/\mathbb{Z} \to H^1(\mathbb{Q}, A) \to Ш_{\mathbb{Q}}(A) \to 0 .$$

(ii) Lemma 2.1 implies every term occurring in our Snake Lemma sequence is finite, and as a direct consequence $\mathrm{Sel}_{\mathbb{Q}}(\mathcal{C}^{\min})[p^\infty] \xrightarrow{\alpha} \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)^\Gamma$ is a quasi-isomorphism. The coinvariants $\Big(\widehat{\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)}\Big)_\Gamma$ must then be of finite type over

$\mathbb{Z}_p$, Nakayama's lemma forces $\widehat{\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)}$ to be of finite type over Λ, and Proposition 1.2(a) follows.

(iii) Assume further that $L(E,1) \neq 0$. By work of Kolyvagin and later Kato [Ka], both $E(\mathbb{Q})$ and $Ш_{\mathbb{Q}}(E)$ are finite. Since $\mathcal{C}^{\min}$ is $\mathbb{Q}$-isogenous to E, clearly the Mordell-Weil and Tate-Shafarevich groups of the optimal curve must also be finite. Equivalently $\#\mathrm{Sel}_{\mathbb{Q}}(\mathcal{C}^{\min}) < \infty$, whence

$$\begin{aligned}&\mathrm{rank}_\Lambda\Big(\widehat{\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)}\Big) \;\leq \\ &\qquad\leq\; \mathrm{corank}_{\mathbb{Z}_p}\Big(\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)^\Gamma\Big) \;=\; \mathrm{corank}_{\mathbb{Z}_p}\Big(\mathrm{Sel}_{\mathbb{Q}}(\mathcal{C}^{\min})[p^\infty]\Big) \;=\; 0.\end{aligned}$$

It follows that $\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)$ is Λ-cotorsion, and Proposition 1.2(b) is established. The special value of $Ш_{\mathbb{Q}}(\rho_\infty)$ at σ_2 is determined (modulo p-adic units) by the Γ-Euler characteristic of $\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)$, namely

$$\chi\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big) \;:=\; \prod_{j=0}^{\infty}\Big(\#H^j\big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\big)\Big)^{(-1)^j} \;=\; \frac{\#H^0\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big)}{\#H^1\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big)}$$

as Γ has cohomological dimension one.
After a brisk diagram chase around Figure 1, we discover that

$$\chi\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big) \;=\; \frac{\#\mathrm{Sel}_{\mathbb{Q}}(\mathcal{C}^{\min})[p^\infty] \;\times\; \#\Big(\mathrm{Im}(\lambda_0) \cap \big(\bigoplus_{l\in\Sigma}\mathrm{Ker}(\delta_l)\big)\Big)}{\#\mathrm{Ker}(\beta) \;\times\; \#H^1\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big)}$$

$$=\; \frac{\#Ш_{\mathbb{Q}}(\mathcal{C}^{\min})[p^\infty] \quad\times\quad \prod_{l\in\Sigma}\#\mathrm{Ker}(\delta_l)}{\#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma \;\times\; \#H^1\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big) \;\times\; \prod_{l\in\Sigma}\Big[\mathrm{Ker}(\delta_l) : \mathrm{Im}(\lambda_0)\cap\mathrm{Ker}(\delta_l)\Big]}.$$

Proposition 2.2.
(a) $\#Ker(\delta_l) \;=\; \Big|\big[\mathcal{C}^{\min}(\mathbb{Q}_l) : \mathcal{C}_0^{\min}(\mathbb{Q}_l)\big]\Big|_p^{-1} \times \Big|Tam_l(\rho_\infty;2)\Big|_p$ *if* $l \neq p$;

(b) $\#Ker(\delta_p) = 1$ *and* $\Big|\big[\mathcal{C}^{\min}(\mathbb{Q}_p) : \mathcal{C}_0^{\min}(\mathbb{Q}_p)\big]\Big|_p = 1$ *if Hypothesis(Frb) holds for* E.

Proposition 2.3. *If* $L(E,1) \neq 0$, *then*

$$\#H^1\Big(\Gamma, Sel_{\mathbb{Q}}(\rho_\infty)\Big) \;\times\; \prod_{l\in\Sigma}\Big[Ker(\delta_l) : Im(\lambda_0)\cap Ker(\delta_l)\Big] \quad=\quad \#\mathcal{C}^{\min}(\mathbb{Q})[p^\infty]\,.$$

The former result is proved in the next section, and the latter assertion in §4. Substituting them back into our computation of the Γ-Euler characteristic,

$$\chi\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big) \;\approx\; \frac{\#Ш_{\mathbb{Q}}(\mathcal{C}^{\min}) \;\times\; \prod_{l\in\Sigma}\big[\mathcal{C}^{\min}(\mathbb{Q}_l) : \mathcal{C}_0^{\min}(\mathbb{Q}_l)\big]}{\#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma \;\times\; \#\mathcal{C}^{\min}(\mathbb{Q}) \;\times\; \prod_{l\in\Sigma-\{p\}}\mathrm{Tam}_l(\rho_\infty;2)}$$

where the notation $x \approx y$ is employed whenever $x = uy$ for some unit $u \in \mathbb{Z}_p^\times$. Setting $\mathcal{L}_p^{\mathrm{wt},\dagger}(E) \;:=\; \#\mathcal{C}^{\min}(\mathbb{Q}) \Big/ \#A_{\mathbb{T}_\infty}(\mathbb{Q})_\Gamma$, the above can be rewritten as

$$\frac{\mathcal{L}_p^{\mathrm{wt},\dagger}(E)}{\prod_{l\in\Sigma-\{p\}} \mathrm{Tam}_l(\rho_\infty;2)} \;\times\; \frac{\#\text{Ш}_{\mathbb{Q}}(\mathcal{C}^{\min}) \;\times\; \prod_{l\in\Sigma}\left[\mathcal{C}^{\min}(\mathbb{Q}_l) : \mathcal{C}_0^{\min}(\mathbb{Q}_l)\right]}{\#\mathcal{C}^{\min}(\mathbb{Q})^2} \; .$$

Cassels' Isogeny Theorem allows us to switch $\mathcal{C}^{\min}$ with the isogenous curve E, although this scales the formula by the ratio of periods $\int_{E(\mathbb{R})}\omega_E \Big/ \int_{\mathcal{C}^{\min}(\mathbb{R})}\omega_{\mathcal{C}^{\min}}$. Observing that $\sigma_2\Big(\text{Ш}_{\mathbb{Q}}(\rho_\infty)\Big) \;\approx\; \chi\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big)$, Theorem 1.4 is finally proved.

3. Computing the Local Kernels

We now examine the kernels of the homorphisms δ_l for all prime numbers $l \in \Sigma$. Let's start by considering $l \neq p$. By its very definition, δ_l is the dual of

$$\widehat{\delta_l} \;:\; H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big) \otimes_\Lambda \mathbb{Z}_p \;\hookrightarrow\; H^1_{\mathrm{nr}}\big(\mathbb{Q}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)$$

where $H^1_{\mathrm{nr}}(\cdots)$ denotes the p-saturation of $H^1\left(\mathrm{Frob}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}\right) \cong \frac{\mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}}{(\mathrm{Frob}_l - 1)}$.
The key term we need to calculate is

$$\#\mathrm{Ker}(\delta_l) \;=\; \#\mathrm{Coker}\big(\widehat{\delta_l}\big) \;=\; \Big[H^1_{\mathrm{nr}}\big(\mathbb{Q}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})\big) : H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big) \otimes_\Lambda \mathbb{Z}_p\Big] \, .$$

Firstly, the sequence $0 \to \mathbb{T}_\infty^{I_l} \otimes_\Lambda \mathbb{Z}_p \to \mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l} \to H^1\big(I_l, \mathbb{T}_\infty\big)^\Gamma \to 0$ is exact, and $\mathbb{T}_\infty^{I_l} \otimes_\Lambda \mathbb{Z}_p$ coincides with $\big(\mathbb{T}_\infty \otimes_\Lambda \mathbb{Z}_p\big)^{I_l} = \mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}$ since the Galois action and diamond operators commute on $\mathbb{T}_\infty$. As a corollary $H^1\big(I_l, \mathbb{T}_\infty\big)^\Gamma$ must be zero.
The group $\mathrm{Gal}\big(\mathbb{Q}_l^{\mathrm{unr}}/\mathbb{Q}_l\big)$ is topologically generated by Frobenius, hence

$$\begin{aligned} H^1\Big(\mathrm{Frob}_l, \mathbb{T}_\infty^{I_l}\Big)_\Gamma &\cong \left(\frac{\mathbb{T}_\infty^{I_l}}{(\mathrm{Frob}_l - 1).\mathbb{T}_\infty^{I_l}}\right) \otimes_\Lambda \mathbb{Z}_p \\ &= \left(\frac{\big(\mathbb{T}_\infty \otimes_\Lambda \mathbb{Z}_p\big)^{I_l}}{(\mathrm{Frob}_l - 1).\big(\mathbb{T}_\infty \otimes_\Lambda \mathbb{Z}_p\big)^{I_l}}\right) \cong H^1\Big(\mathrm{Frob}_l, \mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}\Big). \end{aligned}$$

Since the local cohomology $H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big)$ is always Λ-torsion when the prime $l \neq p$, inflation-restriction provides us with a short exact sequence

$$0 \;\to\; H^1\Big(\mathrm{Frob}_l, \mathbb{T}_\infty^{I_l}\Big) \;\overset{\mathrm{infl}}{\to}\; H^1\big(\mathbb{Q}_l, \mathbb{T}_\infty\big) \;\overset{\mathrm{rest}}{\to}\; \mathrm{Tors}_\Lambda\Big(H^1\big(I_l, \mathbb{T}_\infty\big)^{\mathrm{Frob}_l}\Big) \;\to\; 0 \, .$$

The boundary map $\mathrm{Tors}_\Lambda\Big(H^1\big(I_l,\mathbb{T}_\infty\big)^{\mathrm{Frob}_l}\Big)^\Gamma \to H^1\Big(\mathrm{Frob}_l,\mathbb{T}_\infty^{I_l}\Big)_\Gamma$ trivialises because $H^1\big(I_l,\mathbb{T}_\infty\big)^\Gamma = 0$, so the Γ-coinvariants $H^1\Big(\mathrm{Frob}_l,\mathbb{T}_\infty^{I_l}\Big)_\Gamma$ inject into $H^1\big(\mathbb{Q}_l,\mathbb{T}_\infty\big)_\Gamma$ under inflation.

We deduce that there is a commutative diagram, with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] \\
H^1\Big(\mathrm{Frob}_l,\mathbb{T}_\infty^{I_l}\Big)_\Gamma \arrow[r, hook, "\mathrm{infl}"] \arrow[d, equal] & H^1\big(\mathbb{Q}_l,\mathbb{T}_\infty\big)_\Gamma \arrow[r, two heads, "\mathrm{rest}"] \arrow[d] & \mathrm{Tors}_\Lambda\Big(H^1\big(I_l,\mathbb{T}_\infty\big)^{\mathrm{Frob}_l}\Big)_\Gamma \arrow[d, "\theta"'] \\
H^1\Big(\mathrm{Frob}_l,\mathrm{Ta}_p(\mathcal{C}^{\min})^{I_l}\Big) \arrow[r, hook, "\mathrm{infl}"] & H^1_{\mathrm{nr}}\big(\mathbb{Q}_l,\mathrm{Ta}_p(\mathcal{C}^{\min})\big) \arrow[r, two heads, "\mathrm{rest}"] \arrow[d] & H^1\big(I_l,\mathrm{Ta}_p(\mathcal{C}^{\min})\big)^{\mathrm{Frob}_l}[p^\infty] \arrow[d] \\
 & H^2\big(\mathbb{Q}_l,\mathbb{T}_\infty\big)^\Gamma \arrow[r, phantom, "\cong"] \arrow[d] & \mathrm{Coker}(\theta) \arrow[d] \\
 & 0 & 0
\end{tikzcd}$$

Figure 2.

Remark: Using Figure 2 to compute indices, general nonsense informs us that

$$\begin{aligned}
\#\mathrm{Ker}(\delta_l) \quad &= \quad \Big[H^1_{\mathrm{nr}}\big(\mathbb{Q}_l,\mathrm{Ta}_p(\mathcal{C}^{\min})\big) : H^1\big(\mathbb{Q}_l,\mathbb{T}_\infty\big)_\Gamma\Big] \quad = \quad \#\mathrm{Coker}(\theta) \\
&= \quad \frac{\#H^1\Big(I_l,\mathrm{Ta}_p(\mathcal{C}^{\min})\Big)^{\mathrm{Frob}_l}[p^\infty]}{\#\mathrm{Tors}_\Lambda\Big(H^1\big(I_l,\mathbb{T}_\infty\big)^{\mathrm{Frob}_l}\Big)_\Gamma} \quad \approx \quad \frac{\Big[\mathcal{C}^{\min}(\mathbb{Q}_l) : \mathcal{C}_0^{\min}(\mathbb{Q}_l)\Big]}{\mathrm{Tam}_l(\rho_\infty;2)} \; .
\end{aligned}$$

In one fell swoop this proves Proposition 2.2(a), Lemma 1.3 and half of Lemma 2.1.

Let's concentrate instead on $l = p$. The kernel of δ_p is dual to the cokernel of

$$\widehat{\delta_p} \;:\; H^1_{\mathcal{G}}\big(\mathbb{Q}_p,\mathbb{T}_\infty\big)\otimes_\Lambda \mathbb{Z}_p \;\hookrightarrow\; H^1_g\big(\mathbb{Q}_p,\mathrm{Ta}_p(\mathcal{C}^{\min})\big)\;.$$

Clearly the $\mathbb{Z}_p$-rank of $H^1_{\mathcal{G}}\big(\mathbb{Q}_p,\mathbb{T}_\infty\big)\otimes_\Lambda \mathbb{Z}_p$ is bounded below by the Λ-rank of $H^1_{\mathcal{G}}\big(\mathbb{Q}_p,\mathbb{T}_\infty\big)$ which equals one, thanks to a specialisation argument in [DS, Th 3]. On the other hand

$$\mathrm{rank}_{\mathbb{Z}_p}\Big(H^1_g\big(\mathbb{Q}_p,\mathrm{Ta}_p(\mathcal{C}^{\min})\big)\Big) \;=\; \dim_{\mathbb{Q}_p}\Big(\mathcal{C}^{\min}(\mathbb{Q}_p)\,\widehat{\otimes}\,\mathbb{Q}_p\Big) \;=\; 1$$

because the formal group of $\mathcal{C}^{\min}_{/\mathbb{Z}_p}$ has semistable height one. We conclude that

$$\#\mathrm{Ker}(\delta_p) \;=\; \#\mathrm{Coker}\big(\widehat{\delta_p}\big) \;=\; \Big[H^1_g\big(\mathbb{Q}_p,\mathrm{Ta}_p(\mathcal{C}^{\min})\big) : H^1_{\mathcal{G}}\big(\mathbb{Q}_p,\mathbb{T}_\infty\big)_\Gamma\Big]$$

must be finite, which completes the demonstration of Lemma 2.1.

Remarks: (i) For any de Rham $G_{\mathbb{Q}_p}$-representation V, Bloch and Kato [BK] define a dual exponential map

$$\exp_V^* \ : \ H^1\big(\mathbb{Q}_p, V\big) \ \longrightarrow \ \mathrm{Fil}^0\mathbf{D}_{\mathrm{dR}}(V) \ := \ \Big(V \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}^+\Big)^{G_{\mathbb{Q}_p}}$$

whose kernel is $H_g^1\big(\mathbb{Q}_p, V\big)$. If V equals the p-adic representation $\mathrm{Ta}_p(\mathcal{C}^{\min}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, then the cotangent space $\mathrm{Fil}^0\mathbf{D}_{\mathrm{dR}}(V) \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} H_{\mathrm{dR}}^1\big(\mathcal{C}^{\min}/\mathbb{Q}\big)$ is a $\mathbb{Q}_p$-line, generated by a Néron differential $\omega_{\mathcal{C}^{\min}}$ on the optimal elliptic curve.

(ii) Applying $\exp_V^*$ above and then cupping with the dual basis $\omega_{\mathcal{C}^{\min}}^*$, we obtain a homomorphism

$$\exp_\omega^* \ : \ \frac{H^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)}{H_g^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)} \ \longrightarrow \ \Big(\mathrm{Ta}_p(\mathcal{C}^{\min}) \otimes_{\mathbb{Z}_p} B_{\mathrm{dR}}^+\Big)^{G_{\mathbb{Q}_p}} \ \overset{-\,\cup\,\omega_{\mathcal{C}^{\min}}^*}{\longrightarrow} \ \mathbb{Q}_p$$

which sends Kato's zeta element [Ka, Th 13.1] to a non-zero multiple of $\frac{L_{Np}(\mathcal{C}^{\min},1)}{\Omega_{\mathcal{C}^{\min}}^+}$. In particular $L_{Np}(\mathcal{C}^{\min},1) = L_{Np}(E,1) \neq 0$, so the image of the composition $\exp_\omega^*$ must be a lattice $p^{n_1}\mathbb{Z}_p \subset \mathbb{Q}_p$ say. Let's abbreviate the quotient H^1/H_g^1 by $H_{/g}^1$. Notice also that the $\mathbb{Z}_p$-rank of $H_{/g}^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)$ equals one and the module is p^∞-torsion free, hence $\exp_\omega^*$ is injective.

In [De, Th 3.3] we showed the existence of a big dual exponential map

$$\mathrm{EXP}_{\mathbb{T}_\infty}^* \ : \ H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \ \longrightarrow \ \Lambda[1/p]\,, \qquad \mathrm{Ker}\big(\mathrm{EXP}_{\mathbb{T}_\infty}^*\big) \ = \ H_{\mathcal{G}}^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)$$

interpolating the standard $\exp^*$'s at the arithmetic points (we skip over the details). At weight two, $\mathrm{EXP}_{\mathbb{T}_\infty}^*$ modulo $u_0 - 1$ coincides with $\exp_\omega^*$ up to a non-zero scalar. The weight-deformation of Kato's zeta-element lives in $\mathrm{loc}_p\Big(H^1\big(\mathbb{Q}, \mathbb{T}_\infty\big)\Big)$, and via

$$H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \ \overset{\mathrm{mod}\ u_0-1}{\longrightarrow} \ H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma \ \overset{\mathrm{proj}}{\twoheadrightarrow} \ \frac{H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma}{H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma \cap H_g^1} \ \overset{\exp_\omega^*}{\hookrightarrow} \ \mathbb{Q}_p$$

is sent to the L-value $\frac{L_{Np}(\mathcal{C}^{\min},1)}{\Omega_{\mathcal{C}^{\min}}^+} \times$ (a Λ-adic period). In this case, the image of $H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma$ under $\exp_\omega^*$ will be a lattice $p^{n_2}\mathbb{Z}_p \subset \mathbb{Q}_p$ for some $n_2 \geq n_1$.
Key Claim: There is a commutative diagram, with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H_{\mathcal{G}}^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma \arrow[r, "\varepsilon"] \arrow[d] & H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma \arrow[r, "\exp^*(-)\,\cup\,\omega_{\mathcal{C}^{\min}}^*"] \arrow[d, "\mathrm{nat}"'] & p^{n_2}\mathbb{Z}_p \arrow[r] \arrow[d, "\mathrm{id}"'] & 0 \\
0 \arrow[r] & H_g^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big) \arrow[r] & H^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big) \arrow[r, "\exp^*(-)\,\cup\,\omega_{\mathcal{C}^{\min}}^*"] & p^{n_1}\mathbb{Z}_p \arrow[r] & 0.
\end{tikzcd}$$

To verify this assertion, we need to prove the injectivity of the top-left map ε. Recall that $H^1_{\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) = X(\mathbb{Q}_p)$ is Λ-saturated inside the local H^1, thus the quotient $H^1_{/\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)$ is Λ-free. In particular, both $H^1_{\mathcal{G}}$ and H^1 share the same Λ-torsion submodules, so at weight two $H^1_{\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma$ and $H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma$ must have identical $\mathbb{Z}_p$-torsion. It follows from the invariants/coinvariants sequence

$$\begin{array}{lllllll} 0 & \rightarrow & H^1_{\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)^\Gamma & \rightarrow & H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)^\Gamma & \rightarrow & H^1_{/\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)^\Gamma \\ & \overset{\partial}{\rightarrow} & H^1_{\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma & \overset{\varepsilon}{\rightarrow} & H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma & \rightarrow & H^1_{/\mathcal{G}}\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma \;\; \rightarrow \;\; 0 \end{array}$$

that ε fails to be injective, if and only if the image of ∂ has $\mathbb{Z}_p$-rank at least one. However,

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\partial) \;\; &= \\ &= \;\; \mathrm{rank}_{\mathbb{Z}_p}\Big(H^1_{\mathcal{G}}\big(\cdots\big)_\Gamma\Big) - \mathrm{rank}_{\mathbb{Z}_p}\Big(H^1\big(\cdots\big)_\Gamma\Big) + \mathrm{rank}_{\mathbb{Z}_p}\Big(H^1_{/\mathcal{G}}\big(\cdots\big)_\Gamma\Big) \\ &\leq \;\; \mathrm{rank}_{\mathbb{Z}_p}\Big(H^1_{\mathcal{G}}\big(\cdots\big)_\Gamma\Big) - \mathrm{rank}_{\mathbb{Z}_p}\Big(H^1\big(\cdots\big)_\Gamma\Big) + \mathrm{rank}_{\mathbb{Z}_p}\big(p^{n_2}\mathbb{Z}_p\big) \end{aligned}$$

as the rank of $H^1_{/\mathcal{G}}\big(\cdots\big)_\Gamma$ is bounded by the rank of $H^1\big(\cdots\big)_\Gamma \Big/ \big(H^1\big(\cdots\big)_\Gamma \cap H^1_g\big)$. The right-hand side above is equal to zero, hence $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\partial)$ is forced to be zero. The non-triviality of the boundary map ∂ can therefore never happen, and the injectivity of ε follows as well.

Remark: Using our Key Claim to calculate $\Big[H^1_g\big(\cdots\big) : H^1_{\mathcal{G}}\big(\cdots\big)_\Gamma\Big]$, we find that

$$\begin{aligned} \#\mathrm{Ker}(\delta_p) \;\; &= \;\; p^{-(n_2-n_1)} \times \Big[H^1\big(\mathbb{Q}_p, \mathrm{Ta}_p(\mathcal{C}^{\min})\big) : H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)_\Gamma\Big] \\ &= \;\; p^{-(n_2-n_1)} \times \#H^2\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)^\Gamma \;\; = \;\; p^{-(n_2-n_1)} \times \#H^0\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big)_\Gamma \end{aligned}$$

where the very last equality arises from the non-degeneracy of the local pairing $H^2\big(\mathbb{Q}_p, \mathbb{T}_\infty\big) \times H^0\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$.

By an argument familiar from §2,

$$\begin{aligned} &\#H^0\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}\big)_\Gamma \\ &\qquad \leq \;\; \#H^0\big(\mathbb{Q}_p, A_{\mathbb{T}_\infty}^\Gamma\big) \;\; = \;\; \#H^0\Big(\mathbb{Q}_p, \mathrm{Hom}_{\mathrm{cont}}\big(\mathbb{T}_\infty \otimes_\Lambda \mathbb{Z}_p, \mu_{p^\infty}\big)\Big) \\ &\qquad = \;\; \#H^0\Big(\mathbb{Q}_p, \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Ta}_p(\mathcal{C}^{\min}), \mu_{p^\infty}\big)\Big) \;\; = \;\; \#\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty] \end{aligned}$$

again due to the pro-cyclicity of Γ. Because $n_2 - n_1 \geq 0$, we get an upper bound

$$\#\mathrm{Ker}(\delta_p) \;\; \leq \;\; p^{-(n_2-n_1)}\#\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty] \;\; \leq \;\; \#\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty]\;;$$

we proceed by showing that the right-hand side is trivial under Hypothesis(Frb).

Case (i): $p \nmid N_E$ and $a_p(E) \neq +1$.

Here E and the isogenous curve $\mathcal{C}^{\min}$ have good ordinary reduction at the prime p; in particular, the formal group of $\mathcal{C}^{\min}_{/\mathbb{Z}_p}$ possesses no points of order p since $p \neq 2$. It follows that $\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty]$ injects into the subgroup of $\mathbb{F}_p$-rational points on $\widetilde{\mathcal{C}^{\min}}$, the reduced elliptic curve. Moreover

$$\#\widetilde{\mathcal{C}^{\min}}(\mathbb{F}_p) \quad = \quad p+1-a_p(E) \quad \not\equiv \quad 0 \pmod{p} \qquad \text{as} \quad a_p(E) \not\equiv +1,$$

meaning $\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty] \cong \widetilde{\mathcal{C}^{\min}}(\mathbb{F}_p)[p^\infty]$ is the trivial group.

Case (ii): $p \| N_E$ and $a_p(E) = -1$.

Both E and $\mathcal{C}^{\min}$ have non-split multiplicative reduction at p. The Tamagawa factor $[\mathcal{C}^{\min}(\mathbb{Q}_p) : \mathcal{C}^{\min}_0(\mathbb{Q}_p)]$ is either 1, 2, 3 or 4, all of which are coprime to $p \geq 5$. We thus have an isomorphism $\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty] \cong \mathcal{C}^{\min}_0(\mathbb{Q}_p)[p^\infty]$. Again the formal group is p-torsion free, so $\mathcal{C}^{\min}_0(\mathbb{Q}_p)[p^\infty]$ coincides with the p^∞-torsion in the group of non-singular points $\widetilde{\mathcal{C}^{\min}}(\mathbb{F}_p) - \{\text{node}\}$. But these non-singular points look like $\mathbb{F}_p^\times$ which has no points of order p, so neither does $\mathcal{C}^{\min}(\mathbb{Q}_p)$.

Case (iii): $p \| N_E$ and $a_p(E) = +1$, $p \nmid \mathrm{ord}_p\Big(\mathbf{q}_{\mathrm{Tate}}(\mathcal{C}^{\min})\Big)$.

This last situation corresponds to our elliptic curves being split multiplicative at p. The group of connected components $\mathcal{C}^{\min}(\mathbb{Q}_p)\big/\mathcal{C}^{\min}_0(\mathbb{Q}_p) \cong \mathbb{Z}\big/\mathrm{ord}_p\Big(\mathbf{q}_{\mathrm{Tate}}(\mathcal{C}^{\min})\Big)\mathbb{Z}$ has order coprime to p, by assumption. Again $\mathcal{C}^{\min}(\mathbb{Q}_p)[p^\infty] \cong \mathcal{C}^{\min}_0(\mathbb{Q}_p)[p^\infty]$, and an identical argument to case (ii) establishes that the p-part of $\mathcal{C}^{\min}(\mathbb{Q}_p)$ is trivial.

4. Global Euler-Poincaré Characteristics

It remains to give the proof of Proposition 2.3, i.e. to demonstrate why

$$\#H^1\Big(\Gamma, \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big) \times \prod_{l \in \Sigma} \Big[\mathrm{Ker}(\delta_l) : \mathrm{Im}(\lambda_0) \cap \mathrm{Ker}(\delta_l)\Big] \quad = \quad \#\mathcal{C}^{\min}(\mathbb{Q})[p^\infty]$$

whenever the analytic rank of E is zero.

Let's start by writing down the Poitou-Tate sequence for the optimal curve. It is an easy exercise to verify that $H^1\big(\mathbb{Q}_l,\ \mathcal{C}^{\min}[p^\infty]\big)\Big/H^1_\star\big(\mathbb{Q}_l,\ \mathcal{C}^{\min}[p^\infty]\big)$ is isomorphic to $H^1\big(\mathbb{Q}_l, \mathcal{C}^{\min}\big)[p^\infty]$ where '$\star = \mathrm{nr}$' if $l \neq p$, and '$\star = g$' if $l = p$. The exactness of the sequence

$$0 \to \mathrm{Sel}_{\mathbb{Q}}\big(\mathcal{C}^{\min}\big)[p^\infty] \to H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\Big) \overset{\lambda_0}{\to} \bigoplus_{l \in \Sigma} H^1\Big(\mathbb{Q}_l,\ \mathcal{C}^{\min}\Big)[p^\infty]$$
$$\to \mathrm{Hom}_{\mathrm{cont}}\Big(\mathcal{C}^{\min}(\mathbb{Q})\widehat{\otimes}\mathbb{Z}_p\ ,\ \mathbb{Q}/\mathbb{Z}\Big) \to H^2\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\Big) \to \cdots$$

is then an old result of Cassels.

Lemma 4.1. *If* $\mathrm{Sel}_{\mathbb{Q}}\big(\mathcal{C}^{\min}\big)[p^\infty]$ *is finite, then* $H^2\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\big)=0$.

The proof is well-known to the experts. It's a basic consequence of the cyclotomic Iwasawa theory of elliptic curves, e.g. see Coates' textbook on the subject.

If we mimic the same approach Λ-adically, the Poitou-Tate exact sequence reads as

$$0\to \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\to$$
$$\to H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},A_{\mathbb{T}_\infty}\Big)\xrightarrow{\lambda_\infty^\dagger}\bigoplus_{l\in\Sigma}\frac{H^1\big(\mathbb{Q}_l,A_{\mathbb{T}_\infty}\big)}{H^1_\star\big(\mathbb{Q}_l,A_{\mathbb{T}_\infty}\big)}\to\widehat{\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)}\to\cdots$$

where the compact Selmer group is defined to be

$$\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)\ :=$$
$$:=\ \mathrm{Ker}\left(H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathbb{T}_\infty\big)\xrightarrow{\oplus\mathrm{res}_l}\bigoplus_{l\neq p}\frac{H^1\big(\mathbb{Q}_l,\mathbb{T}_\infty\big)}{H^1\big(\mathbb{Q}_l,A_{\mathbb{T}_\infty}\big)^\perp}\oplus\frac{H^1\big(\mathbb{Q}_p,\mathbb{T}_\infty\big)}{X(\mathbb{Q}_p)}\right).$$

In fact $H^1\big(\mathbb{Q}_l,A_{\mathbb{T}_\infty}\big)$ is orthogonal to all of $H^1\big(\mathbb{Q}_l,\mathbb{T}_\infty\big)$ under Pontrjagin duality, so the local conditions at $l\neq p$ are completely redundant.

Proposition 4.2. *If* $L(E,1)\neq 0$, *then the compact version* $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ *is zero.*

The proof is rather lengthy – we postpone it till the end of this section.

As a corollary, the restriction map $\lambda_\infty^\dagger$ must be surjective at the Λ-adic level. Taking Γ-cohomology, we obtain a long exact sequence

$$0\longrightarrow\mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)^\Gamma\longrightarrow H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\Big)^\Gamma\xrightarrow{\lambda_\infty}\bigoplus_{l\in\Sigma}\left(\frac{H^1\big(\mathbb{Q}_l,A_{\mathbb{T}_\infty}\big)}{H^1_\star\big(\mathbb{Q}_l,A_{\mathbb{T}_\infty}\big)}\right)^\Gamma$$
$$\longrightarrow H^1\Big(\Gamma,\ \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big)\longrightarrow H^1\Big(\Gamma,\ H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\big)\Big).$$

The right-most term is zero, since it is contained inside $H^2\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\Big)$ which vanishes by Lemma 4.1. We can then compare the cokernels of λ_0 and

λ_∞ via the commutative diagram, with exact columns:

$$\begin{tikzcd}
\vdots \arrow[d] & \vdots \arrow[d] \\
H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathcal{C}^{\min}[p^\infty]\Big) \arrow[r, "\beta"] \arrow[d, "\lambda_0"'] & H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\ A_{\mathbb{T}_\infty}\Big)^\Gamma \arrow[d, "\lambda_\infty"'] \\
\bigoplus_{l\in\Sigma} H^1\Big(\mathbb{Q}_l,\ \mathcal{C}^{\min}\Big)[p^\infty] \arrow[r, "\oplus\delta_l"] \arrow[d] & \bigoplus_{l\in\Sigma}\left(\frac{H^1(\mathbb{Q}_l, A_{\mathbb{T}_\infty})}{H^1_\star(\mathbb{Q}_l, A_{\mathbb{T}_\infty})}\right)^\Gamma \arrow[d] \\
\mathrm{Hom}_{\mathrm{cont}}\Big(\mathcal{C}^{\min}(\mathbb{Q})\widehat{\otimes}\mathbb{Z}_p\ ,\ \mathbb{Q}/\mathbb{Z}\Big) \arrow[r, dashed] \arrow[d] & H^1\Big(\Gamma,\ \mathrm{Sel}_{\mathbb{Q}}(\rho_\infty)\Big) \arrow[d] \\
0 & 0
\end{tikzcd}$$

Figure 3.

Remark: Focussing momentarily on the homomorphisms δ_l and λ_0, one deduces

$$\Big[\mathrm{Ker}\big(\oplus\,\delta_l\big) : \mathrm{Ker}\big(\oplus\,\delta_l\big)\cap\mathrm{Im}(\lambda_0)\Big] \quad = \quad \frac{\Big[\bigoplus_{l\in\Sigma} H^1\big(\mathbb{Q}_l,\ \mathcal{C}^{\min}\big)[p^\infty] : \mathrm{Im}(\lambda_0)\Big]}{\Big[\mathrm{Im}\big(\oplus\,\delta_l\big) : \oplus\delta_l\big(\mathrm{Im}(\lambda_0)\big)\Big]}$$

upon applying the Snake Lemma to the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}\big(\oplus\,\delta_l\big) \arrow[r] & H^1\big(\mathbb{Q}_l,\ \mathcal{C}^{\min}\big)[p^\infty] \arrow[r, "\oplus\delta_l"] & \mathrm{Im}\big(\oplus\,\delta_l\big) \arrow[r] & 0 \\
& \bigcup & \bigcup & \bigcup & \\
0 \arrow[r] & \mathrm{Ker}\big(\oplus\,\delta_l\big)\cap\mathrm{Im}(\lambda_0) \arrow[r] & \mathrm{Im}(\lambda_0) \arrow[r, "\oplus\delta_l"] & \oplus\delta_l\big(\mathrm{Im}(\lambda_0)\big) \arrow[r] & 0\,.
\end{tikzcd}$$

The numerator above equals $\#\mathrm{Hom}_{\mathrm{cont}}\Big(\mathcal{C}^{\min}(\mathbb{Q})\widehat{\otimes}\mathbb{Z}_p, \mathbb{Q}/\mathbb{Z}\Big)$, which has the same size as the p-primary subgroup of $\mathcal{C}^{\min}(\mathbb{Q})$. Casting a cold eye over Figure 3, one exploits the surjectivity of $\oplus\delta_l$ to conclude the denominator term is $\#\mathrm{Coker}(\lambda_\infty)$. Equivalently,

$$\prod_{l\in\Sigma}\Big[\mathrm{Ker}(\delta_l) : \mathrm{Im}(\lambda_0)\cap\mathrm{Ker}(\delta_l)\Big] \quad = \quad \frac{\#\mathcal{C}^{\min}(\mathbb{Q})[p^\infty]}{\#\mathrm{Coker}(\lambda_\infty)}$$

which finishes off the demonstration of 2.3.

The proof of Proposition 4.2:
There are three stages. We first show that the compact Selmer group is Λ-torsion. Using a version of Nekovář's control theory along the critical line $(s,k) \in \{1\} \times \mathbb{Z}_p$, we next establish its finiteness. Lastly, we embed $\mathfrak{Sel}$ inside a tower of rational points, whose structure is narrow enough to imply the Selmer group is zero.

Examining the behaviour of our big dual exponential $\mathrm{EXP}^*_{\mathbb{T}_\infty}$ from [De, Th 3.3], there is a tautological sequence of Λ-homomorphisms

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty) \arrow[r] & H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathbb{T}_\infty\big) \arrow[r, "\mathrm{loc}_p(-)\ \mathrm{mod}\ X(\mathbb{Q}_p)"] & \dfrac{H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)}{X(\mathbb{Q}_p)} \arrow[d, "\mathrm{EXP}^*_{\mathbb{T}_\infty}"'] \\
 & & & \Lambda[1/p]
\end{tikzcd}$$

which is exact along the row. A global Euler characteristic calculation shows that

$$\begin{aligned}
\mathrm{rank}_\Lambda\Big(H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_\infty\big)\Big) \ &= \ \mathrm{rank}_\Lambda\Big(H^2\big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_\infty\big)\Big) + 1 \\
&\leq \ \mathrm{rank}_{\mathbb{Z}_p}\Big(H^2\big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathrm{Ta}_p(\mathcal{C}^{\min})\big)\Big) + 1 \\
&\overset{\text{by Kato}}{=} \ 0 \ + \ 1
\end{aligned}$$

– the final equality lies very deep, and follows from [Ka, Th 14.5(1)].
On the other hand, the weight-deformation of Kato's zeta-element will generate rank one Λ-submodules inside both of $H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathbb{T}_\infty\big)$ and $H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)\Big/X(\mathbb{Q}_p)$. To verify this claim, observe that $\mathrm{EXP}^*_{\mathbb{T}_\infty}$ modulo $u_0 - 1$ sends the zeta-element to a multiple of $\frac{L_{Np}(\mathcal{C}^{\min},1)}{\Omega^+_{\mathcal{C}^{\min}}}$, which is non-zero. This means the image of $\mathrm{EXP}^*_{\mathbb{T}_\infty} \circ \mathrm{loc}_p$ is not contained in the augmentation ideal, and so is abstractly isomorphic to Λ.

Remark: In summary, we have just shown that the global H^1 has Λ-rank one. Because the quotient $H^1\big(\mathbb{Q}_p, \mathbb{T}_\infty\big)\Big/X(\mathbb{Q}_p)$ is Λ-torsion free and also has rank one, we may identify $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ with the Λ-torsion submodule of $H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q},\ \mathbb{T}_\infty\big)$.

Question. *Does $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ contain any pseudo-summands of the form $\Lambda\big/F_j^{e_j}\Lambda$*

for some irreducible distinguished polynomial F_j and for $e_j \in \mathbb{N}$?

To provide an answer, we will need to specialise at arithmetic points of $\mathrm{Spec}(\Lambda)^{\mathrm{alg}}$. For any de Rham $\mathrm{Gal}\big(\mathbb{Q}_\Sigma/\mathbb{Q}\big)$-lattice $\mathbf{T}$, the Selmer group $H^1_{g,\mathrm{Spec}\mathbb{Z}}$

is defined by

$$H^1_{g,\mathrm{Spec}\mathbb{Z}}\big(\mathbb{Q},\mathbf{T}\big) := \mathrm{Ker}\left(H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q},\mathbf{T}\big) \overset{\oplus\mathrm{res}_l}{\longrightarrow} \bigoplus_{l\neq p} H^1\big(I_l,\mathbf{T}\big) \oplus \frac{H^1\big(\mathbb{Q}_p,\mathbf{T}\big)}{H^1_g\big(\mathbb{Q}_p,\mathbf{T}\big)}\right) .$$

Control Theorem. [Sm, Th 5.1] *For all bar finitely many integral weights $k \geq 2$, the induced specialisation*

$$\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty) \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p \quad\longrightarrow\quad H^1_{g,\mathrm{Spec}\mathbb{Z}}\Big(\mathbb{Q}\ ,\ \mathbb{T}_\infty \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p\Big)$$

has finite kernel and cokernel, bounded independently of the choice of $\sigma_k : \Lambda \twoheadrightarrow \mathbb{Z}_p$.

Kato's Theorem. [Ka, Th 14.2] *For all integral weights $k \geq 3$, the Bloch-Kato compact Selmer group $H^1_{f,\mathrm{Spec}\mathbb{Z}}\Big(\mathbb{Q}\ ,\ \mathbb{T}_\infty \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p\Big)$ is finite.*

Actually Kato proves this result for discrete Selmer groups, but they are equivalent statements. Note that $\mathbb{T}_\infty \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p$ is a lattice inside $V^*_{\mathbf{f}_k}$, the contragredient of Deligne's $G_{\mathbb{Q}}$-representation attached to the eigenform $\mathbf{f}_k \in \mathcal{S}_k^{\mathrm{ord}}\big(\Gamma_0(Np^r),\omega^{2-k}\big)$. The non-vanishing of the L-value $L(\mathbf{f}_k,1)$ forces these Selmer groups to be finite.

Corollary 4.3. *For almost all $k \geq 2$, the order of $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty) \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p$ is bounded.*

Proof: We first observe that $H^1_{g,\mathrm{Spec}\mathbb{Z}}(\mathbb{Q},V^*_{\mathbf{f}_k})$ coincides with $H^1_{f,\mathrm{Spec}\mathbb{Z}}(\mathbb{Q},V^*_{\mathbf{f}_k})$ unless the local condition $H^1_g(\mathbb{Q}_p,V^*_{\mathbf{f}_k})$ is strictly larger than $H^1_f(\mathbb{Q}_p,V^*_{\mathbf{f}_k})$. However,

$$\dim_{\mathbb{Q}_p}\Big(H^1_{g/f}(\mathbb{Q}_p,V^*_{\mathbf{f}_k})\Big) \quad=\quad \dim_{\mathbb{Q}_p}\Big(\mathbf{D}_{\mathrm{cris}}\big(V_{\mathbf{f}_k}(1)\big)/(\varphi-1)\Big) \text{ by [BK, Cor 3.8.4]}$$

and an argument involving slopes of the Frobenius φ shows this dimension is zero.

By Kato's theorem $H^1_{f,\mathrm{Spec}\mathbb{Z}}$ is finite, so it lies in $H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\mathbb{T}_\infty\otimes_{\Lambda,\sigma_k}\mathbb{Z}_p\Big)[p^\infty]$; the latter torsion is identified with $H^0\Big(\mathbb{Q}_\Sigma/\mathbb{Q},\big(\mathbb{T}_\infty \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p\big)\otimes\mathbb{Q}/\mathbb{Z}\Big)$ via a standard technique in continuous cohomology. It follows from the Control Theorem, that

$$\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)\otimes_{\Lambda,\sigma_k}\mathbb{Z}_p \overset{\mathrm{nat}}{\to} H^1_{f,\mathrm{Spec}\mathbb{Z}}\Big(\mathbb{Q},\mathbb{T}_\infty\otimes_{\Lambda,\sigma_k}\mathbb{Z}_p\Big) \hookrightarrow \Big(\big(\mathbb{T}_\infty\otimes_{\Lambda,\sigma_k}\mathbb{Z}_p\big)\otimes\mathbb{Q}/\mathbb{Z}\Big)^{G_{\mathbb{Q}}}$$

has kernel killed by a universal power p^{ν_1} say, independent of the weight k. Let us choose a prime $l \nmid Np$. By definition $1-a_l(\mathbf{f}_k).\mathrm{Frob}_l + l < l >^{k-2} .\mathrm{Frob}_l^2$ is zero on $V^*_{\mathbf{f}_k}$, and $1-a_l(\mathbf{f}_k)+l<l>^{k-2}$ must kill off $\Big(\big(\mathbb{T}_\infty\otimes_{\Lambda,\sigma_k}\mathbb{Z}_p\big)\otimes\mathbb{Q}/\mathbb{Z}\Big)^{G_{\mathbb{Q}}}$

because Frobenius acts trivially on the $G_{\mathbb{Q}}$-invariants. We claim that there are infinitely many choices of l for which $1 - a_l(\mathbf{f}_k) + l < l >^{k-2} \neq 0$. If not,

$$1 - a_l(\mathbf{f}_k)l^{-s} + l < l >^{k-2} l^{-2s} \;=\; \big(1 - l^{-s}\big)\big(1 - \omega^{2-k}(l)l^{k-1-s}\big) \quad \text{for all } l \notin S$$

where S is some finite set containing Σ. Proceeding further down this cul-de-sac, we obtain an equality of incomplete L-functions $L_S(\mathbf{f}_k, s) = \zeta_S(s)L_S(\omega^{2-k}, s+1-k)$ which is patently ridiculous, as $\mathbf{f}_k$ is not an Eisenstein series!
If $k \equiv k' \bmod (p-1)p^c$, then

$$1 - a_l(\mathbf{f}_k) + l < l >^{k-2} \;\equiv\; 1 - a_l(\mathbf{f}_{k'}) + l < l >^{k'-2} \quad \text{modulo } p^{c+1}\ .$$

For each class τ modulo $p-1$, we can cover weight-space by a finite collection of open disks $D_1^\tau, \ldots, D_{n(\tau)}^\tau$ upon which $\mathrm{ord}_p\big(1 - a_l(\mathbf{f}_k) + l < l >^{k-2}\ \big)$ is constant for every $k \in D_j^\tau$, $k \equiv \tau (\bmod\ p-1)$. Setting ν_2 equal to the non-negative integer

$$\max_{\tau \bmod p-1} \left\{ \max_{1 \leq j \leq n(\tau)} \Big\{ \mathrm{ord}_p\big(1 - a_l(\mathbf{f}_k) + l < l >^{k-2}\ \big) \text{ with } k \in D_j^\tau,\ k \equiv \tau \Big\} \right\},$$

clearly p^{ν_2} annihilates all the $\Big(\big(\mathbb{T}_\infty \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p\big) \otimes \mathbb{Q}/\mathbb{Z}\Big)^{G_{\mathbb{Q}}}$'s. We deduce that $p^{\nu_1+\nu_2}$ kills off $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty) \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p$ for almost all $k \geq 3$, and the corollary is proved.

Remark: The answer to the question posed above is therefore negative, i.e. there can exist no pseudo-summands of the shape $\Lambda/F_j^{e_j}\Lambda$ lying inside of $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ (otherwise the specialisations $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty) \otimes_{\Lambda,\sigma_k} \mathbb{Z}_p$ would have unbounded order for varying weights $k \geq 2$, which violates Corollary 4.3). The compact Selmer group is of finite-type over the local ring Λ, and it follows from the structure theory that $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ must be a finite abelian p-group, of order dividing $p^{\nu_1+\nu_2}$.

Let us recall the definition of the degeneration maps between modular curves. For integers $d \geq 1$ and $m, n \geq 5$ with $dm \big| n$, the finite map $\pi_d : X_1(n) \to X_1(m)$ operates on the affine curves $Y_1(-)$ by the rule

$$\pi_d\left(A,\ \mu_n \overset{\theta}{\hookrightarrow} A[n]\right) \;=\; \left(A',\ \mu_m \overset{\theta'}{\hookrightarrow} A'[m]\right)$$

where $A' = A/\theta(\mu_d)$, and the injection $\theta' : \mu_m \hookrightarrow \mu_{n/d} \overset{d}{\overset{\sim}{\leftarrow}} \mu_n/\mu_d \overset{\theta \bmod \mu_d}{\hookrightarrow} A/\theta(\mu_d)$.

Hida [H1] identified the $\Gamma^{p^{r-1}}$-coinvariants of $\mathbb{T}_\infty$, with the Tate module of a p-divisible subgroup of jac $X_1(n)$ at level $n = Np^r$. The natural composition

$$H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_\infty\Big) \cong \varprojlim_{r\geq 1} H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q}, \big(\mathbb{T}_\infty\big)_{\Gamma^{p^{r-1}}}\Big) \hookrightarrow \varprojlim_{\pi_{p\,*}} H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}}\Big)$$

injects $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ into the projective limit $\varprojlim_{\pi_{p\,*}}\Big(H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}}\Big)[p^\infty]\Big)$. Again it's continuous cohomology, so the $\mathbb{Z}_p$-torsion in $H^1\Big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}}\Big)$ is then isomorphic to $H^0\Big(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}} \otimes \mathbb{Q}/\mathbb{Z}\Big) = J_r^{\mathrm{ord}}(\mathbb{Q})[p^\infty]$ as finite groups.

Lemma. *(Nekovár̃)* [NP, 1.6.6] *(i)* $\pi_{1\,*}\big(\mathbf{e}_{\mathrm{ord}}.Ta_p(J_{r+1})\big) \subset p\,\big(\mathbf{e}_{\mathrm{ord}}.Ta_p(J_r)\big)$*;* *Let* $\frac{1}{p}\pi_{1\,*} : Ta_p(J_{r+1})^{\mathrm{ord}} \to Ta_p(J_r)^{\mathrm{ord}}$ *denote the map satisfying* $p\left(\frac{1}{p}\pi_{1\,*}\right) = \pi_{1\,*}$.

(ii) $\left(\frac{1}{p}\pi_{1\,*}\right) \circ \pi_1^* =$ *multiplication by* p *on* $\mathbf{e}_{\mathrm{ord}}.Ta_p(J_r)$*;*

(iii) $\pi_1^* \circ \left(\frac{1}{p}\pi_{1\,*}\right) = \sum_{\gamma\in\Gamma_r/\Gamma_{r+1}}\langle\gamma\rangle$ *on* $\mathbf{e}_{\mathrm{ord}}.Ta_p(J_{r+1})$ *where* $\Gamma_r = \Gamma^{p^{r-1}}$*;*

(iv) $\pi_{p\,*} = U_p \circ \left(\frac{1}{p}\pi_{1\,*}\right)$ *on* $\mathbf{e}_{\mathrm{ord}}.Ta_p(J_{r+1})$.

We shall use these facts directly, to show the triviality of the compact Selmer group. Because it is finite of order dividing $p^{\nu_1+\nu_2}$, for large enough $r \gg 1$ we can realise $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty)$ as a subgroup $\mathbb{S}_r$ of jac $X_1(Np^r)^{\mathrm{ord}}(\mathbb{Q})[p^{\nu_1+\nu_2}]$.

The sequence of $\mathbb{S}_r$'s is compatible with respect to the degeneration maps $\pi_{p\,*}$ and π_1^* : jac $X_1(Np^r)(\overline{\mathbb{Q}})[p^\infty] \longrightarrow$ jac $X_1(Np^{r+1})(\overline{\mathbb{Q}})[p^\infty]$, so for any $e \geq 0$

$$\mathbb{S}_r \;=\; \big(\pi_{p\,*}\big)^e\Big(\mathbb{S}_{r+e}\Big) \;\cong\; \big(\pi_{p\,*}\big)^e \circ \big(\pi_1^*\big)^e\Big(\mathbb{S}_r\Big)\,.$$

By part (iv) of this lemma $\big(\pi_{p\,*}\big)^e$ coincides with $\Big(U_p \circ \left(\frac{1}{p}\pi_{1\,*}\right)\Big)^e$, and the covariant action of the U_p-operator is invertible on the ordinary locus. Consequently

$$\mathbb{S}_r \;\cong\; a_p(\mathbf{f})^e \times \left(\frac{1}{p}\pi_{1\,*}\right)^e \circ \big(\pi_1^*\big)^e\Big(\mathbb{S}_r\Big) \;\overset{\text{by (ii)}}{=}\; a_p(\mathbf{f})^e \times p^e\,\big(\mathbb{S}_r\big)$$

and picking $e \geq \nu_1 + \nu_2$, we see that $\mathfrak{Sel}_{\mathbb{Q}}(\mathbb{T}_\infty) \cong \mathbb{S}_r \subset J_r[p^{\nu_1+\nu_2}]$ must be zero. The proof of Proposition 4.2 is thankfully over.

References

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in the Grothendieck Festchrift I, Progress in Math. 86, Birkhäuser (1990), 333-400.

[CH] J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, Journal Math. Soc. Japan 53 (2001), 175-235.

[De] D. Delbourgo, *Super Euler systems and ordinary deformations of modular symbols*, preprint (2004).

[DS] D. Delbourgo and P. Smith, *Kummer theory for big Galois representations*, to appear in Math. Proc. of the Camb. Phil. Soc.

[GS] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. 111 (1993), 401-447.

[H1] H. Hida, *Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. 85 (1986), 545-613.

[H2] H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. École Norm. Sup. (4) 19 (1986), 231-273.

[Ka] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, preprint (2002).

[MW] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Math. 59 (1986), 231-264.

[NP] J. Nekovář and A. Plater, *On the parity ranks of Selmer groups*, Asian Journal Math. (2) 4 (2000), 437-498.

[Sm] P. Smith, PhD Thesis, University of Nottingham (2006).

[St] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. 98 (1989), 75-106.

Daniel Delbourgo
Department of Mathematics
University Park
Nottingham
England NG7 2RD
dd@maths.nott.ac.uk

Coleman Integration Versus Schneider Integration on Semistable Curves

To John Coates, on the occasion of his 60th birthday

Ehud de Shalit

Received: August 17, 2005
Revised: February 27, 2006

Abstract. The purpose of this short note is to clarify the relation between p-adic integration on curves with semistable reduction, and the filtered (Φ, N)-module attached to the curve, following the work of Coleman and Iovita.

2000 Mathematics Subject Classification:
Keywords and Phrases:

0.1. The filtered (Φ, N)-module attached to a semistable curve. Let K be a local field of characteristic 0 and residual characteristic p. Denote by $\mathcal{O}_K$ its ring of integers, and by κ its residue field. Denote by K_0 the fraction field of the Witt vectors of κ, and by σ its Frobenius automorphism. Thus K/K_0 is a finite, totally ramified extension.

By a *curve X over $\mathcal{O}_K$* we shall mean a proper flat scheme over $\mathcal{O}_K$ of relative dimension 1. We denote its generic fiber by X_K and its special fiber by X_κ. We assume that X has *semistable reduction.* This means that X is regular and X_κ is a reduced curve whose singularities are ordinary double points. [Some authors use a less restrictive definition, in which X need not be regular, but this will require some modifications in what we do below.] We assume also that X_κ is *split*: the irreducible components of the (geometric) special fiber, its singular points, and the two tangents at each singular point, are all defined over κ. This can be achieved if we replace K by a finite unramified extension.

Let $H = H^1_{dR}(X_K/K)$ be the first de-Rham cohomology of X_K. It can be identified with the space of *differentials of the second kind* on X_K modulo exact differentials. H is a finite dimensional vector space over K, and it carries the Hodge filtration (differentials of the first kind)

$$0 \subset F^1_{dR} = H^0(X_K, \Omega^1) \subset F^0_{dR} = H. \tag{0.1}$$

Let $X_\kappa^\times$ be the log-scheme associated to the special fiber with its induced log-structure [Ill]. Let $D = H^1_{crys}(X_\kappa^\times/K_0)$ be its first log-crystalline cohomology [LS, H-K]. Recall that D is a finite dimensional vector space over K_0, which comes equipped with a σ-linear bijective endomorphism Φ (*Frobenius*) and a nilpotent endomorphism N (*monodromy*) satisfying the relation

$$N\Phi = p\Phi N. \tag{0.2}$$

For every prime π of K Hyodo and Kato constructed a *comparison isomorphism*

$$\rho_\pi : D \otimes_{K_0} K \simeq H \tag{0.3}$$

and the following relation holds for any two choices of a uniformizer

$$\rho_{\pi'} = \rho_\pi \circ \exp\left(\log(\pi'/\pi)N\right). \tag{0.4}$$

Note that the exponential is in fact a finite sum because N is nilpotent.
The structure $(H, F^{\cdot}_{dR}, D, \Phi, N, \rho_\pi)$ is the *filtered* (Φ, N)*-module* attached to X.

0.2. The weight decomposition. Let $\phi = \Phi^f$, where $f = [\kappa : \mathbb{F}_p]$, be the relative Frobenius, which now acts linearly on D. Write $q = p^f$ for the cardinality of κ. By [LS] (see [Mo] in higher dimensions) we have a *weight decomposition*

$$D = D^0 \oplus D^1 \oplus D^2 \tag{0.5}$$

where ϕ acts on D^i with eigenvalues which are q-Weil numbers of weight i (algebraic integers whose absolute value in any complex embedding is $q^{i/2}$). From the relation $N\phi = q\phi N$ we deduce that N must vanish on D^0 and D^1, and must map D^2 to D^0. In fact, it is known that it maps D^2 *isomorphically* onto D^0. This is a special case of the p-adic monodromy-weight conjecture.
By means of the isomorphism ρ_π we transport the weight decomposition to H,

$$H = H^0 \oplus H^1 \oplus H^2_\pi \tag{0.6}$$

where only the last summand, but not H^0 or H^1, depends on π, because N vanishes on D^0 and D^1. The weight filtration is defined by

$$F^i_W H = \sum_{j \le i} H^j. \tag{0.7}$$

Our goal is to *explain the weight decomposition of H in terms of the generic fiber only,* using two transcendental processes in rigid analysis - Schneider and Coleman integration. The main theorem is a reformulation of the work of Coleman and Iovita [Co-I1], and only the presentation, and a few trivial observations, are new. We have a vague hope that similar techniques might help to understand the weight decomposition, and in particular the monodromy-weight conjecture, for the cohomology of higher dimensional varieties as well. For p-adically uniformized varieties this was done in [dS], see also [Ito]. We also note that [Co-I2] and [GK] treat Frobenius and monodromy in more general situations, the first reference in cohomology of curves with coefficients, and the second in higher dimensions.

0.3. Schneider integration. To describe the main theorem, consider the *degeneration complex* Δ of X (also called the dual graph of the special fiber). Its *vertices* Δ_0 are the irreducible components of X_κ. Its *edges* Δ_1 are the singular points of X_κ (recall that the special fiber is assumed to be split). Each singular point, being an ordinary double point, determines two distinct analytic branches. The irreducible components on which these analytic branches lie, which may be the same, are the two end points of the edge. An *orientation* of an edge is an ordering of the two analytic branches at the singularity. We denote by $\vec{\Delta}_1$ the set of oriented edges, and by $\vec{\Delta}_1(v)$ the oriented edges originating at a vertx v. Note that if the two end points of an edge e are distinct, at most one of the oriented edges $\varepsilon, \bar{\varepsilon}$ lying over e may belong to $\vec{\Delta}_1(v)$, but if e is a loop based at v, then both of them belong there.

We introduce the space of *harmonic* 1-*cochains* on Δ which we denote by $C^1_{har}(\Delta)$. These are the maps $f : \vec{\Delta}_1 \to K$ satisfying

$$\text{(i) } f(\bar{\varepsilon}) = -f(\varepsilon), \text{ (ii) } \forall v \sum_{\varepsilon\in\vec{\Delta}_1(v)} f(\varepsilon) = 0. \tag{0.8}$$

There is a canonical isomorphism

$$\nu : C^1_{har}(\Delta) \simeq H^1(\Delta, K), \tag{0.9}$$

which sends a harmonic cochain to the singular cohomology class that it represents.

Let X^{an} denote the rigid analytic curve (over $\bar{K}$) attached to $X_{\bar{K}}$. There is a well known "*retraction*" map $r : X^{an} \to |\Delta|$. The inverse image under r of a vertex v consists of an affinoid with good reduction X_v. The *reduction* of X_v is the smooth part of Y_v, the irreducible component of X_κ labelled by v. The inverse image under r of an open edge e is an annulus X_e, isomorphic to

$$\{z|\ |\pi| < |z| < 1\}, \tag{0.10}$$

and an orientation of e determines an orientation of the annulus. All the points in X_e reduce in the special fiber to the singular point labelled by e.

If ω is a regular differential, and ε is an orientation on e, $res_\varepsilon(\omega)$ will denote the residue of ω with respect to a local parameter z on X_e compatible with ε. Clearly

$$res_{\bar{\varepsilon}}\omega = -res_\varepsilon\omega, \tag{0.11}$$

and the rigid analytic Cauchy theorem guarantees that

$$\sum_{\varepsilon\in\vec{\Delta}_1(v)} res_\varepsilon(\omega) = 0. \tag{0.12}$$

Defining

$$c_\omega(\varepsilon) = res_\varepsilon(\omega) \tag{0.13}$$

we obtain a harmonic 1-cochain c_ω. This definition extends without any difficulty to differentials of the second kind. Indeed, such a differential may be locally (Zariski) modified by an exact differential to make it regular, so on each

X_e we may assume it is regular and define its residue as before. Cauchy's theorem still holds, so c_ω is harmonic. Since all the residues along annuli of exact differentials vanish, we get a well defined map

$$H \to C^1_{har}(\Delta), \quad [\omega] \mapsto c_\omega. \tag{0.14}$$

Passing to $H^1(\Delta, K)$ we obtain the *Schneider class*

$$S_\omega = \nu(c_\omega) \in H^1(\Delta, K) \tag{0.15}$$

of ω.

0.4. Coleman integration. To define the Coleman class of a differential of the second kind ω we use Coleman's p-adic integration [Co], [Co-dS]. Let $\tilde{\Delta}$ be the tree which is the universal covering of Δ, and

$$\tilde{X}^{an} = X^{an} \times_\Delta \tilde{\Delta} \tag{0.16}$$

the rigid analytic curve which is the fiber product of X^{an} with $\tilde{\Delta}$ over Δ (the map from X^{an} to Δ being the retraction map r). We shall denote by Γ the group of deck transformations of the covering $\tilde{\Delta} \to \Delta$ (or, equivalently of $\tilde{X}^{an} \to X^{an}$). We shall continue to denote by r also the map from $\tilde{X}^{an}$ to $|\tilde{\Delta}|$. Let $\tilde{X}(\tilde{v})$, for $\tilde{v} \in \tilde{\Delta}_0$, be the inverse image under r of the *star* of a vertex $\tilde{v}$. (The star is the union of the vertex with the open edges originating at $\tilde{v}$. Note that a loop in Δ based at v lifts in $\tilde{\Delta}$ to two distinct edges starting at $\tilde{v}$. If we assume that Δ has no loops, then $\tilde{X}(\tilde{v})$ is isomorphic to $X(v)$, the inverse image of the star of v in X^{an}.) In Coleman's language $\tilde{X}(\tilde{v})$ is a wide open space, and (if v is the image of $\tilde{v}$ in Δ) $\tilde{X}_{\tilde{v}} \approx X_v$ is an underlying affinoid with good reduction in $\tilde{X}(\tilde{v})$. One can define a Coleman primitive $F_{\pi,\tilde{v}}$ of ω in $\tilde{X}(\tilde{v})$. It is a locally analytic function which satisfies $dF_{\pi,\tilde{v}} = \omega$, and is uniquely determined up to an additive constant by its behavior under a rigid analytic (overconvergent) lifting of Frobenius to $\tilde{X}_{\tilde{v}}$. As the notation suggests, $F_{\pi,\tilde{v}}$ depends (on the annuli surrounding $\tilde{X}_{\tilde{v}}$ in $\tilde{X}(\tilde{v})$) on the choice of π. For a given π, though, and neighboring vertices $\tilde{v}$, $\tilde{u}$ of $\tilde{\Delta}$, $F_{\pi,\tilde{v}} - F_{\pi,\tilde{u}}$ is constant on the annulus where it is defined. Since $\tilde{\Delta}$ is a tree, it is possible to choose the constants in such a way that the $F_{\pi,\tilde{v}}$ glue to give a primitive F_π of ω on all of $\tilde{X}^{an}$. Since ω is Γ-invariant,

$$C_{\pi,\omega}(\gamma) = \gamma(F_\pi) - F_\pi = F_\pi \circ \gamma^{-1} - F_\pi \tag{0.17}$$

is constant for every deck transformation $\gamma \in \Gamma$. The homomorphism

$$C_{\pi,\omega} \in H^1(\Gamma, K) = H^1(\Delta, K) \tag{0.18}$$

is the obstruction to descending F_π to X^{an}. It vanishes if and only if F_π lives on X^{an}, not merely on $\tilde{X}^{an}$, namely if and only if we can "Coleman integrate" ω on X.

We shall prove that

$$C_{\pi',\omega} - C_{\pi,\omega} = -\log(\pi'/\pi) S_\omega. \tag{0.19}$$

Our reformulation of the paper [Co-I] can now be stated as follows.

Theorem 0.1. *(1) One has a canonical identification $H/F^1_W H \simeq C^1_{har}(\Delta)$ via the residue homomorphism. In other words, the cochains c_ω give us all the harmonic cochains, and $c_\omega = 0$ if and only if $S_\omega = 0$, if and only if $\omega \in F^1_W H$.*
(2) One has a canonical identification $F^0_W = H^0 = H^1(\Delta, K)$ and $C_{\pi,\omega}$ is the projection of $[\omega]$ onto H^0 relative to the decomposition $H = H^0 \oplus H^1 \oplus H^2_\pi$.
(3) The map ν corresponds to the monodoromy isomorphism

$$\nu : H/F^1_W H \simeq H^0 \tag{0.20}$$

derived from N.

Corollary 0.2. *The subspace H^1 is characterized as the space of differentials of the second kind for which a global Coleman primitive exists on X, regardless of π.*

Proof. Indeed, in view of the relation between $C_{\pi,\omega}$, $C_{\pi',\omega}$ and S_ω, the following are equivalent: (i) $C_{\pi,\omega} = 0$ for all π (ii) $C_{\pi,\omega} = 0$ for two π whose ratio is not a root of unity, (iii) $C_{\pi,\omega} = 0$ for some π and $S_\omega = 0$. In view of the theorem, the last property is equivalent to $[\omega] \in H^1$. □

Another corollary is the following. Denote by $g(X_K)$ the genus of the curve and by $g(\Delta)$ the genus of Δ.

Corollary 0.3. *For generic (all but finitely many) π the image of $C_{\pi,\omega}$ is all of $H^1(\Delta, K)$, and the dimension of the space of Coleman-integrable differentials of the second kind modulo exact differentials is $2g(X_K) - g(\Delta)$.*

Proof. Since S is surjective, so is C_π for all but finitely many π. □

The Hodge filtration did not play any role so far. The position of the differentials of the first kind in H with respect to the weight decomposition is mysterious. It is known that they are transversal to H^0, and that together with $F^1_W H$ they span H, but their intersection with H^1 can be large or small. All we can say is the following.

Corollary 0.4. *For generic π, the dimension of the Coleman-integrable differentials of the first kind is $g(X_K) - g(\Delta)$. The dimension of the space of differentials of the first kind for which a Coleman primitive exists for all π is*

$$g(X_K) - 2g(\Delta) \leq \dim(H^1 \cap F^1_{dR}) \leq g(X_K) - g(\Delta). \tag{0.21}$$

Proof. Since F^1_{dR} maps *onto* $C^1_{har}(\Delta)$ under the residue map, $S|_{F^1_{dR}}$ is still surjective, so the first assertion is proved as in the previous corollary. The upper bound in the second assertion follows from it, while the lower bound is obvious by counting dimensions. □

Remark 0.1. *In [Cz], Colmez defines primitives for* every *differential of the second kind on X_K, regardless of the type of reduction. His primitives are independent of a choice of π, and in general do not coincide with Coleman's primitives, except for the case of good reduction. He embeds the curve in its Jacobian, and uses the group structure of the latter to extend his integral from* *a neighborhood of the origin to the whole Jacobian. As an example, the reader may keep in mind the case of a Tate elliptic curve, of multiplicative period q_E. Colmez' primitive of the differential of the first kind in this case would be the same as Coleman's primitive, based on a branch of the p-adic logarithm which vanishes on q_E. It is clear that for curves of higher genus no branch of the logarithm conforms to all the periods. It is precisely the consideration of Coleman's theory, as opposed to Colmez', that gives us the possibility to identify the weight decomposition in the generic fiber (granted a choice of π is fixed).*

1. The proof

1.1. Establishing the relation between $C_{\pi,\omega}$ and S_ω. Denote by $\log_\pi$ the unique logarithm on $\bar{K}^\times$ for which $\log_\pi(\pi) = 0$. We recall that Coleman's primitive $F_{\pi,\tilde{v}}$ on the wide open $\tilde{X}(\tilde{v})$ satisfies the following. If $\tilde{\varepsilon} = (\tilde{v}, \tilde{u})$ is an oriented edge of $\tilde{\Delta}$, and $\tilde{X}_{\tilde{\varepsilon}}$ the corresponding oriented annulus in $\tilde{X}^{an}$, and if z is a local parameter on $\tilde{X}_{\tilde{\varepsilon}}$, then we may expand

$$\omega|_{\tilde{X}_{\tilde{\varepsilon}}} = \sum a_n z^n dz \tag{1.1}$$

and, up to an additive constant,

$$F_{\pi,\tilde{v}}|_{\tilde{X}_{\tilde{\varepsilon}}} = \sum_{n\neq -1} a_n(n+1)^{-1} z^{n+1} + a_{-1}\log_\pi(z). \tag{1.2}$$

Since

$$\log_{\pi'}(z) - \log_\pi(z) = -\log(\pi'/\pi) ord_K(z) \tag{1.3}$$

we get that (again, up to a constant)

$$F_{\pi'} - F_\pi|_{\tilde{X}_{\tilde{\varepsilon}}} = -\log(\pi'/\pi) res_\varepsilon(\omega) ord_K(z). \tag{1.4}$$

On an affinoid $\tilde{X}_{\tilde{v}}$, Coleman's primitive is independent of π, up to a constant. Let $\gamma \in \Gamma$ and normalize $F_{\pi'}$ and F_π so that they agree on $\tilde{X}_{\tilde{v}}$. On $\tilde{X}_{\gamma^{-1}(\tilde{v})}$ we shall then have

$$F_{\pi'} - F_\pi = -\log(\pi'/\pi) \sum_{\varepsilon\in(\tilde{v},\gamma^{-1}(\tilde{v}))} res_\varepsilon \omega, \tag{1.5}$$

where the sum is over the oriented edges leading from $\tilde{v}$ to $\gamma^{-1}(\tilde{v})$. This sum is just $S_\omega(\gamma)$, because S_ω is obtained from c_ω via the connecting homomorphism

$$C^1_{har}(\Delta) = C^1_{har}(\tilde{\Delta})^\Gamma \to H^1(\Gamma, K) \tag{1.6}$$

which is associated with the short exact sequence

$$0 \to K \to \tilde{C}^0_{har}(\tilde{\Delta}) \to C^1_{har}(\tilde{\Delta}) \to 0, \tag{1.7}$$

where $\tilde{C}^0_{har}(\tilde{\Delta})$ are the 0-cochains on the tree satisfying the mean value property. It follows that

$$C_{\pi',\omega}(\gamma) - C_{\pi,\omega}(\gamma) = -\log(\pi'/\pi) S_\omega(\gamma), \tag{1.8}$$

as we had to prove.

If we assume theorem 1, then (1.8) follows also from (0.4) and the fact that $N^2 = 0$ (and vice versa). In the rest of this chapter we shall show how to derive the main theorem from the paper [Co-I].

1.2. The weight filtration on H. Determining the weight *filtration* on H in terms of the general fiber, and finding an expression for N, do not require a choice of π, or the use of Coleman integration. These will be needed only for the weight *decomposition*, to be considered in the next section.

By GAGA, H can be identified with rigid de-Rham cohomology $H^1_{dR}(X^{an}_K)$. For simplicity let us assume from now on that Δ contains no loops, so we identify the wide open set $\tilde{X}(\tilde{v})$ with its image $X(v)$ in X^{an}. The covering $\mathcal{U} = \{X(v)\}$ of X^{an} is admissible and acyclic, defined over K. It follows that we may identify H with the space of rigid 1-hyper-cocycles

$$(1.9) \qquad \left\{ \begin{array}{c} (\omega_v, f_\varepsilon);\ \omega_v \in \Omega(X(v)),\ f_\varepsilon \in \mathcal{O}(X_\varepsilon),\ df_\varepsilon = \omega_v - \omega_u|_{X_\varepsilon} \\ \text{if } \varepsilon \text{ connects } u \text{ to } v, \text{and } f_{\bar{\varepsilon}} = -f_\varepsilon \end{array} \right\},$$

modulo the space of rigid 1-hyper-coboundaries: elements of the type $(df_v, f_v - f_u)$ for $f_v \in \mathcal{O}(X(v))$. Specifically, if ω is a differential of the second kind, we pick rational functions g_v so that $\omega_v = \omega - dg_v$ is holomorphic on $X(v)$, and put $f_\varepsilon = g_u - g_v$. The class $[\omega]$ is then represented by $(\omega_v, f_\varepsilon)$.

Since X_v is an affinoid with good reduction, the Frobenius morphism ϕ (of degree q) lifts to characteristic 0, to a rigid analytic mapping ϕ_v of X_v to itself. This rigid analytic Frobenius is *overconvergent:* there exists a strict neighborhood $X_v \subset X'_v \subset X(v)$ such that ϕ_v extends to a morphism of X'_v to $X(v)$. This X'_v can (and will) be chosen to consist of X_v together with an open annulus for each edge originating at v, and then the inclusion $X'_v \subset X(v)$ induces isomorphism on de Rham cohomology. We can therefore regard ϕ^*_v as an endomorphism of $H^1_{dR}(X(v))$. In fact, if we let Y^0_v be the smooth part of Y_v, the reduction of X_v, $H^1_{dR}(X(v))$ is nothing but the Monsky-Washnitzer cohomology of Y^0_v (tensored with K) and ϕ^*_v is its Frobenius. It is independent of the lifting.

The roots of the characteristic polynomial of ϕ^*_v on $H^1_{dR}(X(v))$ have weights 1 or 2. Moreover, there is an exact sequence

$$(1.10) \qquad 0 \to F^1_W H^1_{dR}(X(v)) \to H^1_{dR}(X(v)) \overset{res}{\to} \left(\oplus_{\varepsilon \in \vec{\Delta}_v} K\right)_0 \to 0$$

where res is the residue map, and F^1_W is the weight 1 subspace. The subscript 0 on the quotient means that we take only those elements in the direct sum whose coordinates add up to 0. On the weight 2 quotient ϕ^*_v acts by multiplication by q.

Let $F^0_W H$ be the subspace of H represented by classes $[(0, k_\varepsilon)]$, where the k_ε are constants. It is thus isomorphic to $H^1(\Delta, K)$. Coleman and Iovita prove that under the Hyodo-Kato isomorphism this subspace is the image of the weight zero part of D (combine Lemma I.4.2 and Theorem II.5.4 of their paper).

The quotient

$$(1.11) \qquad H/F^0_W H$$

is the image of H in $H^1_{dR}(\tilde{X}^{an})$ under pullback. It is the space of differentials of the second kind on X^{an}, modulo those which become exact on $\tilde{X}^{an}$. The residue map gives the filtration

$$0 \to gr^1_W H = F^1_W H/F^0_W H \to H/F^0_W H \overset{res}{\to} C^1_{har}(\Delta) \to 0, \tag{1.12}$$

which is the direct sum, over the vertices of Δ, of the short exact sequences recorded above. The surjectivity of the global residue map results from a dimension counting. Once again, Coleman and Iovita prove that under the Hyodo-Kato isomorphism, the Frobenius structure of $H/F^0_W H$ is the one described above, rigid analytically, in terms of the ϕ^*_v. (Compare how they define, in Section I.1, the Frobenius structure on

$$Ker(H^1_{dR}(X^0) \to H^1_{dR}(X^1)^-), \tag{1.13}$$

which is our $H/F^0_W H$, and apply their Theorem II.5.4.) It follows that F^1_W is indeed the weight 1 filtration, and $C^1_{har} = gr^2_W H$. Finally, that the monodromy operator is derived from the isomorphism ν between $C^1_{har}(\Delta)$ and $H^1(\Delta, K)$ also follows from [Co-I] (combine the description of N in Section I.1.1 and the commutative diagram on p.185). This checks all the statements of our main theorem, except for the identification of the weight decomposition in terms of Coleman integration.

1.3. The weight decomposition on H. Fix a choice of π. In Section I.1 of [Co-I] the authors describe a splitting of the projection $H \to H/F^0_W H$, whose image is $H^1 \oplus H^2_\pi$. Recall that an element of $H/F^0_W H$ is a collection $\{[\omega_v]\}$ of classes $[\omega_v] \in H^1_{dR}(X(v))$, such that for any oriented edge ε, connecting u to v, $res_\varepsilon \omega_u = res_\varepsilon \omega_v$. Let $F_{\pi,v}$ be the Coleman integral of ω_v on $X(v)$, described above, which is determined up to a constant. Since the residues of ω_u and ω_v on X_ε agree, the function

$$f_{\pi,\varepsilon} = F_{\pi,v} - F_{\pi,u} \in \mathcal{O}(X_\varepsilon) \tag{1.14}$$

is rigid analytic in the annulus. The 1-hyper-cocyle $(\omega_v, f_{\pi,\varepsilon})$ is well-defined up to a coboundary, and its class in H gives the desired splitting.

It is now easy to check that C_π vanishes on classes ω which are in the image of this splitting. Indeed, suppose the differential of the second kind ω is such that

$$\omega = \omega_v + dg_v \tag{1.15}$$

for a meromorphic function g_v on $X(v)$, and $g_u - g_v = f_{\pi,\varepsilon} = F_{\pi,v} - F_{\pi,u}$ on X_ε. Then $F_{\pi,u} + g_u$ agree on the annuli, hence glue to give a well defined Coleman meromorphic function $F_{\pi,\omega}$ on X^{an}, which is a global primitive of ω. It follows that $C_{\pi,\omega} = 0$.

On the other hand, if we start with a 1-hypercocycle $(0, k_\varepsilon)$ where the k_ε are constants, and if ω is a differential of the second kind for which there are meromorphic functions g_v on $X(v)$ such that $\omega = dg_v$ there, and $g_v - g_u = k_\varepsilon$ for an edge connecting u to v, then $[(k_\varepsilon)] \in H^1(\Delta, K)$ is the obstruction to integrating ω globally on X^{an}, hence is equal to $C_{\pi,\omega}$.

These computations show that C_π annihilates $H^1 \oplus H^2_\pi$, and is the identity map on H^0. This completes the proof of Theorem 1.

1.4. Relation to the Neron model of the Jacobian. Even though the primitive $\tilde{F}_{\pi,\omega}$ of a differential of the second kind ω need not descend to X^{an}, we may use it to define the integral

$$\int_D \omega \tag{1.16}$$

over *certain* divisors of degree 0, namely those who specialize in X_κ to divisors which avoid the singular points and are of degree 0 on each of the irreducible components Y_v separately. This is because such a divisor D intersects each affinoid X_v in a divisor D_v of degree 0, while $F_{\pi,v}$ is well defined, up to a constant, and independently of π, on X_v. Observe that the divisors in question are precisely those whose classes in Pic^0 represent the connected component $\mathcal{J}^0$ of the Neron model of the Jacobian of X_K.

References

[Co] R.Coleman, *Torsion points on curves and p-adic abelian integrals,* Ann. of Math. (2) 121 (1985), 111-168.

[Co-dS] R.Coleman and E.de Shalit, *P-adic regulators on curves and special values of p-adic L-functions,* Inv.Math. 93 (1988), 239-266.

[Co-I1] R.Coleman and A.Iovita, *The Frobenius and monodromy operators for curves and abelian varieties,* Duke Math.J. 97 (1999), 171-215.

[Co-I2] R.Coleman and A.Iovita, *Hidden structures on curves,* preprint, 2003.

[Cz] P.Colmez, *Périodes p-adiques des variétés abéliennes,* Math.Ann. 292 (1992), 629-644.

[dS] E.de Shalit, *The p-adic monodromy-weight conjecture for p-adically uniformized varieties,* Comp. Math. 141 (2005), 101-120.

[GK] E.Grosse-Kloenne, *Čech filtration and monodromy in Hyodo-Kato cohomology,* preprint, 2004.

[H-K] O.Hyodo and K.Kato, *Semistable reduction and crystalline cohomology with logarithmic poles,* in *Périodes p-adiques,* Astérisque 223 (1994), 221-268.

[Ill] L.Illusie, *Logarithmic spaces (according to K.Kato),* in *Barsotti symposium in algebraic geometry,* eds. V.Cristante and W.Messing, Perspectives in Mathematics, vol. 15 (Academic Press, San Diego, 1994), 183-204.

[I] T.Ito, *Weight-monodormy conjecture for p-adically uniformized varieties,* Preprint (2003), math.NT/0301201.

[LS] B.Le-Stum, *La structure de Hyodo-Kato pur les courbes,* Rend. Sem. Mat. Univ. Padova 94 (1995), 279-301.

[Mo] A.Mokrane, *La suite spectrale des poids en coho,ologie de Hyodo-Kato,* Duke Math.J. 72 (1993), 301-337.

Ehud de Shalit
Institute of Mathematics
Hebrew University
deshalit@math.huji.ac.il

On The Structure of Certain Galois Cohomology Groups

To John Coates on the occasion of his 60th birthday

Ralph Greenberg

Received: October 31, 2005
Revised: February 14, 2006

Abstract. This paper primarily concerns Galois cohomology groups associated to Galois representations over a complete local ring R. The underlying Galois module and the corresponding cohomology groups which we consider are discrete R-modules. Under certain hypotheses, we prove that the first cohomology group is an *almost divisible* R-module. We also consider the subgroup of locally trivial elements in the second cohomology group, proving under certain hypotheses that it is a *coreflexive* R-module.

2000 Mathematics Subject Classification: 11R23, 11R34
Keywords and Phrases: Galois cohomology, Iwasawa theory

1 Introduction

Suppose that K is a finite extension of $\mathbb{Q}$ and that Σ is a finite set of primes of K. Let K_Σ denote the maximal extension of K unramified outside of Σ. We assume that Σ contains all archimedean primes and all primes lying over some fixed rational prime p. The Galois cohomology groups that we consider in this article are associated to a continuous representation

$$\rho : \mathrm{Gal}(K_\Sigma/K) \longrightarrow GL_n(R)$$

where R is a complete local ring. We assume that R is Noetherian and commutative. Let $\mathfrak{m}$ denote the maximal ideal of R. We also assume that the residue field $R/\mathfrak{m}$ is finite and has characteristic p. Thus, R is compact in its

$\mathfrak{m}$-adic topology, as will be any finitely generated R-module. Let $\mathcal{T}$ denote the underlying free R-module on which $\mathrm{Gal}(K_\Sigma/K)$ acts via ρ. We define

$$\mathcal{D} = \mathcal{T} \otimes_R \widehat{R},$$

where $\widehat{R} = \mathrm{Hom}(R, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontryagin dual of R with a trivial action of $\mathrm{Gal}(K_\Sigma/K)$. Thus, $\mathcal{D}$ is a discrete abelian group which is isomorphic to $\widehat{R}^n$ as an R-module and which has a continuous R-linear action of $\mathrm{Gal}(K_\Sigma/K)$ given by ρ.

The Galois cohomology groups $H^i(K_\Sigma/K, \mathcal{D})$, where $i \geq 0$, can be considered as discrete R-modules too. The action of $\mathrm{Gal}(K_\Sigma/K)$ on $\mathcal{D}$ is R-linear and so, for any $r \in R$, the map $\mathcal{D} \to \mathcal{D}$ induced by multiplication by r induces a corresponding map on $H^i(K_\Sigma/K, \mathcal{D})$. This defines the R-module structure. It is not hard to prove that these Galois cohomology groups are cofinitely generated over R. That is, their Pontryagin duals are finitely generated R-modules. We will also consider the subgroup defined by

$$Ш^i(K, \Sigma, \mathcal{D}) = \ker\big(H^i(K_\Sigma/K, \mathcal{D}) \to \prod_{v \in \Sigma} H^i(K_v, \mathcal{D})\big).$$

Here K_v denotes the v-adic completion of K. Thus, $Ш^i(K, \Sigma, \mathcal{D})$ consists of cohomology classes which are locally trivial at all primes in Σ and is easily seen to be an R-submodule of $H^i(K_\Sigma/K, \mathcal{D})$. Of course, it is obvious that $Ш^0(K, \Sigma, \mathcal{D}) = 0$. It turns out that $Ш^i(K, \Sigma, \mathcal{D}) = 0$ for $i \geq 3$ too. However, the groups $Ш^1(K, \Sigma, \mathcal{D})$ and $Ш^2(K, \Sigma, \mathcal{D})$ can be nontrivial and are rather mysterious objects in general.

Suppose that one has a surjective, continuous ring homomorphism $\phi : R \to \mathcal{O}$, where $\mathcal{O}$ is a finite, integral extension of $\mathbb{Z}_p$. Such homomorphisms exist if R is a domain and has characteristic 0. Then $\mathcal{P}_\phi = \ker(\phi)$ is a prime ideal of R. One can reduce the above representation modulo $\mathcal{P}_\phi$ to obtain a representation $\rho_\phi : \mathrm{Gal}(K_\Sigma/K) \longrightarrow GL_n(\mathcal{O})$ which is simply the composition of ρ with the homomorphism $GL_n(R) \to GL_n(\mathcal{O})$ induced by ϕ. Thus, ρ is a deformation of ρ_ϕ and one can think of ρ as a family of such representations. The underlying Galois module for ρ_ϕ is $T_\phi = \mathcal{T}/\mathcal{P}_\phi\mathcal{T}$. This is a free $\mathcal{O}$-module of rank n. Let $D_\phi = T_\phi \otimes_{\mathcal{O}} \widehat{\mathcal{O}}$, where $\widehat{\mathcal{O}}$ is the Pontryagin dual of $\mathcal{O}$ with trivial Galois action. The Pontryagin dual of $R/\mathcal{P}_\phi$ is $\widehat{R}[\mathcal{P}_\phi]$, the submodule of $\widehat{R}$ annihilated by $\mathcal{P}_\phi$. Since $R/\mathcal{P}_\phi \cong \mathcal{O}$, we have $\widehat{R}[\mathcal{P}_\phi] \cong \widehat{\mathcal{O}}$. One can identify D_ϕ with $\mathcal{D}[\mathcal{P}_\phi]$. We can compare the cohomology of D_ϕ with $\mathcal{D}$ since one has a natural homomorphism

$$H^i(K_\Sigma/K, D_\phi) = H^i(K_\Sigma/K, \mathcal{D}[\mathcal{P}_\phi]) \longrightarrow H^i(K_\Sigma/K, \mathcal{D})[\mathcal{P}_\phi].$$

However, unless one makes certain hypotheses, this homomorphism may fail to be injective and/or surjective. Note also that all of the representation ρ_ϕ have the same residual representation, namely $\overline{\rho}$, the reduction of ρ modulo $\mathfrak{m}$. This gives the action of $\mathrm{Gal}(K_\Sigma/K)$ on $T_\phi/\mathfrak{m}T_\phi \cong \mathcal{T}/\mathfrak{m}\mathcal{T}$ or, alternatively, on the isomorphic Galois modules $D_\phi[\mathfrak{m}] \cong \mathcal{D}[\mathfrak{m}]$.

Assume that R is a domain. Let X denote the Pontryagin dual of $H^1(K_\Sigma/K, \mathcal{D})$. One can derive a certain lower bound for $\mathrm{rank}_R(X)$ by using Tate's theorems on global Galois cohomology groups. Let Y denote the torsion R-submodule of X. The main result of this paper is to show that if $\mathrm{rank}_R(X)$ is equal to the lower bound and if R and ρ satisfy certain additional assumptions, then the associated prime ideals for Y are all of height 1. Thus, under certain hypotheses, we will show that X has no nonzero pseudo-null R-submodules. By definition, a finitely generated, torsion R-module Z is said to be *"pseudo-null"* if the localization $Z_{\mathcal{P}}$ is trivial for every prime ideal $\mathcal{P}$ of R of height 1, or, equivalently, if the associated prime ideals for Z have height at least 2.

If the Krull dimension of R is $d = m+1$, where $m \geq 0$, then it is known that R contains a subring Λ such that *(i)* Λ is isomorphic to either $\mathbb{Z}_p[[T_1, ..., T_m]]$ or $\mathbb{F}_p[[T_1, ..., T_{m+1}]]$, depending on whether R has characteristic 0 or p, and *(ii)* R is finitely generated as a Λ-module. (See theorem 6.3 in [D].) One important assumption that we will often make is that R is reflexive as a Λ-module. We then say that R is a reflexive domain. It turns out that this does not depend on the choice of the subring Λ. An equivalent, intrinsic way of stating this assumption is the following: $R = \bigcap_{\mathcal{P}} R_{\mathcal{P}}$*, where* $\mathcal{P}$ *varies over all prime ideals of* R *of height 1.* Here $R_{\mathcal{P}}$ denotes the localization of R at $\mathcal{P}$, viewed as a subring of the fraction field $\mathcal{K}$ of R. Such rings form a large class. For example, if R is integrally closed, then R is reflexive. Or, if R is Cohen-Macaulay, then R will actually be a free Λ-module and so will also be reflexive. We will also say that a finitely generated, torsion-free R-module X is reflexive if $X = \bigcap_{\mathcal{P}} X_{\mathcal{P}}$, where $\mathcal{P}$ again varies over all the prime ideals of R of height 1 and $X_{\mathcal{P}} = X \otimes_R R_{\mathcal{P}}$ considered as an R- submodule of the $\mathcal{K}$-vector space $X \otimes_R \mathcal{K}$.

We will use the following standard terminology throughout this paper. If A is a discrete R-module, let $X = \widehat{A}$ denote its Pontryagin dual. We say that A is a cofinitely generated R-module if X is finitely generated as an R-module, A is a cotorsion R-module if X is a torsion R-module, and A is a cofree R-module if X is a free R-module. We define $\mathrm{corank}_R(A)$ to be $\mathrm{rank}_R(X)$. Similar terminology will be used for Λ-modules. Although it is not so standard, we will say that A is coreflexive if X is reflexive, either as an R-module or as a Λ-module, and that A is co-pseudo-null if X is pseudo-null. For most of these terms, it doesn't matter whether the ring is Λ or a finite, integral extension R of Λ. For example, as we will show in section 2, A is a coreflexive R-module if and only if it is a coreflexive Λ-module. A similar statement is true for co-pseudo-null modules. However, the module $\mathcal{D}$ defined above for a representation ρ is a cofree R-module and a coreflexive, but not necessarily cofree, Λ-module, assuming that R is a reflexive domain.

Assume that X is a torsion-free R-module. Then, if r is any nonzero element of R, multiplication by r defines an injective map $X \to X$. The corresponding map on the Pontryagin dual is then surjective. Thus, $A = \widehat{X}$ will be a divisible R-module. Conversely, if A is a divisible R-module, then X is torsion-free. If R is a finite, integral extension of Λ, then A is divisible as an R-module if and only if A is divisible as a Λ-module. The kernel of multiplication by an element $r \in R$ will be denoted by $A[r]$. More generally, if I is any ideal of R or Λ, we let $A[I] = \{a \in A \mid ia = 0 \text{ for all } i \in I\}$.

Suppose v is a prime of K. Let $\overline{K}, \overline{K}_v$ denote algebraic closures of the indicated fields and let $\mathrm{G}_K = \mathrm{Gal}(\overline{K}/K)$, $\mathrm{G}_{K_v} = \mathrm{Gal}(\overline{K}_v/K_v)$. We can fix an embedding $\overline{K} \to \overline{K}_v$ and this induces continuous homomorphisms $\mathrm{G}_{K_v} \to \mathrm{G}_K \to \mathrm{Gal}(K_\Sigma/K)$. Thus, we get a continuous R-linear action of G_{K_v} on $\mathcal{T}$ and on $\mathcal{D}$. Define $\mathcal{T}^* = \mathrm{Hom}(\mathcal{D}, \mu_{p^\infty})$, where μ_{p^∞} denotes the group of p-power roots of unity. Note that $\mathcal{T}^*$ is a free R-module of rank n. Choosing a basis, the natural action of $\mathrm{Gal}(K_\Sigma/K)$ on $\mathcal{T}^*$ is given by a continuous homomorphism $\rho^* : \mathrm{Gal}(K_\Sigma/K) \longrightarrow GL_n(R)$. Consider the action of G_{K_v} on $\mathcal{T}^*$. The set of G_{K_v}-invariant elements $(\mathcal{T}^*)^{\mathrm{G}_{K_v}} = \mathrm{Hom}_{\mathrm{G}_{K_v}}(\mathcal{D}, \mu_{p^\infty})$ is an R-submodule. The following theorem is the main result of this paper.

Theorem 1. *Suppose that R is a reflexive domain. Suppose also that $\mathcal{T}^*$ satisfies the following two local assumptions:*

(a) For every prime $v \in \Sigma$, the R-module $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is reflexive.

(b) There is at least one non-archimedean prime $v_o \in \Sigma$ such that $(\mathcal{T}^*)^{G_{K_{v_o}}} = 0$.

Then $Ш^2(K, \Sigma, \mathcal{D})$ is a coreflexive R-module. If $Ш^2(K, \Sigma, \mathcal{D}) = 0$, then the Pontryagin dual of $H^1(K_\Sigma/K, \mathcal{D})$ has no nonzero, pseudo-null R-submodules.

The proof of this theorem will be given in section 6, but some comments about the role of various assumptions may be helpful here. The assumption that R is a domain is not essential. It suffices to just assume that R contains a formal power series ring Λ over either $\mathbb{Z}_p$ or $\mathbb{F}_p$ and that R is a finitely generated, reflexive module over Λ. Then $\mathcal{D}$ will be a coreflexive Λ-module. In fact, it is precisely that assumption which is needed in the argument. In particular, it implies that if π is an irreducible element of Λ, then $\mathcal{D}[\pi]$ is a divisible module over the ring $\Lambda/(\pi)$. Coreflexive Λ-modules are characterized by that property. (See corollary 2.6.1.) The assertion that $Ш^2(K, \Sigma, \mathcal{D})$ is also a coreflexive Λ-module implies that it is Λ-divisible, but is actually a much stronger statement. Reflexive Λ-modules are a rather small subclass of the class of torsion-free Λ-modules.

The conclusion in theorem 1 concerning $H^1(K_\Sigma/K, \mathcal{D})$ can be expressed in another way which seems quite natural. It suffices to consider it just as a Λ-module. The ring Λ is a UFD and so we can say that two nonzero elements of Λ are relatively prime if they have no irreducible factor in common. We make the following definition.

Definition. *Assume that A is a discrete Λ-module. We say that A is an "almost divisible" Λ-module if there exists a nonzero element $\theta \in \Lambda$ with the* *following property: If $\lambda \in \Lambda$ is a nonzero element relatively prime to θ, then $\lambda A = A$.*

If A is a cofinitely generated Λ-module, then it is not hard to see that A is an almost divisible Λ-module if and only if the Pontryagin dual of A has no nonzero pseudo-null Λ-submodules. (See proposition 2.4.) Under the latter condition, one could take θ to be any nonzero annihilator of the torsion Λ-submodule Y of $X = \widehat{A}$, e.g., a generator of the characteristic ideal of Y. Thus, theorem 1 asserts that, under certain assumptions, the Λ-module $H^1(K_\Sigma/K, \mathcal{D})$ is almost divisible.

The main local ingredient in the proof is to show that $H^1(K_v, \mathcal{D})$ is an almost divisible Λ-module for all $v \in \Sigma$. Assumption *(a)* guarantees this. In fact, it is sufficient to assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is reflexive as a Λ-module for all $v \in \Sigma$. This implies that the map $H^2(K_v, \mathcal{D}[P]) \longrightarrow H^2(K_v, \mathcal{D})$ is injective for all but a finite number of prime ideals P in Λ of height 1; the almost divisibility of $H^1(K_v, \mathcal{D})$ follows from that. The hypothesis that $Ш^2(K, \Sigma, \mathcal{D}) = 0$ then allows us to deduce that the map $H^2(K_\Sigma/K, \mathcal{D}[P]) \longrightarrow H^2(K_\Sigma/K, \mathcal{D})$ is injective for all but finitely many such P's, which implies the almost divisibility of $H^1(K_\Sigma/K, \mathcal{D})$.

Both assumptions *(a)* and *(b)* are used in the proof that $Ш^2(K, \Sigma, \mathcal{D})$ is a coreflexive Λ-module. Assumption *(b)* obviously implies that $(\mathcal{T}^*)^{\mathrm{Gal}(K_\Sigma/K)}$ vanishes. That fact, in turn, implies that the global-to-local map defining $Ш^2(K, \Sigma, \mathcal{D})$ is surjective. Such a surjectivity statement plays an important role in our proof of theorem 1. We will discuss the validity of the local assumptions at the end of section 5. Local assumption *(a)* is easily verified for archimedean primes if p is odd, but is actually not needed in that case. It is needed when $p = 2$ and, unfortunately, could then fail to be satisfied. For non-archimedean primes, the local assumptions are often satisfied simply because $(\mathcal{T}^*)^{G_{K_v}} = 0$ for *all* such $v \in \Sigma$. However, there are interesting examples where this fails to be true for at least some v's in Σ and so it is too restrictive to make that assumption.

The hypothesis that $Ш^2(K, \Sigma, \mathcal{D}) = 0$ is quite interesting in itself. Under the assumptions in theorem 1, $Ш^2(K, \Sigma, \mathcal{D})$ will be coreflexive, and hence divisible, as an R-module. Therefore, the statement that $Ш^2(K, \Sigma, \mathcal{D}) = 0$ would then be equivalent to the seemingly weaker statement that $\mathrm{corank}_R\big(Ш^2(K, \Sigma, \mathcal{D})\big) = 0$. Just for convenience, we will give a name to that statement.

Hypothesis L: *$Ш^2(K, \Sigma, \mathcal{D})$ is a cotorsion R-module.*

Of course, it is only under certain assumptions that this statement implies that $Ш^2(K, \Sigma, \mathcal{D})$ actually vanishes. We will now describe two equivalent formulations of hypothesis L which are more easily verified in practice. To state the first one, let $\mathcal{D}^* = \mathcal{T}^* \otimes_R \widehat{R}$. Then we will show that

$$\mathrm{corank}_R\big(\text{Ш}^2(K,\Sigma,\mathcal{D})\big) = \mathrm{corank}_R\big(\text{Ш}^1(K,\Sigma,\mathcal{D}^*)\big) \tag{1}$$

This will be proposition 4.4. Thus, one reformulation of hypothesis L is the assertion that $\text{Ш}^1(K,\Sigma,\mathcal{D}^*)$ is a cotorsion R-module. This formulation has the advantage that it is easier to study H^1 and hence Ш^1. We should mention that even under strong hypotheses like those in theorem 1, it is quite possible for $\text{Ш}^1(K,\Sigma,\mathcal{D}^*)$ to be a nonzero, cotorsion R-module.

A second equivalent formulation can be given in terms of the R-corank of $H^1(K_\Sigma/K,\mathcal{D})$. As we mentioned before, we will derive a lower bound on this corank by using theorems of Tate. Those theorems concern finite Galois modules, but can be extended to Galois modules such as $\mathcal{D}$ in a straightforward way. The precise statement is given in proposition 4.3. It is derived partly from a formula for the Euler-Poincaré characteristic. For $i \geq 0$, we let $h_i = \mathrm{corank}_R\big(H^i(K_\Sigma/K,\mathcal{D})\big)$. Let r_2 denote the number of complex primes of K. For each real prime v of K, let $n_v^- = \mathrm{corank}_R\big(\mathcal{D}/\mathcal{D}^{G_{K_v}}\big)$. Then

$$h_1 = h_0 + h_2 + \delta.$$

where $\delta = r_2 n + \sum_{v \text{ real}} n_v^-$. The Euler-Poincaré characteristic $h_0 - h_1 + h_2$ is equal to $-\delta$. Thus, h_1 is essentially determined by h_0 and h_2 since the quantity δ is usually easy to evaluate. On the other hand, one gets a lower bound on h_2 by studying the global-to-local map

$$\gamma : H^2(K_\Sigma/K,\mathcal{D}) \longrightarrow P^2(K,\Sigma,\mathcal{D}),$$

where $P^2(K,\Sigma,\mathcal{D}) = \prod_{v\in\Sigma} H^2(K_v,\mathcal{D})$. The cokernel of γ is determined by Tate's theorems: $\mathrm{coker}(\gamma) \cong H^0(K_\Sigma/K,\mathcal{T}^*)^\wedge$. Thus, one can obtain a certain lower bound for h_2 and hence for h_1. In proposition 4.3, we give this lower bound in terms of the ranks or coranks of various H^0's. The assertion that h_1 is equal to this lower bound is equivalent to the assertion that $\ker(\gamma)$ has R-corank 0, which is indeed equivalent to hypothesis L.

The local duality theorem of Poitou and Tate asserts that the Pontryagin dual of $H^2(K_v,\mathcal{D})$ is isomorphic to $H^0(K_v,\mathcal{T}^*) = (\mathcal{T}^*)^{G_{K_v}}$. Thus, if we assume that $(\mathcal{T}^*)^{G_{K_v}} = 0$ for all non-archimedean $v \in \Sigma$, then $H^2(K_v,\mathcal{D}) = 0$ for all such v. If we also assume that p is odd, then obviously $H^2(K_v,\mathcal{D}) = 0$ for all archimedean v. Under these assumptions, $P^2(K,\Sigma,\mathcal{D}) = 0$ and Hypothesis L would then be equivalent to the assertion that $H^2(K_\Sigma/K,\mathcal{D}) = 0$.

The validity of Hypothesis L seems to be a very subtle question. We will discuss this at the end of section 6. It can fail to be satisfied if R has Krull dimension 1. If R has characteristic 0, then, apart from simple counterexamples constructed by extension of scalars, it is not at all clear what one should expect when the Krull dimension is greater than 1. However, one can construct nontrivial counterexamples where R has arbitrarily large Krull dimension and R has characteristic p.

Theorem 1 has a number of interesting consequences in classical Iwasawa theory. These will be the subject of a subsequent paper. We will just give an outline of some of them here. In fact, our original motivation for this work was to improve certain results in our earlier paper [Gr89]. There we considered the cyclotomic $\mathbb{Z}_p$-extension K_∞ of a number field K and a discrete $\mathrm{Gal}(K_\Sigma/K)$-module D isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ as a $\mathbb{Z}_p$-module. We obtain such a Galois module from a vector space V of dimension n over $\mathbb{Q}_p$ which has a continuous $\mathbb{Q}_p$-linear action of $\mathrm{Gal}(K_\Sigma/K)$. Let T be a Galois-invariant $\mathbb{Z}_p$-lattice in V and let $D = V/T$. The Galois action defines a representation $\rho_o : \mathrm{Gal}(K_\Sigma/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(T) \cong GL_n(\mathbb{Z}_p)$. Since only primes of K lying above p can ramify in K_∞/K, we have $K_\infty \subset K_\Sigma$. One therefore has a natural action of $\Gamma = \mathrm{Gal}(K_\infty/K)$ on the Galois cohomology groups $H^i(K_\Sigma/K_\infty, D)$ for any $i \geq 0$. Now $H^i(K_\Sigma/K_\infty, D)$ is also a $\mathbb{Z}_p$-module. One can then regard $H^i(K_\Sigma/K_\infty, D)$ as a discrete Λ-module, where $\Lambda = \mathbb{Z}_p[[\Gamma]]$, the completed $\mathbb{Z}_p$-group algebra for Γ. The ring Λ is isomorphic to the formal power series ring $\mathbb{Z}_p[[T]]$ in one variable and is a complete Noetherian local domain of Krull dimension 2. The modules $H^i(K_\Sigma/K_\infty, D)$ are cofinitely generated over Λ.

Propositions 4 and 5 in [Gr89] assert that if p is an odd prime, then $H^2(K_\Sigma/K_\infty, D)$ is a cofree Λ-module, and if $H^2(K_\Sigma/K_\infty, D) = 0$, then the Pontryagin dual of $H^1(K_\Sigma/K_\infty, D)$ contains no nonzero, finite Λ-modules. One consequence of theorem 1 is the following significantly more general result. We allow p to be *any* prime and K_∞/K to be *any* Galois extension such that $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p^m$ for some $m \geq 1$. For any $i \geq 0$, we define $\text{Ш}^i(K_\infty, \Sigma, D)$ to be the subgroup of $H^i(K_\Sigma/K_\infty, D)$ consisting of cocycle classes which are locally trivial at all primes of K_∞ lying above the primes in Σ. Again, Γ acts continuously on those Galois cohomology groups and so we can regard them as modules over the ring $\Lambda = \mathbb{Z}_p[[\Gamma]]$. This ring is now isomorphic to the formal power series ring $\mathbb{Z}_p[[T_1, ..., T_m]]$ in m variables and has Krull dimension $d = m + 1$. The group $\text{Ш}^i(K_\infty, \Sigma, D)$ is a Λ-submodule of $H^i(K_\Sigma/K_\infty, D)$. All of these Λ-modules are cofinitely generated.

Theorem 2. *Suppose that K_∞/K is a $\mathbb{Z}_p^m$-extension, where $m \geq 1$ and p is a prime. Then $\text{Ш}^2(K_\infty, \Sigma, D)$ is a coreflexive Λ-module. If $\text{Ш}^2(K_\infty, \Sigma, D)$ vanishes, then the Pontryagin dual of $H^1(K_\Sigma/K_\infty, D)$ has no nonzero, pseudo-null Λ-submodules.*

The results proved in [Gr89] which were mentioned above concern the case where K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K. For odd p, one then has $\text{Ш}^2(K_\infty, \Sigma, D) = H^2(K_\Sigma/K_\infty, D)$. The assertion about cofreeness follows since $m = 1$ and so a cofinitely generated Λ-module A is coreflexive if and only if it is cofree. (See remark 2.6.2.) Also, A is co-pseudo-null if and only if it is finite. In that special case, theorem 2 is more general only because it includes $p = 2$.

The relationship to theorem 1 is based on a version of Shapiro's lemma which relates the above cohomology groups to those associated with a suitably defined

$\mathrm{Gal}(K_\Sigma/K)$-module $\mathcal{D}$. We can regard Γ as a subgroup of the multiplicative group $\Lambda^\times$ of Λ. This gives a homomorphism $\Gamma \to GL_1(\Lambda)$. and hence a representation over Λ of $\mathrm{Gal}(K_\Sigma/K)$ of rank 1 factoring through Γ. We will denote this representation by κ. Define $\mathcal{T} = T \otimes_{\mathbb{Z}_p} \Lambda$. Thus, $\mathcal{T}$ is a free Λ-module of rank n. We let $\mathrm{Gal}(K_\Sigma/K)$ act on $\mathcal{T}$ by $\rho = \rho_o \otimes \kappa^{-1}$. We then define, as before, $\mathcal{D} = \mathcal{T} \otimes_\Lambda \widehat{\Lambda}$, which is a cofree Λ-module with a Λ-linear action of $\mathrm{Gal}(K_\Sigma/K)$. The Galois action is through the first factor $\mathcal{T}$. We will say that $\mathcal{D}$ is induced from D via the $\mathbb{Z}_p^m$-extension K_∞/K. Sometimes we will use the notation: $\mathcal{D} = \mathrm{Ind}_{K_\infty/K}(D)$. Of course, the ring R is now Λ which is certainly a reflexive domain. We have the following comparison theorem.

Theorem 3. *For $i \geq 0$, $H^i(K_\Sigma/K, \mathcal{D}) \cong H^i(K_\Sigma/K_\infty, D)$ as Λ-modules.*

There is a similar comparison theorem for the local Galois cohomology groups which is compatible with the isomorphism in theorem 3 and so, for any $i \geq 0$, one obtains an isomorphism

$$Ш^i(K, \Sigma, \mathcal{D}) \cong Ш^i(K_\infty, \Sigma, D) \tag{2}$$

as Λ-modules. In particular, one can deduce from (1) and (2) that $Ш^2(K_\infty, \Sigma, D)$ has the same Λ-corank as $Ш^1(K_\infty, \Sigma, D^*)$, where D^* denotes $\mathrm{Hom}(T, \mu_{p^\infty})$.

Both of the local assumptions in theorem 1 turn out to be automatically satisfied for $\mathcal{D}$ and so theorem 2 is indeed a consequence of theorem 1. The verification of those assumptions is rather straightforward. The most subtle point is the consideration of primes that split completely in K_∞/K, including the archimedean primes of K if $p = 2$. For any v which does not split completely, one sees easily that $(\mathcal{T}^*)^{G_{K_v}} = 0$. Thus, hypothesis *(b)* is satisfied since at least one of the primes of K lying over p must be ramified in K_∞/K; one could take v_o to be one of those primes. If v does split completely, then one shows that $(\mathcal{T}^*)^{G_{K_v}}$ is a direct summand in the free Λ-module $\mathcal{T}^*$. This implies that the corresponding quotient, the complementary direct summand, is also a free Λ-module and hence reflexive.

As a consequence, we can say that $Ш^2(K_\infty, \Sigma, D)$ is a coreflexive Λ-module. We believe that it is reasonable to make the following conjecture.

Conjecture L. *Suppose that K_∞ is an arbitrary $\mathbb{Z}_p^m$-extension of a number field K, Σ is any finite set of primes of K containing the primes lying above p and ∞, and D is a $\mathrm{Gal}(K_\Sigma/K)$-module which is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ as a group for some $n \geq 1$. Then $Ш^2(K_\infty, \Sigma, D) = 0$.*

That is, hypothesis L should hold for $\mathcal{D} = \mathrm{Ind}_{K_\infty/K}(D)$. Equivalently, $Ш^1(K_\infty, \Sigma, D^*)$ should be a cotorsion Λ-module. Furthermore, it turns out that the global-to-local map γ is now actually surjective. The Λ-module $P^2(K, \Sigma, \mathcal{D})$ can, in general, be nonzero and even have positive Λ-corank. To be precise, only primes v of K which split completely in K_∞/K can make a nonzero contribution to $P^2(K, \Sigma, \mathcal{D})$. The contribution to the Λ-corank can only come from the non-archimedean primes. If v is a non-archimedean prime of K which splits completely in K_∞/K, then we have

$$\operatorname{corank}_\Lambda\big(H^2(K_v, \mathcal{D})\big) = \operatorname{corank}_{\mathbb{Z}_p}\big(H^2(K_v, D)\big)$$

and this can be positive.

As an illustration, consider the special case where $D = \mu_{p^\infty}$. In this case, $D^* = \mathbb{Q}_p/\mathbb{Z}_p$ (with trivial Galois action). One then has the following concrete description of $\text{Ш}^1(K_\infty, \Sigma, D^*)$. Let L_∞ denote the maximal, abelian, pro-p-extension of K_∞ which is unramified at all primes. Let $L_\infty^{'}$ be the subfield in which all primes of K_∞ split completely. Then we have

$$\text{Ш}^1(K_\infty, \Sigma, \mathbb{Q}_p/\mathbb{Z}_p) = \operatorname{Hom}\big(\operatorname{Gal}(L_\infty^{'}/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)\big)$$

It is known that $\operatorname{Gal}(L_\infty/K_\infty)$ is a finitely generated, torsion Λ-module. (This is a theorem of Iwasawa if $m = 1$ and is proved in [Gr73] for arbitrary m.) Hence the same thing is true for the quotient Λ-module $\operatorname{Gal}(L_\infty^{'}/K_\infty)$. Therefore, $\text{Ш}^1(K_\infty, \Sigma, \mathbb{Q}_p/\mathbb{Z}_p)$ is indeed Λ-cotorsion. Thus, conjecture L is valid for $D = \mu_{p^\infty}$ for an arbitrary $\mathbb{Z}_p^m$-extension K_∞/K. Note also that $\operatorname{corank}_{\mathbb{Z}_p}\big(H^2(K_v, \mu_{p^\infty})\big) = 1$ for any non-archimedean prime v. Hence, if Σ contains non-archimedean primes which split completely in K_∞/K, then $H^2(K_\Sigma/K_\infty, \mu_{p^\infty})$ will have a positive Λ-corank. Since $\text{Ш}^2(K_\infty, \Sigma, \mu_{p^\infty}) = 0$, as just explained, it follows that $\operatorname{corank}_\Lambda\big(H^2(K_\Sigma/K_\infty, \mu_{p^\infty})\big)$ is precisely the number of such primes, i.e., the cardinality of Υ. Therefore, the Λ-corank of $H^1(K_\Sigma/K_\infty, \mu_{p^\infty})$ will be equal to $r_1 + r_2 + |\Upsilon|$. Non-archimedean primes that split completely in a $\mathbb{Z}_p^m$-extension can exist. For example, let K be an imaginary quadratic field and let K_∞ denote the so-called "anti-cyclotomic" $\mathbb{Z}_p$-extension of K. Thus, K_∞ is a Galois extension of $\mathbb{Q}$ and $\operatorname{Gal}(K_\infty/\mathbb{Q})$ is a dihedral group. One sees easily that if v is any prime of K not lying over p which is inert in $K/\mathbb{Q}$, then v splits completely in K_∞/K.

As a second illustration, consider the Galois module $D = \mathbb{Q}_p/\mathbb{Z}_p$ with a trivial action of $\operatorname{Gal}(K_\Sigma/K)$. For an arbitrary $\mathbb{Z}_p^m$-extension K_∞/K, it is not hard to see that $\text{Ш}^2(K_\infty, \Sigma, D) = H^2(K_\Sigma/K_\infty, D)$. This is so because $H^2(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ for all primes v of K. Let M_∞^Σ denote the maximal abelian pro-p-extension of K_∞ contained in K_Σ. Then $H^1(K_\Sigma/K_\infty, D) = \operatorname{Hom}\big(\operatorname{Gal}(M_\infty^\Sigma/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p\big)$, which is just the Pontryagin dual of $\operatorname{Gal}(M_\infty^\Sigma/K_\infty)$. In this case, $n = 1$ and $n_v^- = 0$ for all real primes. Conjecture L is therefore equivalent to the statement that the Λ-module $\operatorname{Gal}(M_\infty^\Sigma/K_\infty)$ has rank r_2. Theorem 3 together with other remarks we have made has the following consequence.

Theorem 4. *Let p be a prime. Suppose that K_∞/K is any $\mathbb{Z}_p^m$-extension, where $m \geq 1$. Then $\operatorname{Gal}(M_\infty^\Sigma/K_\infty)$ is a finitely generated Λ-module and $\operatorname{rank}_\Lambda\big(\operatorname{Gal}(M_\infty^\Sigma/K_\infty)\big) \geq r_2$. If $\operatorname{rank}_\Lambda\big(\operatorname{Gal}(M_\infty^\Sigma/K_\infty)\big) = r_2$, then $\operatorname{Gal}(M_\infty^\Sigma/K_\infty)$ has no nonzero pseudo-null Λ-submodules.*

Let M_∞ denote the maximal abelian pro-p-extension of K_∞ which is unramified at all primes of K_∞ not lying above p or ∞. One can show that $\mathrm{Gal}(M_\infty^\Sigma/M_\infty)$ is a torsion Λ-module and so the equality in the above theorem is equivalent to the assertion that the Λ-rank of $\mathrm{Gal}(M_\infty/K_\infty)$ is equal to r_2. Note that $M_\infty = M_\infty^\Sigma$ if one takes $\Sigma = \{v \mid v|p \text{ or } v|\infty\}$. In that case, the above theorem is proved in [NQD]. A somewhat different, but closely related, result is proved in [Gr78]. Theorem 1 can be viewed as a rather broad generalization of these results in classical Iwasawa theory.

The statement that $\mathrm{corank}_\Lambda\big(\mathrm{Gal}(M_\infty/K_\infty)\big) = r_2$ is known as the *Weak Leopoldt Conjecture for K_∞/K*. That name arises from the fact that if one considers a $\mathbb{Z}_p$-extension K_∞/K and the Galois module $D = \mathbb{Q}_p/\mathbb{Z}_p$, the conjecture is equivalent to the following assertion:

Let K_n denote the n-th layer in the $\mathbb{Z}_p$-extension K_∞/K. Let M_n be the compositum of all $\mathbb{Z}_p$-extensions of K_n. Let $\delta_n = \mathrm{rank}_{\mathbb{Z}_p}\big(\mathrm{Gal}(M_n/K_n)\big) - r_2p^n$. Then δ_n is bounded as $n \to \infty$.

The well-known conjecture of Leopoldt would assert that $\delta_n = 1$ for all n.

If a $\mathbb{Z}_p^m$-extension K_∞ of K contains μ_{p^∞}, then the Galois modules μ_{p^∞} and $\mathbb{Q}_p/\mathbb{Z}_p$ are isomorphic over K_∞. Since conjecture L is valid for $D = \mu_{p^\infty}$, it is then also valid for $D = \mathbb{Q}_p/\mathbb{Z}_p$. One deduces easily that conjecture L is valid for $D = \mathbb{Q}_p/\mathbb{Z}_p$ if one just assumes that K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension of K. Thus, under that assumption, it follows unconditionally that $\mathrm{Gal}(M_\infty^\Sigma/K_\infty)$ has no nonzero pseudo-null Λ-submodules. If K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K, then this result was originally proved by Iwasawa. It is theorem 18 in [Iw73]. He showed that that Galois group indeed has Λ-rank r_2 and deduced the non-existence of finite Λ-submodules from that.

There is a long history behind the topics discussed in this article. We have already mentioned Iwasawa's theorem in [Iw73]. A similar, but less general, result is proved in his much earlier paper [Iw59]. There he assumes a special case of Leopoldt's conjecture. Those theorems of Iwasawa were generalized in [Gr78], [NQD], and [Pe84] for similarly-defined Galois groups over $\mathbb{Z}_p^m$-extensions of a number field. The generalization to Galois cohomology groups for arbitrary Galois modules of the form $D = V/T$ has also been considered by several authors, e.g., see [Sch], [Gr89], and [J]. The conjecture concerning the possible vanishing of $H^2(K_\Sigma/K_\infty, D)$, and its relevance to the question of finite submodules, can be found in those references. Perrin-Riou has a substantial discussion of these issues in [Pe95], Appendice B, referring to that conjecture as the *Conjecture de Leopoldt faible* because it generalizes the assertion of the same name mentioned before. We also want to mention that the idea of proving the non-existence of nonzero pseudo-null submodules under an assumption like hypothesis L was inspired by the thesis of McConnell [McC].

Considerable progress has been made in one important special case, namely $D = E[p^\infty]$, where E is an elliptic curve defined over $\mathbb{Q}$. If one takes K_∞ to be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, where p is an odd prime, then conjecture L was verified in [C-M] under certain hypotheses. This case is now settled completely; a theorem of Kato asserts that $H^2(K_\Sigma/K_\infty, E[p^\infty]) = 0$ if K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K, $K/\mathbb{Q}$ is assumed to be abelian and p is assumed to be odd. Kato's theorem applies more generally when $D = V/T$ and V is the p-adic representation associated to a cuspform.

More recently, similar types of questions have been studied when K_∞/K is a p-adic Lie extension. The ring Λ is then non-commutative. Nevertheless, Venjakob has defined the notion of pseudo-nullity and proved the non-existence of nonzero pseudo-null submodules in certain Galois groups. We refer the readers to [Ve] for a discussion of this situation. In [C-S], Coates and Sujatha study the group $\text{Ш}^1(K_\infty, \Sigma, E[p^\infty])$, where E is an elliptic curve defined over K. Those authors refer to this group as the *"fine Selmer group"* for E over K_∞ and conjecture that it is actually a co-pseudo-null Λ-module under certain assumptions.

Another topic which we intend to study in a future paper concerns the structure of a Selmer group $\mathrm{Sel}_{\mathcal{D}}(K)$ which can be attached to the representation ρ under certain assumptions. This Selmer group will be an R-submodule of $H^1(K_\Sigma/K, \mathcal{D})$ defined by imposing certain local conditions on the cocycles. Theorem 1 can then be effectively used to prove that the Pontryagin dual of $\mathrm{Sel}_{\mathcal{D}}(K)$ has no nonzero pseudo-null R-submodules under various sets of assumptions. One crucial assumption will be that $\mathrm{Sel}_{\mathcal{D}}(K)$ is a cotorsion R-module. Such a theorem is useful in that one can then study how the Selmer group behaves under specialization, i.e., reducing the representation ρ modulo a prime ideal $\mathcal{P}$ of R.

The study of Iwasawa theory in the context of a representation ρ was initiated in [Gr94]. More recently, Nekovar has taken a rather innovative point of view towards studying *large* representations and the associated cohomology and Selmer groups, introducing his idea of Selmer complexes [Nek]. It may be possible to give nice proofs of some of the theorems in this paper from such a point of view. In section 9.3 of his article, Nekovar does give such proofs in the context of classical Iwasawa theory. (See his proposition 9.3.1, corollary 9.3.2 and propositions 9.3.6, 9.3.7.)

This research was partially support by grants from the National Science Foundation. Part of this research was carried out during two visits to the Institut des Hautes Études Scientifiques. The author is gratefully to IHÉS for their support and hospitality during those visits. The author also wishes to take this opportunity to thank John Coates for numerous valuable and stimulating discussions over the years. They have been influential on many aspects of the author's research, including the topic of this paper.

2 Some Module Theory.

Theorem 1 and some of the other theorems mentioned in the introduction concern modules over a complete Noetherian local domain R. This section will include a variety of module-theoretic results that will be useful in the proofs. In particular, we will point out that several properties, such as pseudo-nullity or reflexivity, can be studied by simply considering the modules as Λ-modules. The main advantage of doing so is that Λ is a regular local ring and so has the following helpful property: *Every prime ideal of Λ of height 1 is principal.* This is useful in proofs by induction on the Krull dimension. Such arguments would work for any regular, Noetherian local ring. It seems worthwhile to state and prove various results in greater generality than we really need. However, in some cases, we haven't determined how general the theorems can be.

We will use the notation $\mathrm{Spec}_{ht=1}(R)$ to denote the set of prime ideals of height 1 in a ring R. The terminology *"almost all"* means *all but finitely many.* If I is any ideal of R, we will let $V(I)$ denote the set of prime ideals of R containing I.

A. Behavior of ranks and coranks under specialization. Consider a finitely generated module X over an integral domain R. If $\mathcal{K}$ is the fraction field of R, then $\mathrm{rank}_R(X) = \dim_{\mathcal{K}}(X \otimes_R \mathcal{K})$. The following result holds:

Proposition 2.1. *Let $r = \mathrm{rank}_R(X)$. Then $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) \geq r$ for every prime ideal $\mathcal{P}$ of R. There exists a nonzero ideal I of R such that $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) > r$ if and only if $\mathcal{P} \in V(I)$. In particular, $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = r$ for all but finitely many prime ideals $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$.*

Proof. We prove a somewhat more general result by a linear algebra argument. Suppose that $s \geq r$. We will show that there is an ideal I_s with the property:

$$\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) > s \iff \mathcal{P} \in V(I_s)$$

The ideal I_s will be a Fitting ideal. Suppose that X has g generators as an R-module. Thus X is a quotient of the free R-module $F = R^g$. Therefore, one has an exact sequence of R-modules

$$R^h \xrightarrow{\phi} R^g \xrightarrow{\psi} X \longrightarrow 0$$

The map ϕ is multiplication by a certain $g \times h$ matrix α. Let f denote the rank of the matrix α. The R-rank of the image of ϕ is equal to f and so we have $r = g - f$. By matrix theory, there is at least one $f \times f$-submatrix (obtained by omitting a certain number of rows and/or columns) of the matrix α whose determinant is nonzero, but there is no larger square submatrix with nonzero determinant.

For every prime ideal $\mathcal{P}$ of R, the above exact sequence induces a free presentation of $X/\mathcal{P}X$.

$$(R/\mathcal{P})^h \xrightarrow{\phi_{\mathcal{P}}} (R/\mathcal{P})^g \xrightarrow{\psi_{\mathcal{P}}} X/\mathcal{P}X \longrightarrow 0$$

The second term is $F/\mathcal{P}F$ and exactness at that term follows from the fact that the image of $\mathcal{P}F$ under ψ is $\mathcal{P}X$. The homomorphism $\phi_{\mathcal{P}}$ is multiplication by the matrix $\alpha_{\mathcal{P}}$, the reduction of α modulo $\mathcal{P}$. We have

$$\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = g - \mathrm{rank}(\alpha_{\mathcal{P}}).$$

The description of the rank in terms of the determinants of submatrices shows that $\mathrm{rank}(\alpha_{\mathcal{P}}) \le \mathrm{rank}(\alpha)$ for every prime ideal $\mathcal{P}$ of R. If $g \ge s \ge r$, let $e = g-s$ so that $0 \le e \le f$. Let I_s denote the ideal in R generated by the determinants of all $e \times e$ submatrices of the matrix α. If $e = 0$, then take $I_s = R$. Since $e \le f$, it is clear that I_s is a nonzero ideal. Then $\alpha_{\mathcal{P}}$ has rank $< e$ if and only if $I_s \subseteq \mathcal{P}$. This implies that $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) > g - e = s$ if and only if $I_s \subseteq \mathcal{P}$ as stated. Finally, we recall the simple fact that if I is any nonzero ideal in a Noetherian domain R, then there can exist only finitely many prime ideals of R of height 1 which contain I. ■

Corollary 2.1.1. *Let X_1 and X_2 be finitely generated R-modules. Suppose that $\phi : X_1 \to X_2$ is an R-module homomorphism. Let $r_1 = \mathrm{rank}_R\big(\ker(\phi)\big)$ and $r_2 = \mathrm{rank}_R\big(\mathrm{coker}(\phi)\big)$. For every prime ideal $\mathcal{P}$ of R, let*

$$\phi_{\mathcal{P}} : X_1/\mathcal{P}X_1 \to X_2/\mathcal{P}X_2$$

be the induced map. There exists a nonzero ideal I of R such that

$$\mathrm{rank}_{R/\mathcal{P}}\big(\ker(\phi_{\mathcal{P}})\big) = r_1, \quad \mathrm{rank}_{R/\mathcal{P}}\big(\mathrm{coker}(\phi_{\mathcal{P}})\big) = r_2$$

if $\mathcal{P} \notin V(I)$. These equalities hold for almost all $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$

Proof. Let $X = \mathrm{coker}(\phi) = X_2/\phi(X_1)$. The cokernel of $\phi_{\mathcal{P}}$ is isomorphic $X/\mathcal{P}X$ and so the statement about the cokernels follows from proposition 2.1. Now the $(R/\mathcal{P})$-rank of the kernel of $\phi_{\mathcal{P}}$ is determined by the $(R/\mathcal{P})$-ranks of $X_1/\mathcal{P}X_1$, $X_2/\mathcal{P}X_2$, and $\mathrm{coker}(\phi_{\mathcal{P}})$. We can apply proposition 2.1 to X, X_1 and X_2, which gives certain nonzero ideals of R in each case. Take I to be the intersection of those ideals. ■

Remark 2.1.2. Consider the special case where X_1 and X_2 are free R-modules. Then the map ϕ is given by a matrix and the behavior of the ranks of the kernels and cokernels in the above corollary is determined by the rank of the matrix and its reduction modulo $\mathcal{P}$ as in the proof of proposition 2.1. The following consequence will be useful later.

Suppose that X_1 and X_2 are free R-modules. Then for every prime ideal $\mathcal{P}$ of R, we have $\mathrm{rank}_{R/\mathcal{P}}\big(\ker(\phi_{\mathcal{P}})\big) \ge \mathrm{rank}_R\big(\ker(\phi)\big)$.

This can also be easily deduced from the corollary. A similar inequality holds for the cokernels of ϕ and $\phi_{\mathcal{P}}$.

Suppose that R is a complete Noetherian local domain with finite residue field. Then X is compact and its Pontryagin dual $A = \widehat{X}$ is a cofinitely generated, discrete R-module. The Pontryagin dual of $X/\mathcal{P}X$ is $A[\mathcal{P}]$, the set of elements of A annihilated by $\mathcal{P}$. Thus, one has $\mathrm{corank}_{R/\mathcal{P}}(A[\mathcal{P}]) = \mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X)$. If A_1 and A_2 are two cofinitely generated R-modules and $\psi : A_1 \to A_2$ is an R-module homomorphism, then one can define the adjoint map ϕ of ψ, an R-module homomorphism from $X_2 = \widehat{A_2}$ to $X_1 = \widehat{A_1}$. The kernel and cokernel of ψ are dual, respectively, to the cokernel and kernel of ϕ. We will say that A_1 and A_2 are R-isogenous if there exists an R-module homomorphism ψ such that $\ker(\psi)$ and $\mathrm{coker}(\psi)$ are both R-cotorsion. We then refer to ψ as an R-isogeny. It is easy to see that R-isogeny is an equivalence relation on cofinitely generated R-modules.

Remark 2.1.3. The above proposition and corollary can be easily translated into their "dual" versions for discrete, cofinitely generated R-modules. For example,

1. *If $r = \mathrm{corank}_R(A)$, then $\mathrm{corank}_{R/\mathcal{P}}(A[\mathcal{P}]) \geq r$ for every prime ideal $\mathcal{P}$ of R. There exists a nonzero ideal I of R with the following property: $\mathrm{corank}_{R/\mathcal{P}}(A[\mathcal{P}]) = r$ if and only if $I \not\subseteq \mathcal{P}$. The equality $\mathrm{corank}_{R/\mathcal{P}}(A[\mathcal{P}]) = r$ holds for almost all $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$.*

2. *Suppose that A_1 and A_2 are cofinitely generated, discrete R-modules and that $\psi : A_1 \to A_2$ is an R-module homomorphism. Let $c_1 = \mathrm{corank}_R\big(\ker(\psi)\big)$ and $c_2 = \mathrm{corank}_R\big(\mathrm{coker}(\psi)\big)$. For every prime ideal $\mathcal{P}$ of R, let $\psi_{\mathcal{P}} : A_1[\mathcal{P}] \to A_2[\mathcal{P}]$ be the induced map. There exists a nonzero ideal I of R such that*

$$\mathrm{corank}_{R/\mathcal{P}}\big(\ker(\psi_{\mathcal{P}})\big) = c_1, \quad \mathrm{corank}_{R/\mathcal{P}}\big(\mathrm{coker}(\psi_{\mathcal{P}})\big) = c_2$$

if $\mathcal{P} \notin V(I)$. In particular, if ψ is an R-isogeny, then $\psi_{\mathcal{P}}$ is an $(R/\mathcal{P})$-isogeny if $\mathcal{P} \notin V(I)$.

Remark 2.1.2 can also be translated to the discrete version and asserts that if the above A_1 and A_2 are cofree R-modules, then

$$\mathrm{corank}_{R/\mathcal{P}}\big(\ker(\psi_{\mathcal{P}})\big) \geq c_1, \quad \mathrm{corank}_{R/\mathcal{P}}\big(\mathrm{coker}(\psi_{\mathcal{P}})\big) \geq c_2$$

for every prime ideal $\mathcal{P}$ of R.

Remark 2.1.4. As mentioned before, if I is a nonzero ideal in a Noetherian domain R, then there exist only finitely many prime ideals $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$ which contain I. This is only important if R has infinitely many prime ideals of height 1. Suppose that R is a finite, integral extension of a formal power series ring Λ, as we usually consider in this article. Then if the Krull dimension of R is at least 2, the set of prime ideals of R of height 1 is indeed infinite. This follows from the corresponding fact for the ring Λ which will have the same Krull dimension. In fact, if $\mathcal{Q}$ is any prime ideal of R of height at least 2, then $\mathcal{Q}$ contains infinitely many prime ideals of R of height 1. Corollary 2.5.1 provides a useful strengthening of this fact when $R = \Lambda$. It will also be useful to point out that in the ring Λ, assuming its Krull dimension d is at least 2, there exist infinitely many prime ideals P of height 1 with the property that Λ/P is also a formal power series ring. The Krull dimension of Λ/P will be $d-1$.

The ideal I occurring in proposition 2.1 is not unique. In the special case where X is a torsion R-module, so that $r=0$, one can take $I = \mathrm{Ann}_R(X)$. That is:

Proposition 2.2. *Suppose that X is a finitely generated, torsion R-module and that $\mathcal{P}$ is a prime ideal of R. Then* $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) > 0$ *if and only if* $\mathrm{Ann}_R(X) \subseteq \mathcal{P}$.

Proof. This follows by a simple localization argument. Let $R_\mathcal{P}$ denote the localization of R at $\mathcal{P}$. Then $\mathcal{M} = \mathcal{P}R_\mathcal{P}$ is the maximal ideal of $R_\mathcal{P}$. Let k denote the residue field $R_\mathcal{P}/\mathcal{M}$. Let $X_\mathcal{P} = X \otimes_R R_\mathcal{P}$, the localization of X at $\mathcal{P}$. Then $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = \dim_k(X_\mathcal{P}/\mathcal{M}X_\mathcal{P})$. Furthermore, we have

$$\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = 0 \Longleftrightarrow X_\mathcal{P} = \mathcal{M}X_\mathcal{P} \Longleftrightarrow X_\mathcal{P} = 0,$$

the last equivalence following from Nakayama's Lemma. Finally, $X_\mathcal{P} = 0$ if and only if $\mathrm{Ann}_R(X) \not\subseteq \mathcal{P}$. ■

Remark 2.2.1. Proposition 2.2 can be easily restated in terms of the discrete, cofinitely generated, cotorsion R-module $A = \widehat{X}$. Note that the annihilator ideals in R for A and for X are the same. As we will discuss below, the height of the prime ideals $\mathcal{P}$ for which $A[\mathcal{P}]$ fails to be $(R/\mathcal{P})$-cotorsion is of some significance, especially whether or not such prime ideals can have height 1.

A contrasting situation occurs when X is a torsion-free R-module. We then have the following simple result.

Proposition 2.3. *Assume that X is a finitely generated, torsion-free R-module and that $\mathcal{P}$ is a prime ideal of R of height 1 which is also a principal ideal. Then* $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = \mathrm{rank}_R(X)$. *In particular, if R is a regular local ring, then* $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = \mathrm{rank}_R(X)$ *for all* $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$.

Proof. The assumption about $\mathcal{P}$ implies that the localization $R_\mathcal{P}$ is a discrete valuation ring and hence a principal ideal domain. Therefore $X_\mathcal{P}$ is a free $R_\mathcal{P}$-module of finite rank. Letting $k = R_\mathcal{P}/\mathcal{M}$ again, it is then clear that $\dim_k(X_\mathcal{P}/\mathcal{M}X_\mathcal{P}) = \mathrm{rank}_{R_\mathcal{P}}(X_\mathcal{P})$. The above equality follows from this. ■

If X is a free R-module, then the situation is better. One then has the obvious equality $\mathrm{rank}_{R/\mathcal{P}}(X/\mathcal{P}X) = \mathrm{rank}_R(X)$ for all prime ideals $\mathcal{P}$ of R.

B. Associated prime ideals and pseudo-nullity. Assume that X is a finitely generated, torsion R-module. A prime ideal $\mathcal{P}$ of R is called an associated prime ideal for X if $\mathcal{P} = \mathrm{Ann}_R(x)$ for some nonzero element $x \in X$. Assuming that R is Noetherian, there are only finitely many associated prime ideals for X. We say that X is a *pseudo-null* R-module if no prime ideal of R associated with X has height 1. If R has Krull dimension 1, then every nonzero prime ideal has height 1 and so a pseudo-null R-module must be trivial. If R

is a local ring of Krull dimension 2 and has finite residue field, then X is a pseudo-null R-module if and only if X is finite.

If R is a finite, integral extension of a Noetherian domain Λ, then an R-module X can be viewed as a Λ-module. We say that a prime ideal $\mathcal{P}$ of R lies over a prime ideal P of Λ if $P = \mathcal{P} \cap \Lambda$. The height of $\mathcal{P}$ in R will then be the same as the height of P in Λ. For a given prime ideal P of Λ, there exist only finitely many prime ideals $\mathcal{P}$ lying over P. It is clear that if $\mathcal{P}$ is an associated prime ideal for the R-module X and if $\mathcal{P}$ lies over P, then P is an associated prime ideal for the Λ-module X. Conversely, if P is an associated prime ideal for the Λ-module X, then there exists at least one prime ideal $\mathcal{P}$ of R lying over P which is an associated prime ideal for the R-module X. To see this, consider the R-submodule $Y = X[P]$ which is nonzero. Suppose that the associated prime ideals of R for Y are $\mathcal{P}_1, ..., \mathcal{P}_t$. Let $P_i = \mathcal{P}_i \ cap\Lambda$ for $1 \leq i \leq t$. Thus, each P_i is an associated prime ideal for the Λ-module Y and so $P \subseteq P_i$ for each i. There is some product of the $\mathcal{P}_i$'s which is contained in $\mathrm{Ann}_R(Y)$ and the corresponding product of the P_i's is contained in $\mathrm{Ann}_\Lambda(Y) = P$. Thus, $P_i \subseteq P$ for at least one i. This implies that $P_i = P$ and so, indeed, at least one of the prime ideals $\mathcal{P}_i$ lies over P. These observations justify the following statement:

1. *X is pseudo-null as an R-module if and only if X is pseudo-null as a Λ-module.*

The ring Λ is a UFD. Every prime ideal of height 1 is generated by an irreducible element of Λ. One can give the following alternative definition of pseudo-nullity:

2. *A finitely generated Λ-module X is pseudo-null if and only if $\mathrm{Ann}(X)$ contains two relatively prime elements.*

Another equivalent criterion for pseudo-nullity comes from the following observations. If Q is an associated prime ideal of X, then $X[Q] \neq 0$ and so $X[P] \neq 0$ for every ideal $P \subseteq Q$. If Q has height ≥ 2, then Q contains infinitely many prime ideals P of height 1. On the other hand, if the associated prime ideals for X all have height 1, then $X[P] = 0$ for all the non-associated prime ideals P of height 1. To summarize:

3. *A finitely generated Λ-module X has a nonzero pseudo-null Λ-submodule if and only if there exist infinitely many prime ideals $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ such that $X[P] \neq 0$.*

If $A = \widehat{X}$, then $X[P] \neq 0$ if and only if $PA \neq A$. Hence, the above remarks imply the following result.

Proposition 2.4. *Suppose that A is a cofinitely generated, discrete Λ-module. The following three statements are equivalent:*

(a) $PA = A$ for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$.

(b) The Pontryagin dual of A has no nonzero pseudo-null Λ-submodules.

(c) A is an almost divisible Λ-module.

As mentioned before, if P has height 1, then $P = (\pi)$ where π is an irreducible element of Λ. The statement that $PA = A$ means that $\pi A = A$, i.e., A is *divisible by π*. Let Y denote the torsion Λ-submodule of $X = \widehat{A}$. Then, assuming statement *(b)*, one has $PA = A$ if and only if $P \notin \mathrm{Supp}(Y)$. In the definition of "almost divisible," one can take θ to be any nonzero element of Λ divisible by all irreducible elements π which generate prime ideals in $\mathrm{Supp}(Y)$, e.g., θ could be a generator of the characteristic ideal of the Λ-module Y.

One can ask about the behavior of pseudo-null modules under specialization. Here is one useful result.

Proposition 2.5. *Suppose that the Krull dimension of Λ is at least 3 and that X is a finitely generated, pseudo-null Λ-module. Then there exist infinitely many prime ideals $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ such that X/PX is pseudo-null as a (Λ/P)-module.*

Proof. One can consider Λ as a formal power series ring $\Lambda_o[[T]]$ in one variable, where the subring Λ_o is a formal power series ring (over either $\mathbb{Z}_p$ or $\mathbb{F}_p$) in one less variable. One can choose Λ_o so that X is a finitely generated, torsion module over Λ_o. (See Lemma 2 in [Gr78] if Λ has characteristic 0. The proof there works if Λ has characteristic p.) Since the Krull dimension of Λ_o is at least 2, there exist infinitely many prime ideals P_o of Λ_o of height 1. The module X/P_oX will be a finitely generated, torsion (Λ_o/P_o)-module for all but finitely many such P_o's. Now $P_o = (\pi_o)$, where π_o is an irreducible element of Λ_o. Clearly, π_o is also irreducible in Λ. The ideal $P = \pi_o\Lambda$ is a prime ideal of height 1 in Λ. Since X/PX is finitely generated and torsion over Λ_o/P_o, and $\Lambda/P \cong (\Lambda_o/P_o)[[T]]$, it follows that X/PX is a pseudo-null (Λ/P)-module. ■

One surprising consequence concerns the existence of infinitely many height 1 prime ideals of a different sort.

Corollary 2.5.1. *Suppose that Λ has Krull dimension at least 2 and that X is a finitely generated, pseudo-null Λ-module. Then there exist infinitely many prime ideals $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ such that $P \subset \mathrm{Ann}_\Lambda(X)$.*

Proof. We will argue by induction. If Λ has Krull dimension 2, the the result is rather easy to prove. In that case, one has $\mathfrak{m}_\Lambda^n \subset \mathrm{Ann}_\Lambda(X)$ for some $n > 0$. It suffices to prove that $\mathfrak{m}_\Lambda^n$ contains infinitely many irreducible elements which generate distinct ideals. First consider $\Lambda = \mathbb{Z}_p[[T]]$. There exist field extensions of $\mathbb{Q}_p$ of degree $\geq n$. For any such extension F, choose a generator over $\mathbb{Q}_p$ which is in a large power of the maximal ideal of F. Then its minimal polynomial over $\mathbb{Q}_p$ will be in $\mathfrak{m}_\Lambda^n$ and will be an irreducible elements of Λ. By varying the extension F or the generator, one obtains the desired irredicible elements of Λ. The same argument works for $\mathbb{F}_p[[S,T]]$ since the fraction field of $\mathbb{F}_p[[S]]$ also has finite, separable extensions of arbitrarily high degree.

In the proof of proposition 2.5, it is clear that we can choose the P_o's so that Λ_o/P_o is also a formal power series ring. The same will then be true for Λ/P. Now assume that the Krull dimension of Λ is at least 3. Choose two elements $\theta_1, \theta_2 \in \mathrm{Ann}(X)$ such that θ_1 and θ_2 are relatively prime. The Λ-module $Y = \Lambda/(\theta_1, \theta_2)$ is then pseudo-null. Choose P so that $\overline{\Lambda} = \Lambda/P$ is a formal power series ring and so that $\overline{Y} = Y/PY$ is a pseudo-null $\overline{\Lambda}$-module. Let $\overline{\theta_1}$ and $\overline{\theta_2}$ denote the images of θ_1 and θ_2 in $\overline{\Lambda}$. Then $\overline{Y} = \overline{\Lambda}/(\overline{\theta_1}, \overline{\theta_2})$ and the fact that this is pseudo-null means that $\overline{\theta_1}$ and $\overline{\theta_2}$ are relatively prime in that ring. Clearly, the ideal $\mathrm{Ann}_{\overline{\Lambda}}(\overline{Y})$ in $\overline{\Lambda}$ is generated by $\overline{\theta_1}$ and $\overline{\theta_2}$. We assume that this ideal contains infinitely many prime ideals of $\overline{\Lambda}$ of height 1. Any such prime ideal has a generator of the form $\overline{\alpha_1}\overline{\theta_1} + \overline{\alpha_2}\overline{\theta_2}$, where $\overline{\alpha_1}, \overline{\alpha_2} \in \overline{\Lambda}$ are the images of $\alpha_1, \alpha_2 \in \Lambda$, say. Let $\eta = \alpha_1\theta_1 + \alpha_2\theta_2$. Then $\eta \in \mathrm{Ann}_\Lambda(X)$ and is easily seen to be an irreducible element of Λ. We can find infinitely many distinct prime ideals $(\eta) \subset \mathrm{Ann}_\Lambda(X)$ in this way. ■

C. Reflexive and coreflexive modules. Let $m \geq 0$. Suppose that the ring Λ is either $\mathbb{Z}_p[[T_1, ..., T_m]]$ (which we take to be $\mathbb{Z}_p$ if $m = 0$) or $\mathbb{F}_p[[T_1, ..., T_{m+1}]]$, so that the Krull-dimension of Λ is $m+1$. Suppose that X is a finitely generated, torsion-free Λ-module. Let $\mathcal{L}$ denote the fraction field of Λ. Let Λ_P be the localization of Λ at P. We can view the localization $X_P = X \otimes_\Lambda \Lambda_P$ as a subset of $\mathcal{V} = X \otimes_\Lambda \mathcal{L}$ which is a vector space over $\mathcal{L}$ of dimension $\mathrm{rank}_\Lambda(X)$. The *reflexive hull* of X is defined to be the Λ-submodule of $\mathcal{V}$ defined by $\widetilde{X} = \bigcap_P X_P$, where this intersection is over all prime ideals $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ and Λ_P is the localization of Λ at P. Then $\widetilde{X}$ is also a finitely generated, torsion-free Λ-module, $X \subseteq \widetilde{X}$, and the quotient $\widetilde{X}/X$ is a pseudo-null Λ-module. Furthermore, suppose that X' is any finitely generated, torsion-free Λ-module such that $X \subseteq X'$ and X'/X is pseudo-null. Since X'/X is Λ-torsion, one can identify X' with a Λ-submodule of $\mathcal{V}$ containing X. Then $X' \subseteq \widetilde{X}$. We say that X is a *reflexive* Λ*-module* if $\widetilde{X} = X$. This is equivalent to the more usual definition that X is isomorphic to its Λ-bidual under the natural map. We will make several useful observations.

Suppose that R is a finite, integral extension of Λ. Let $\mathcal{K}$ denote the fraction field of R. We can define the notion of a reflexive R-module in the same way as above. If X is any finitely generated, torsion-free R-module, the *R-reflexive hull of* X is the R-submodule of the $\mathcal{K}$-vector space $X \otimes_R \mathcal{K}$ defined by $\widetilde{X} = \bigcap_{\mathcal{P}} X_{\mathcal{P}}$, where $\mathcal{P}$ runs over all the prime ideals of R of height 1. This is easily seen to coincide with the Λ-reflexive hull of X as defined above. One uses the fact that, with either definition, $\widetilde{X}$ is torsion-free as both an R-module and a Λ-module, $\widetilde{X}/X$ is pseudo-null as both an R-module and a Λ-module, and $\widetilde{X}$ is maximal with respect to those properties. We can define X to be a reflexive R-module if $\widetilde{X} = X$. But our remarks justify the following equivalence:

1. *An R-module X is reflexive as an R-module if and only if it is reflexive as a Λ-module.*

Thus, it suffices to consider Λ-modules. Suppose that X is a reflexive Λ-

module and that Y is an arbitrary Λ-submodule of X. Both are torsion-free Λ-modules, but, of course, the quotient R-module X/Y may fail to be torsion-free. However, one can make the following important observation:

2. *The Λ-module Y is reflexive if and only if X/Y contains no nonzero pseudo-null Λ-submodules.*

This is rather obvious from the properties of the reflexive hull. Since X is assumed to be reflexive, we have $\widetilde{Y} \subseteq X$. Hence $\widetilde{Y}/Y$ is the maximal pseudo-null Λ-submodule of X/Y. Every pseudo-null Λ-submodule of X/Y is contained in $\widetilde{Y}/Y$. The observation follows from this.

The above observation provides a rather general construction of reflexive Λ-modules. To start, suppose that X is any reflexive Λ-module and that $\mathrm{rank}(X) = r$, e.g., $X = \Lambda^r$. If Y is a Λ-submodule of X such that X/Y is torsion-free, then X/Y certainly cannot contain a nonzero pseudo-null Λ-submodule. Thus Y must be reflexive. Consider the $\mathcal{L}$-vector space $\mathcal{V}$ defined before. It has dimension r over $\mathcal{L}$. Let $\mathcal{W}$ be any $\mathcal{L}$-subspace of $\mathcal{V}$. Let $Y = X \cap \mathcal{W}$. Then $\mathrm{rank}_\Lambda(Y) = \dim_{\mathcal{L}}(\mathcal{W})$. It is clear that X/Y is a torsion-free Λ-module and so the Λ-module Y will be reflexive. To see this, first note that X/Y is a torsion-free Λ-module. Here is one important type of example.

3. *Suppose that a group G acts Λ-linearly on a reflexive Λ-module X. Then $Y = X^G$ must also be reflexive as a Λ-module.*

This is clear since G will act $\mathcal{L}$-linearly on $\mathcal{V}$ and, if we let $\mathcal{W}$ denote the subspace $\mathcal{V}^G$, then $Y = X \cap \mathcal{W}$.

Suppose that $m = 0$. Then Λ is either $\mathbb{Z}_p$ or $\mathbb{F}_p[[T]]$. Both are discrete valuation rings and have just one nonzero prime ideal, its maximal ideal, which has height 1. The module theory is quite simple, and every finitely generated, torsion-free Λ-module is free and hence reflexive. However, suppose that $m \geq 1$. Then Λ has infinitely many prime ideals of height 1. They are all principal since Λ is a UFD. We then have the following useful result. We always take the term reflexive to include the assumption that the module is finitely generated and torsion-free.

Proposition 2.6. *Assume that $m \geq 1$ and that X is a finitely generated Λ-module.*

(a) If X is a reflexive Λ-module and if $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, then X/PX is a torsion-free (Λ/P)-module.

(b) If X/PX is a torsion-free (Λ/P)-module for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, then X is a reflexive Λ-module.

Proof. Suppose first that X is reflexive and that P is any prime ideal of height 1 in Λ. Then we have $P = (\pi)$, where π is an irreducible element of Λ. Therefore, $PX = \pi X$ is isomorphic to X and hence is also a reflexive Λ-module. As observed above, it follows that X/PX contains no nonzero pseudo-null Λ-submodules. But any finitely generated, torsion (Λ/P)-module will be pseudo-null when considered as a Λ-module. This is clear because the annihilator of such a (Λ/P)-module will contain π as well as some nonzero element of Λ which is not divisible by π. Therefore, X/PX must indeed be a torsion-free as a (Λ/P)-module, proving part *(a)*.

Now, under the assumptions of *(b)*, we first show that X must be a torsion-free Λ-module. For if Y is the Λ-torsion submodule of X and if $P = (\pi)$ is any height 1 prime ideal, then the snake lemma implies that there is an injective map $Y/PY \to X/PX$. But, if Y is nonzero, so is Y/PY. Also, if $\lambda \in \Lambda$ is a nonzero annihilator of Y, then Y/PY is a torsion (Λ/P)-module for all but the finitely many prime ideals P of height 1 which contain λ. It follows that $Y = 0$. There are infinitely many such P's.

Let $Z = \widetilde{X}/X$. Then Z is a pseudo-null Λ-module. Assume Z is nonzero. Then there exist infinitely many prime ideals $P = (\pi)$ of Λ of height 1 such that $Z[\pi]$ is nonzero too. Clearly, $Z[\pi]$ is a torsion (Λ/P)-module. Consider the exact sequence

$$0 \to X \to \widetilde{X} \to Z \to 0$$

By the snake lemma, together with the fact that $\widetilde{X}$ is a torsion-free Λ-module, one obtains an injective map $Z[\pi] \to X/PX$. Therefore, for infinitely many P's, X/PX fails to be torsion-free as a (Λ/P)-module, contradicting the hypothesis. Hence $Z = 0$ and X is indeed reflexive. ■

The first part of proposition 2.6 is quite trivial for free modules. In fact, if R is any ring and X is a free R-module, then $X/\mathcal{P}X$ is a free $(R/\mathcal{P})$-module and will certainly be torsion-free if $\mathcal{P}$ is any prime ideal of R.

We often will use proposition 2.6 in its discrete form.

Corollary 2.6.1. *Suppose that $m \geq 1$ and that A is a cofinitely generated Λ-module.*

- *(a) If A is a coreflexive Λ-module, then $A[P]$ is a divisible (Λ/P)-module for every prime ideal P of Λ of height 1.*
- *(b) If $A[P]$ is a divisible (Λ/P)-module for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, then A must be coreflexive as a Λ-module.*

Remark 2.6.2. One simple consequence concerns the case where the Krull-dimension is 2, i.e. Λ is either $\mathbb{Z}_p[[T]]$ or $\mathbb{F}_p[[S,T]]$. Suppose that X is a reflexive Λ-module. The ring $\Lambda/(T)$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{F}_p[[S]]$, both principal ideal domains. Since X/TX is a finitely-generated, torsion-free module over $\Lambda/(T)$, it is therefore a free module. Let $r = \mathrm{rank}_\Lambda(X)$. Proposition 2.3 implies that the rank of X/TX over $\Lambda/(T)$ is also equal to r. Hence X/TX can be generated as a $\Lambda/(T)$-module by exactly r elements. By Nakayama's lemma, X can be generated by r elements as a Λ-module and so it is a quotient of Λ^r. It follows that $X \cong \Lambda^r$. Therefore, we have the following well-known result:

If Λ has Krull dimension 2, then every reflexive Λ-module is free.

It follows that every coreflexive Λ-module is cofree when Λ has Krull dimension 2.

Remark 2.6.3. One can use proposition 2.6 to give examples of reflexive Λ-modules which are not free if the Krull dimension of Λ is at least 3. A torsion-free Λ-module of rank 1 will be isomorphic to an ideal in Λ and it is known that a reflexive ideal must be principal and hence free. Thus, our examples will have rank at least 2. We take $X = \Lambda^r$. Let Y be a Λ-submodule of X with the property that $Z = X/Y$ is a torsion-free Λ-module. Thus, as observed before, Y will be Λ-reflexive. Suppose that $P = (\pi)$ is any prime ideal of Λ of height 1. Then we have an exact sequence

$$0 \longrightarrow Y/PY \longrightarrow X/PX \longrightarrow Z/PZ \longrightarrow 0$$

of (Λ/P)-modules. We can choose P so that Λ/P is also a formal power series ring. Assume that Y is actually a free Λ-module. Then both Y/PY and X/PX would be free (Λ/P)-modules and hence reflexive. Therefore, the quotient module Z/PZ would contain no nonzero pseudo-null (Λ/P)-submodules. However, it is easy to give examples of torsion-free Λ-modules Z which fail to have that property. As one simple example, suppose that Z is the maximal ideal $\mathfrak{m}_\Lambda$ of Λ. Then Λ/Z is annihilated by π and so we have

$$\pi Z \subsetneq \pi\Lambda \subset Z$$

Thus, $\pi\Lambda/\pi Z$ is a (Λ/P)-submodule of Z/PZ, has order p, and will be a pseudo-null (Λ/P)-module since that ring has Krull dimension at least 2. Take r to be the number of generators of Z as a Λ-module and take X as above. Then one has a surjective Λ-module homomorphism $X \to Z$. If we let Y denote the kernel of this homomorphism, then Y is a reflexive Λ-module, but cannot be free.

One can view this remark from the point of view of homological algebra. Nakayama's Lemma implies easily that projective Λ-modules are free. Let d denote the Krull dimension of Λ. Thus, as we just explained, the Λ-module $\mathfrak{m}_\Lambda$ cannot have projective dimension 1 if $d \geq 3$. In fact, one can show that $\mathfrak{m}_\Lambda$ has projective dimension $d-1$.

D. Reflexive domains. In general, if R is any commutative integral domain, we will say that R is a reflexive domain if

$$R = \bigcap_{\mathcal{P}} R_{\mathcal{P}},$$

where $\mathcal{P}$ varies over all prime ideal of R of height 1 and $R_{\mathcal{P}}$ denotes the localization of R at $\mathcal{P}$. If R contains Λ as a subring and is finitely generated as a Λ-module, then R is reflexive in the above sense precisely when R is reflexive as a Λ-module. This is implied by the following result. Note that $\mathcal{K} = R \otimes_\Lambda \mathcal{L}$

is the fraction field of R. We define $\widetilde{R} = \bigcap_{\mathcal{P}} R_{\mathcal{P}}$, where $\mathcal{P}$ varies over all prime ideals of R of height 1. Thus, $\widetilde{R}$ is a subring of $\mathcal{K}$ containing R and R is a reflexive domain if and only if $R = \widetilde{R}$.

Proposition 2.7. *$\widetilde{R}$ is the reflexive hull of R as a Λ-module.*

Proof. Let P be a prime ideal of Λ of height 1. Let $\mathcal{P}_1, ..., \mathcal{P}_g$ be the prime ideals $\mathcal{P}$ of R such that $\mathcal{P} \cap \Lambda = P$. We let $R_P = R \otimes_\Lambda \Lambda_P$, which is the ring of fractions of R corresponding to the multiplicative set $\Lambda - P$. Then R_P is a subring of $\mathcal{K}$. The maximal ideals of R_P are $\mathcal{P}_i R_P, 1 \le i \le g$. The localization of R_P at $\mathcal{P}_i R_P$ is clearly $R_{\mathcal{P}_i}$ and so we have

$$R_P = \bigcap_{1 \le i \le g} R_{\mathcal{P}_i}$$

If $\mathcal{P}$ is any height 1 prime ideal of R, then $P = \mathcal{P} \bigcap \Lambda$ is a height 1 prime ideal of Λ. The proposition follows immediately. ■

Since $\widetilde{R}$ is also a finitely generated Λ-module, and hence an integral extension of Λ, we get the following corollary (which is actually a standard theorem; see corollary 11.4 in [E]).

Corollary 2.7.1. *If R is integrally closed, then R is reflexive.*

Suppose that R is a finite integral extension of Λ. Then it is known that R is a free Λ-module if and only if R is Cohen-Macaulay. (See proposition 2.2.11 in [B-H].) Any free Λ-module is reflexive, Thus, if R is Cohen-Macaulay, then R is reflexive. One simple type of example is $R = \Lambda[\theta]$, where θ is integral over Λ. Also, if R is regular or Gorenstein, then R is Cohen-Macaulay.

The first part of proposition 2.6 is valid for R-modules if R is assumed to be a reflexive domain. That is, if X is a finitely generated, reflexive R-module and $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$, then $X/\mathcal{P}X$ is a torsion-free $(R/\mathcal{P})$-module. The same proof works once one notes that any prime ideal $\mathcal{P}$ of height 1 in a reflexive domain R must be reflexive as an R-module. This is easily verified.

Suppose that R is a complete Noetherian local ring, but is not necessarily a domain. We will say that R is a reflexive ring if it has the following properties: *(i)* R contains a subring Λ which is isomorphic to a formal power series ring over either $\mathbb{Z}_p$ or $\mathbb{F}_p$ and *(ii)* R is a finitely generated, reflexive module over Λ. One important example arises from Hida theory. The universal ordinary Hecke algebra $\mathfrak{h}$ for a given level contains a natural subring Λ isomorphic to the formal power series ring $\mathbb{Z}_p[[T]]$ in one variable and is actually a free Λ-module of finite rank. Thus this ring $\mathfrak{h}$ is reflexive, but is not necessarily a domain. In general, suppose that R satisfies *(i)* and R is a torsion-free Λ-module. Then R is a subring of the $\mathcal{L}$-algebra $R \otimes_\Lambda \mathcal{L}$ and the reflexive hull $\widetilde{R}$ of R as a Λ-module will be a reflexive ring.

E. Different choices of $\mathcal{D}$. In the introduction we considered a free R-module $\mathcal{T}$ and defined $\mathcal{D} = \mathcal{T} \otimes_R \widehat{R}$, a cofree R-module, which we will now denote by $\mathcal{D}_R$. This construction behaves well under specialization at any ideal I of R in the following sense. Consider the free (R/I)-module $\mathcal{T}/I\mathcal{T}$. Applying the construction, we get

$$(\mathcal{T}/I\mathcal{T}) \otimes_{R/I} \widehat{(R/I)} \cong \mathcal{T} \otimes_R (\widehat{R}[I]) \cong \mathcal{D}_R[I].$$

Another construction which will be useful later is to define $\mathcal{D}_\Lambda = \mathcal{T} \otimes_\Lambda \widehat{\Lambda}$. Both constructions can be applied to an arbitrary R-module $\mathcal{T}$. To see the relationship, note that $\mathcal{D}_\Lambda \cong \mathcal{T} \otimes_R \widehat{\Lambda}_R$ where $\widehat{\Lambda}_R = R \otimes_\Lambda \widehat{\Lambda}$, the R-module obtained from $\widehat{\Lambda}$ by extending scalars from Λ to R. We have $\widehat{\Lambda}_R \cong \widehat{R}$ if R is free as a Λ-module. In that case, it would follow that $\mathcal{D}_R$ and $\mathcal{D}_\Lambda$ are isomorphic as R-modules. In general, one can only say that $\mathcal{D}_R$ and $\mathcal{D}_\Lambda$ are R-isogenous. Their R-coranks are equal to $\mathrm{rank}_R(\mathcal{T})$.

The Λ-module $\mathcal{D}_\Lambda$ is always coreflexive. To see this, let $P = (\pi)$ be any prime ideal of height 1 in Λ. Consider the exact sequence induced by multiplication by π.

$$0 \longrightarrow \widehat{\Lambda}[P] \longrightarrow \widehat{\Lambda} \xrightarrow{\pi} \widehat{\Lambda} \longrightarrow 0$$

Tensoring over Λ by $\mathcal{T}$, one gets a surjective homomorphism

$$(\mathcal{T}/P\mathcal{T}) \otimes_{\Lambda/P} (\widehat{\Lambda}[P]) \longrightarrow \mathcal{D}_\Lambda[P] \tag{3}$$

Since $\widehat{\Lambda}[P]$ is (Λ/P)-divisible, so is $(\mathcal{T}/P\mathcal{T}) \otimes_{\Lambda/P} (\widehat{\Lambda}[P])$ and that implies that $\mathcal{D}_\Lambda[P]$ is a divisible (Λ/P)-module. Corollary 2.6.1 then implies that $\mathcal{D}_\Lambda$ is coreflexive. We also remark that if $\mathcal{T}$ is assumed to be a torsion-free Λ-module, then proposition 2.3 implies that $\mathrm{rank}_{\Lambda/P}(\mathcal{T}/P\mathcal{T})$ and $\mathrm{corank}_{\Lambda/P}(\mathcal{D}_\Lambda[P])$ are both equal to $\mathrm{rank}_\Lambda(\mathcal{T})$ and so the map in (3) must be a (Λ/P)-isogeny.

Suppose that $\mathcal{T}_1$ and $\mathcal{T}_2$ are finitely generated R-modules. Let $\mathcal{D}_1 = \mathcal{T}_1 \otimes_R \widehat{R}$ and $\mathcal{D}_2 = \mathcal{T}_2 \otimes_R \widehat{R}$. We then have the following result.

Proposition 2.8. *Suppose that $\phi : \mathcal{T}_1 \to \mathcal{T}_2$ is an R-module homomorphism. Let $\psi : \mathcal{D}_1 \to \mathcal{D}_2$ be the R-module homomorphism determined by*

$$\psi(x \otimes y) = \phi(x) \otimes y$$

for $x \in \mathcal{T}_1,\ y \in \widehat{R}$. Then $\mathrm{corank}_R\big(\ker(\psi)\big) = \mathrm{rank}_R\big(\ker(\phi)\big)$. A similar equality holds for the cokernels of ψ and ϕ.

Proof. Let $\mathcal{T}_3$ denote the cokernel of ϕ. Let $D_3 = \mathcal{T}_3 \otimes_R \widehat{R}$. We then have exact sequences:

$$\mathcal{T}_1 \xrightarrow{\phi} \mathcal{T}_2 \longrightarrow \mathcal{T}_3 \longrightarrow 0, \qquad \mathcal{D}_1 \xrightarrow{\psi} \mathcal{D}_2 \longrightarrow \mathcal{D}_3 \longrightarrow 0$$

The second exact sequence follows from the first by tensoring each term with $\widehat{R}$. Since $\mathrm{corank}_R(\mathcal{D}_i) = \mathrm{rank}_R(\mathcal{T}_i)$ for each i, the stated equalities follow immediately. ■

The proposition is also valid if $\mathcal{D}_i$ is defined to be $\mathcal{T}_i \otimes_\Lambda \widehat{\Lambda}$ instead.

3 Cohomology Groups.

We consider a rather general situation. Suppose that R is a complete Noetherian local ring with maximal ideal $\mathfrak{m}$ and finite residue field k of characteristic p. Suppose that $\mathcal{D}$ is a cofinitely generated R-module and that G is a profinite group which acts continuously and R-linearly on $\mathcal{D}$. Then the cohomology groups $H^i(G, \mathcal{D})$ are also R-modules. Now $\mathcal{D}[\mathfrak{m}]$ is a finite dimensional representation space for G over k and hence over $\mathbb{F}_p$. Denote the distinct, $\mathbb{F}_p$-irreducible subquotients by $\alpha_1, ..., \alpha_t$. We will assume throughout that the cohomology groups $H^i(G, \alpha_k)$ are finite for all $i \geq 0$ and for all k, $1 \leq k \leq t$. This is so if *(i)* $G = G_{K_v}$, where K_v is the v-adic completion of a number field K at any prime v, or if *(ii)* $G = \mathrm{Gal}(K_\Sigma/K)$, where Σ is any finite set of primes of K.

A. Properties inherited from $\mathcal{D}$. First we prove the following result which will be useful in subsequent arguments.

Proposition 3.1. *Let $\mathcal{C} = \mathcal{D}_1/\mathcal{D}_2$, where $\mathcal{D}_1$ and $\mathcal{D}_2$ are G-invariant R-submodules of $\mathcal{D}$. Then every $\mathbb{F}_p$-irreducible subquotient of $\mathcal{C}[\mathfrak{m}]$ is isomorphic to one of the α_k's.*

Proof. First note that $\mathcal{C}$ is a cofinitely generated R-module, and so $\mathcal{C}[\mathfrak{m}]$ is finite. Also, $\mathcal{D} = \bigcup_{n \geq 0} \mathcal{D}[\mathfrak{m}^n]$. It follows that $\mathcal{C}[\mathfrak{m}]$ is a subquotient of $\mathcal{D}[\mathfrak{m}^n]$ for some n. Hence it is enough to prove that the composition factors for the G-module $\mathcal{D}[\mathfrak{m}^n]$ are isomorphic to the α_k's. It suffices to verify this for $\mathcal{D}[\mathfrak{m}^{j+1}]/\mathcal{D}[\mathfrak{m}^j]$ for all $j \geq 0$. Let $\lambda_1, ..., \lambda_g$ be a set of generators for the ideal $\mathfrak{m}^j$. Then one can define an injective G-homomorphism $\mathcal{D}[\mathfrak{m}^{j+1}]/\mathcal{D}[\mathfrak{m}^j] \to \mathcal{D}[\mathfrak{m}]^g$ by mapping the coset of $x \in \mathcal{D}[\mathfrak{m}^{j+1}]$ to $(\lambda_1 x, ..., \lambda_g x)$. The assertion about the composition factors follows from this. ∎

Corollary 3.1.1. *Let $i \geq 0$. If $H^i(G, \alpha_k) = 0$ for all k, $1 \leq k \leq t$, then $H^i(G, \mathcal{C}) = 0$ for every subquotient $\mathcal{C}$ of $\mathcal{D}$ as an $R[G]$-module.*

Proof. The hypothesis implies that $H^i(G, \mathcal{C}[\mathfrak{m}^n]) = 0$ for all $n \geq 0$. Since $\mathcal{C} = \varinjlim_{n} \mathcal{C}[\mathfrak{m}^n]$, it follows that $H^i(G, \mathcal{C}) = 0$ as stated. ∎

Note that $H^0(G, \mathcal{D}) = \mathcal{D}^G$ is just an R-submodule of $\mathcal{D}$, and so is also a cofinitely generated R-module. More generally, we have

Proposition 3.2. *For any $i \geq 0$, $H^i(G, \mathcal{D})$ is a cofinitely generated R-module.*

Proof. We prove this by induction on the minimal number of generators of the maximal ideal $\mathfrak{m}$. Let λ be one element of such a generating set for $\mathfrak{m}$. Consider the two exact sequences

$$0 \to \mathcal{D}[\lambda] \to \mathcal{D} \to \lambda\mathcal{D} \to 0, \qquad 0 \to \lambda\mathcal{D} \to \mathcal{D} \to \mathcal{D}/\lambda\mathcal{D} \to 0$$

The first is induced by multiplication by λ; the second is obvious. If $\mathfrak{m}$ is principa1, then $\mathcal{D}[\lambda] = \mathcal{D}[\mathfrak{m}]$ and $\mathcal{D}/\lambda\mathcal{D} = \mathcal{D}/\mathfrak{m}\mathcal{D}$ are both finite, and the hypothesis that the $H^i(G, \alpha_k)$'s are finite implies that $H^i(G, \mathcal{D}[\lambda])$ and $H^{i-1}(G, \mathcal{D}/\lambda\mathcal{D})$ are both finite. Thus the kernels of the two maps

$$H^i(G, \mathcal{D}) \to H^i(G, \lambda\mathcal{D}), \qquad H^i(G, \lambda\mathcal{D}) \to H^i(G, \mathcal{D})$$

are both finite. But the composite map $\mathcal{D} \to \lambda\mathcal{D} \to \mathcal{D}$ is multiplication by λ, and so the kernel of the composite map $H^i(G, \mathcal{D}) \to H^i(G, \lambda\mathcal{D}) \to H^i(G, \mathcal{D})$ is just $H^i(G, \mathcal{D})[\lambda]$, which is therefore finite. Thus, $H^i(G, \mathcal{D})[\mathfrak{m}]$ is finite, and hence, by Nakayama's lemma (the version for compact R-modules), $H^i(G, \mathcal{D})$ is cofinitely generated as a R-module.

If a minimal generating set for $\mathfrak{m}$ requires g generators, where $g > 1$, then the maximal ideal of $R/(\lambda)$ requires $g - 1$ generators. The $R/(\lambda)$-modules $\mathcal{D}[\lambda]$ and $\mathcal{D}/\lambda\mathcal{D}$ are both cofinitely generated. And so, by induction, we can assume that the $R/(\lambda)$-modules $H^i(G, \mathcal{D}[\lambda])$ and $H^{i-1}(G, \mathcal{D}/\lambda\mathcal{D})$ are also cofinitely generated. The above argument then shows that the $R/(\lambda)$-module $H^i(G, \mathcal{D})[\lambda]$ is cofinitely generated, and hence so is $H^i(G, \mathcal{D})[\mathfrak{m}]$. Nakayama's lemma then implies that the R-module $H^i(G, \mathcal{D})$ is cofinitely generated. ■

Various other properties of $\mathcal{D}$ are inherited by the Galois cohomology groups under certain hypotheses. Some are quite obvious. We assume in the rest of this section that R is a domain.

If $\mathcal{D}$ is R-cotorsion, then so is $H^i(G, \mathcal{D})$.

If $\mathcal{D}$ is a co-pseudo-null R-module, then so is $H^i(G, \mathcal{D})$.

As for the properties of divisibility or coreflexivity, these are also inherited under certain rather stringent hypotheses. We have the following result.

Proposition 3.3. *Suppose that $i \geq 0$. Suppose that $H^{i+1}(G, \alpha_k) = 0$ for $1 \leq k \leq t$.*

(a) If $\mathcal{D}$ is a divisible R-module, then so is $H^i(G, \mathcal{D})$.

(b) If $\mathcal{D}$ is a coreflexive R-module, then so is $H^i(G, \mathcal{D})$.

Note that the hypothesis that the $H^{i+1}(G, \alpha_k)$'s vanish is true if G has p-cohomological dimension equal to i. In particular, this hypothesis is true when $i = 2$ for $G = G_{K_v}$, where v is any non-archimedean prime of K, and for $G = \mathrm{Gal}(K_\Sigma/K)$ when p is an odd prime.

Proof. The ring R is a finitely generated module over a formal power series ring Λ. A finitely generated R-module X is torsion-free as an R-module if and only if it is torsion-free as a Λ-module. Also, X is reflexive as an R-module if and only if it is reflexive as a Λ-module. Thus, we may prove the proposition by using only the Λ-module structure. Prime ideals of Λ of height 1 are principal.

First we consider divisibility. Let $\lambda \in \Lambda$ be nonzero. Then we have the exact sequence

$$0 \to \mathcal{D}[\lambda] \to \mathcal{D} \to \mathcal{D} \to 0$$

induced by multiplication by λ. Hence we get an exact sequence

$$H^i(G, \mathcal{D}) \to H^i(G, \mathcal{D}) \to H^{i+1}(G, \mathcal{D}[\lambda])$$

The hypothesis in corollary 3.1.1 is satisfied for the index $i+1$ for the module $\mathcal{C} = \mathcal{D}[\lambda]$, and so we have $H^{i+1}(G, \mathcal{D}[\lambda]) = 0$. Thus multiplication by λ is surjective on $H^i(G, \mathcal{D})$, proving part *(a)* of the proposition.

Now we consider coreflexivity. Let $P = (\pi)$ be any prime ideal of height 1 in Λ. It suffices to show that $H^i(G, \mathcal{D})[P]$ is a divisible (Λ/P)-module for all such P. Then one can apply corollary 2.6.1 to get the conclusion. Now since $\mathcal{D}$ is Λ-divisible, we get an exact sequence

$$0 \to \mathcal{D}[P] \to \mathcal{D} \to \mathcal{D} \to 0$$

induced by multiplication by π. The corresponding cohomology sequence then gives a surjective map $H^i(G, \mathcal{D}[P]) \to H^i(G, \mathcal{D})[P]$ of (Λ/P)-modules. Corollary 2.6.1 implies that $\mathcal{D}[P]$ is (Λ/P)-divisible, and hence, by part *(a)*, so is $H^i(G, \mathcal{D}[P])$. It follows that $H^i(G, \mathcal{D})[P]$ is indeed divisible as a (Λ/P)-module, proving part *(b)*. ■

B. Behavior under specialization. If I is any ideal of R, then one has an obvious (R/I)-module homomorphism

$$H^i(G, \mathcal{D}[I]) \longrightarrow H^i(G, \mathcal{D})[I] \tag{4}$$

We will discuss the kernel and cokernel. Since $\mathcal{D}[I]^G = \mathcal{D}^G[I]$, this homomorphism is an isomorphism when $i = 0$. If $i \geq 1$, the simplest case to study is when I is a principal ideal and $\mathcal{D}$ is a divisible R-module. If $I = (\xi)$, then we consider the exact sequence induced by multiplication by ξ.

$$0 \longrightarrow \mathcal{D}[I] \longrightarrow \mathcal{D} \xrightarrow{\xi} \mathcal{D} \longrightarrow 0$$

The corresponding map on the cohomology groups is also induced by multiplication by ξ. This gives the exact sequence

$$0 \to H^{i-1}(G, \mathcal{D})/\xi H^{i-1}(G, \mathcal{D}) \to H^i(G, \mathcal{D}[I]) \to H^i(G, \mathcal{D})[I] \to 0 \tag{5}$$

Thus, when I is principal and $\mathcal{D}$ is divisible, the map (5) will at least be surjective. It suffices just to assume that $\mathcal{D}$ is divisible by the element ξ generating I. Here is one rather general and useful result for arbitrary ideals, valid even when $\mathcal{D}$ is not assumed to be divisible.

Proposition 3.4. *Suppose that $\mathcal{D}$ is a cofinitely generated R-module. Let $i \geq 0$. If $i > 0$, assume that $H^{i-1}(G, \alpha_k) = 0$ for $1 \leq k \leq t$. Suppose that I is any ideal of R. Then the map*

$$H^i(G, \mathcal{D}[I]) \longrightarrow H^i(G, \mathcal{D})[I]$$

is an isomorphism.

Proof. We've already remarked that the map is an isomorphism when $i = 0$. If $i > 0$, the assumption implies that $H^{i-1}(G, \mathcal{C}) = 0$ for every subquotient $\mathcal{C}$ of $\mathcal{D}$ as an $R[G]$-module. Therefore, if $\mathcal{D}'$ is an $R[G]$-submodule of $\mathcal{D}$, then $H^{i-1}(G, \mathcal{D}/\mathcal{D}') = 0$ and so the induced map $H^i(G, \mathcal{D}') \to H^i(G, \mathcal{D})$ will be injective.

Suppose first that $I = (\lambda)$ is a principal ideal. Multiplication by λ gives an exact sequence

$$0 \longrightarrow \mathcal{D}[\lambda] \xrightarrow{a} \mathcal{D} \xrightarrow{b} \lambda\mathcal{D} \longrightarrow 0$$

Let $\alpha : H^i(G, \mathcal{D}[\lambda]) \to H^i(G, \mathcal{D})$ and $\beta : H^i(G, \mathcal{D}) \to H^i(G, \lambda\mathcal{D})$ be the maps induced from a and b. The map α is injective and its image is the kernel of the map β. But the map $\gamma : H^i(G, \lambda\mathcal{D}) \to H^i(G, \mathcal{D})$ is also injective and so the maps β and $\gamma \circ \beta$ have the same kernel. The map $\gamma \circ \beta : H^i(G, \mathcal{D}) \to H^i(G, \mathcal{D})$ is just multiplication by λ. Therefore, the image of α is indeed $H^i(G, \mathcal{D})[\lambda]$, which proves the proposition if I is principal - an ideal with one generator.

We will argue by induction on the minimum number of generators of I. Suppose that $\lambda_1, ..., \lambda_g$ is a minimal generating set for I, where $g > 1$. Let $J = (\lambda_1, ..., \lambda_{g-1})$. Assume that the map $H^i(G, \mathcal{D}[J]) \to H^i(G, \mathcal{D})[J]$ is an isomorphism. Then so is the map

$$H^i(G, \mathcal{D}[J])[\lambda_g] \to (H^i(G, \mathcal{D})[J])[\lambda_g] = H^i(G, \mathcal{D})[I]$$

Now $\mathcal{D}[J][\lambda_g] = \mathcal{D}[I]$ and so, applying the proposition to $\mathcal{D}[J]$ and the principal ideal (λ_g), as we may, it follows that the map

$$H^i(G, \mathcal{D}[I]) \to H^i(G, \mathcal{D}[J])[\lambda_g]$$

is an isomorphism. Composing these isomorphisms, we get the isomorphism stated in the proposition for I. ■

Remark 3.4.1. For $i = 1$, the assumption in proposition 3.4 is that the trivial $\mathbb{F}_p$-representation of G is not a composition factor in the $\mathbb{F}_p[G]$-module $\mathcal{D}[\mathfrak{m}]$. Assuming this is satisfied, we have $H^1(G, \mathcal{D}[\mathcal{P}]) \cong H^1(G, \mathcal{D})[\mathcal{P}]$ for every prime ideal $\mathcal{P}$ of R. Let $r = \mathrm{corank}_R\big(H^1(G, \mathcal{D})\big)$. Applying remark 2.1.3 to $A = H^1(G, \mathcal{D})$, we see that $\mathrm{corank}_{R/\mathcal{P}}\big(H^1(G, \mathcal{D}[P])\big) \geq r$ for all $\mathcal{P}$ and that equality holds for all $\mathcal{P} \notin V(I)$, where I is some nonzero ideal of R. A similar statement is true for any i under the assumptions of proposition 3.4.

Remark 3.4.2. Suppose now that $R = \Lambda$ and that $\mathcal{D}$ is a cofree Λ-module. Assume that P is a regular prime ideal of Λ, i.e., that the local ring Λ/P is regular. The ideal P can be generated by a regular sequence $\lambda_1, ..., \lambda_g$ of elements of Λ. (See proposition 2.2.4 in [B-H].) Define $P_0 = (0)$ and, for $1 \leq j \leq g$, define $P_j = (\lambda_1, ..., \lambda_j)$. Then P_j is a prime ideal for $j \geq 0$ and $\mathcal{D}[P_j]$ is cofree and hence divisible as a (Λ/P_j)-module. Note that if $j \geq 1$, then $\mathcal{D}[P_j] = (\mathcal{D}[P_{j-1}])[\lambda_j]$ and multiplication by λ_j defines a surjective map on

$\mathcal{D}[P_{j-1}]$. The induced map $H^i(G,\mathcal{D}[P_j]) \longrightarrow H^i(G,\mathcal{D}[P_{j-1}])[P_j]$ is surjective. Hence

$$\mathrm{corank}_{\Lambda/P_j}\big(H^i(G,\mathcal{D}[P_j])\big) \;\geq\; \mathrm{corank}_{\Lambda/P_j}\big(H^i(G,\mathcal{D}[P_{j-1}])[P_j]\big)$$

On the other hand, remark 2.1.3 implies that

$$\mathrm{corank}_{\Lambda/P_j}\big(H^i(G,\mathcal{D}[P_{j-1}])[P_j]\big) \;\geq\; \mathrm{corank}_{\Lambda/P_{j-1}}\big(H^i(G,\mathcal{D}[P_{j-1}])\big)$$

Since $\mathcal{D}[P_0]=\mathcal{D}$, we have proved that

$$\mathrm{corank}_{\Lambda/P}\big(H^i(G,\mathcal{D}[P])\big) \;\geq\; \mathrm{corank}_{\Lambda}\big(H^i(G,\mathcal{D})\big)$$

for all regular prime ideals of Λ. In particular, suppose that $\Lambda/P \cong \mathbb{Z}_p$. Then

$$\mathrm{corank}_{\Lambda}\big(H^i(G,\mathcal{D})\big) \leq \mathrm{corank}_{\mathbb{Z}_p}\big(H^i(G,\mathcal{D}[P])\big) \leq \dim_{\mathbb{F}_p}\big(H^i(G,\mathcal{D}[\mathfrak{m}_\Lambda])\big).$$

In the following proposition, we consider $\mathcal{D}$ just as a Λ-module and take $I=P$ to be a prime ideal of height 1. However, the result can be extended to a more general class of rings R as explained in remark 3.5.2 below.

Proposition 3.5. *Suppose that $\mathcal{D}$ is a cofinitely generated Λ-module. Let $i \geq 0$. Then, for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, the kernel and cokernel of the map*

$$H^i(G,\mathcal{D}[P]) \longrightarrow H^i(G,\mathcal{D})[P]$$

are cotorsion (Λ/P)-modules and hence $H^i(G,\mathcal{D}[P])$ and $H^i(G,\mathcal{D})[P]$ will have equal (Λ/P)-coranks.

Proof. As already mentioned, the result is obvious for $i=0$. We assume first that $\mathcal{D}$ is Λ-divisible. Suppose that $i \geq 1$. The map in question is surjective. Let π be a generator of P, which is a principal ideal. Since we are assuming that $\mathcal{D}$ is Λ-divisible, we can use (5) for $I=P$. As a Λ-module, $H^{i-1}(G,\mathcal{D})/\pi H^{i-1}(G,\mathcal{D})$ is a quotient of the cofinitely generated, cotorsion Λ-module $A = H^{i-1}(G,\mathcal{D})/H^{i-1}(G,\mathcal{D})_{\Lambda-\mathrm{div}}$. Let $J = \mathrm{Ann}_\Lambda(A)$. Then it is clear that if P does not contain J, then $H^{i-1}(G,\mathcal{D})/\pi H^{i-1}(G,\mathcal{D})$ is a cotorsion (Λ/P)-module. If $\mathcal{D}$ is not Λ-divisible, then one notes that $\mathcal{D}$ is Λ-isogenous to $\mathcal{D}_{\Lambda-\mathrm{div}}$ and so one can easily reduce to the Λ-divisible case. ■

Remark 3.5.1. A similar result holds for the cohomology groups associated to a finitely generated Λ-module $\mathcal{T}$. We assume that G acts continuously and Λ-linearly on $\mathcal{T}$ and that the cohomology groups $H^i(G,\alpha)$ are finite for every simple subquotient α of the G-module $\mathcal{T}/\mathfrak{m}_\Lambda\mathcal{T}$. The G-module $\mathcal{T}$ is now compact and so we consider the continuous cohomology groups. A discussion of their properties can be found in [NSW], chapter II, §3. Since $\mathcal{T} = \varprojlim_n \mathcal{T}/\mathfrak{m}^n\mathcal{T}$, an inverse limit of finite Galois modules, we have

$$H^i_{cts}(G,\mathcal{T}) = \varprojlim_n H^i(G,\mathcal{T}/\mathfrak{m}^n\mathcal{T})$$

This follows from corollary 2.3.5 in [NSW]. Note that our assumption that the $H^i(G, \alpha)$'s are finite is needed for this. It is not hard to show that $H^i_{cts}(G, \mathcal{T})$ is a finitely generated Λ-module. If P is a prime ideal of Λ, one has a natural map $H^i_{cts}(G, \mathcal{T}) \to H^i_{cts}(G, \mathcal{T}/P\mathcal{T})$. Suppose that P is a prime ideal of height 1. Then we have the following compact version of proposition 3.5.

The kernel and cokernel of the map

$$H^i_{cts}(G, \mathcal{T})/PH^i_{cts}(G, \mathcal{T}) \longrightarrow H^i_{cts}(G, \mathcal{T}/P\mathcal{T})$$

are torsion (Λ/P)-modules for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$.

The argument is analogous to that given above. Suppose that $P = (\pi)$. Assuming first that $\mathcal{T}$ is a torsion-free Λ-module, one considers the exact sequence

$$0 \longrightarrow \mathcal{T} \xrightarrow{\pi} \mathcal{T} \longrightarrow \mathcal{T}/P\mathcal{T} \longrightarrow 0$$

induced by multiplication by π. The map in question is induced by this exact sequence. It is injective and its cokernel is isomorphic to $H^{i+1}_{cts}(G, \mathcal{T})[\pi]$, which is a Λ-submodule of $H^{i+1}_{cts}(G, \mathcal{T})_{\Lambda-tors}$, the torsion Λ-submodule of $H^{i+1}_{cts}(G, \mathcal{T})$. Therefore, this cokernel is indeed (Λ/P)-torsion for all but the finitely many $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ containing the annihilator of $H^{i+1}_{cts}(G, \mathcal{T})_{\Lambda-tors}$. As before, one easily reduces the general case to the case where $\mathcal{T}$ is torsion-free.

Remark 3.5.2. Suppose that $\mathcal{D}$ is a cofinitely generated R-module, where R is a finite, integral extension of Λ. Let $\mathcal{K}$ be the field of fractions for R, a finite extension of the field of fractions $\mathcal{L}$ of Λ. We will assume that $\mathcal{K}/\mathcal{L}$ is a separable extension. One can prove that the kernel and cokernel of the map

$$H^i(G, \mathcal{D}[\mathcal{P}]) \longrightarrow H^i(G, \mathcal{D})[\mathcal{P}]$$

will be cotorsion $(R/\mathcal{P})$-modules for almost all $\mathcal{P} \in \mathrm{Spec}_{ht=1}(R)$ as follows. Assume that $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ satisfies the conclusion of proposition 3.5 and is also unramified for the extension $\mathcal{K}/\mathcal{L}$ in the following sense: For all $\mathcal{P}$ lying over P, the maximal ideal in the localization $R_{\mathcal{P}}$ is generated by P. Fix one such $\mathcal{P}$. Consider the following commutative diagram

$$\begin{tikzcd}
H^i(G, \mathcal{D}[\mathcal{P}]) \arrow[r, "\alpha"] \arrow[d, "\beta"] & H^i(G, \mathcal{D})[\mathcal{P}] \arrow[d, "\beta'"] \\
H^i(G, \mathcal{D}[P]) \arrow[r, "\alpha'"] & H^i(G, \mathcal{D})[P]
\end{tikzcd}$$

The horizontal maps α and α' are defined in the obvious way. Both $\ker(\alpha')$ and $\mathrm{coker}(\alpha')$ are (Λ/P)-cotorsion by assumption. Thus, they are annihilated by some element $\lambda \in \Lambda - P$. The inclusion $\mathcal{D}[\mathcal{P}] \to \mathcal{D}[P]$ induces the map β. Since P is assumed to be unramified, $\mathcal{P} \subset PR_{\mathcal{P}}$ and hence there exists an element $\gamma \in R - \mathcal{P}$ such that $\gamma\mathcal{P} \subseteq PR$. This implies that $\gamma\mathcal{D}[P] \subseteq \mathcal{D}[\mathcal{P}]$ and so γ annihilates $\mathcal{D}[P]/\mathcal{D}[\mathcal{P}]$. It follows that $\ker(\beta)$ and $\mathrm{coker}(\beta)$ are annihilated by γ. It is also clear that β' is injective and $\mathrm{coker}(\beta')$ is annihilated by γ. A diagram chase then implies that $\ker(\alpha)$ and $\mathrm{coker}(\alpha)$ are annihilated by $\lambda\gamma$. Since this element of R is not in $\mathcal{P}$, it follows that the kernel and cokernel of α are cotorsion $(R/\mathcal{P})$-modules. This is true for all $\mathcal{P}$ lying over P.

The conclusion of proposition 3.5 is true for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. It remains to show that almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ are unramified in $\mathcal{K}/\mathcal{L}$. Let S denote the integral closure of R in $\mathcal{K}$. Then it is known that S is finitely generated as a Λ-module. (See theorem 6.4 in [D].) Let $\omega_1, ..., \omega_n$ be a fixed basis for $\mathcal{K}$ over $\mathcal{L}$ contained in R. Then for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, the localizations R_P and S_P coincide and are free Λ_P-modules with basis $\omega_1, ..., \omega_n$. Assume that P has this property. Now Λ_P is a discrete valuation ring and $R_P = S_P$ is a Dedekind ring. Since $\mathcal{K}/\mathcal{L}$ is separable, the discriminant of this extension for the fixed basis is nonzero, and the prime ideal P is unramified if it doesn't contain this discriminant. It clearly follows that only finitely many $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ can be ramified in $\mathcal{K}/\mathcal{L}$.

C. Almost divisibility. Suppose that $i \geq 1$ and that $P = (\pi)$ is a prime ideal of Λ of height 1. Then, according to (5), the map $H^i(G, \mathcal{D}[P]) \longrightarrow H^i(G, \mathcal{D})[P]$ will be injective if and only if $H^{i-1}(G, \mathcal{D})/\pi H^{i-1}(G, \mathcal{D}) = 0$, assuming that $\mathcal{D}$ is divisible by π. Thus, we have the following useful equivalence.

Proposition 3.6. *Suppose that $\mathcal{D}$ is an almost divisible, cofinitely generated Λ-module. Let $i \geq 1$. Then the Λ-module $H^{i-1}(G, \mathcal{D})$ is almost divisible if and only if the map*

$$H^i(G, \mathcal{D}[P]) \longrightarrow H^i(G, \mathcal{D})[P]$$

is injective for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$.

Here is one important special case.

Proposition 3.7. *Suppose that $\mathcal{D}$ is a coreflexive Λ-module on which G acts. Let $i \geq 0$. Assume that $H^{i+2}(G, \alpha_k) = 0$ for $1 \leq k \leq t$. If $H^{i+1}(G, \mathcal{D}) = 0$, then $H^i(G, \mathcal{D})$ is an almost divisible Λ-module.*

Proof. By proposition 3.6, it certainly suffices to show that $H^{i+1}(G, \mathcal{D}[P]) = 0$ for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. This follows if we show that $H^{i+1}(G, \mathcal{D}[P])$ is both (Λ/P)-cotorsion and (Λ/P)-divisible. Since $H^{i+1}(G, \mathcal{D}) = 0$, proposition 3.5 implies the first statement for all but finitely many height 1 prime ideals P. By corollary 2.6.1, $\mathcal{D}[P]$ is a divisible (Λ/P)-module, and proposition 3.3 then implies the (Λ/P)-divisibility of $H^{i+1}(G, \mathcal{D}[P])$ for every height 1 prime ideal P of Λ. ■

D. Replacing R by its reflexive closure. Now suppose that $\mathcal{T}$ is a free R-module of rank n and that G is a group which acts continuously and R-linearly on $\mathcal{T}$. Then G acts continuously and $\widetilde{R}$-linearly on $\widetilde{\mathcal{T}} = \mathcal{T} \otimes_R \widetilde{R}$. If R is a finite extension of Λ, then the above proposition implies that $\widetilde{\mathcal{T}}$ is the reflexive hull of $\mathcal{T}$ as a Λ-module. Both R and $\widetilde{R}$ are complete Noetherian local rings. As in the introduction, we define discrete G-modules $\mathcal{D} = \mathcal{T} \otimes_R \widehat{R}$ and $\widetilde{\mathcal{D}} = \widetilde{\mathcal{T}} \otimes_{\widetilde{R}} \widehat{\widetilde{R}}$. Then $\mathcal{D}$ is an R-module, $\widetilde{\mathcal{D}}$ is an $\widetilde{R}$-module, both are cofinitely generated Λ-modules, $\mathcal{D}$ is a divisible Λ-module, $\widetilde{\mathcal{D}}$ is a coreflexive Λ-module, and there is a surjective G-equivariant Λ-module homomorphism $\widetilde{\mathcal{D}} \to \mathcal{D}$ whose kernel $\mathcal{C}$ is a co-pseudo-null Λ-module.

The hypothesis in proposition 3.3 for $\mathcal{D}$ and for $\widetilde{\mathcal{D}}$ are equivalent. To explain this, let $\mathfrak{m}_\Lambda$ denote the maximal ideal of Λ, $\widetilde{\mathfrak{m}}$ the maximal ideal of $\widetilde{R}$. Then we can regard $\mathcal{D}[\mathfrak{m}_\Lambda]$ as a finite-dimensional representation space for G over the residue field $\Lambda/\mathfrak{m}_\Lambda \cong \mathbb{F}_p$ and $\mathcal{D}[\widetilde{\mathfrak{m}}]$ as such a representation space over $\widetilde{R}/\widetilde{\mathfrak{m}}$ and hence over $\mathbb{F}_p$. We then have the following observation.

Proposition 3.8. *The $\mathbb{F}_p$-representations spaces $\mathcal{D}[\mathfrak{m}]$, $\widetilde{\mathcal{D}}[\widetilde{\mathfrak{m}}]$, $\mathcal{D}[\mathfrak{m}_\Lambda]$, and $\widetilde{\mathcal{D}}[\mathfrak{m}_\Lambda]$ for G have the same irreducible subquotients.*

Proof. First note that $\mathcal{D}$ is a quotient of $\widetilde{\mathcal{D}}$. Also, for any nonzero $\lambda \in \Lambda$, one has $\widetilde{\mathcal{D}}/\widetilde{\mathcal{D}}[\lambda] \cong \widetilde{\mathcal{D}}$. One can choose λ so that $\mathcal{C} \subseteq \widetilde{\mathcal{D}}[\lambda]$. Since $\widetilde{\mathcal{D}}/\mathcal{C} \cong \mathcal{D}$, it is clear that $\widetilde{\mathcal{D}}$ is isomorphic to a subquotient of $\mathcal{D}$. Hence proposition 3.1 implies that $\mathcal{D}[\mathfrak{m}]$ and $\widetilde{\mathcal{D}}[\mathfrak{m}]$ have the same irreducible subquotients.

Now $\mathfrak{m}_\Lambda \subseteq \mathfrak{m}$ and so $\mathcal{D}[\mathfrak{m}] \subseteq \mathcal{D}[\mathfrak{m}_\Lambda]$. Also, the fact that $R/\mathfrak{m}_\Lambda R$ is finite implies that $\mathfrak{m}^t \subseteq \mathfrak{m}_\Lambda R$ for some $t \geq 1$. Hence $\mathcal{D}[\mathfrak{m}_\Lambda] \subseteq \mathcal{D}[\mathfrak{m}^t]$. Proposition 3.1 again implies that $\mathcal{D}[\mathfrak{m}_\Lambda]$ and $\mathcal{D}[\mathfrak{m}]$ have the same irreducible subquotients. The same argument applies to $\widetilde{\mathcal{D}}[\mathfrak{m}_\Lambda]$ and $\widetilde{\mathcal{D}}[\widetilde{\mathfrak{m}}]$. The proposition follows from these observations. ■

The surjective homomorphism $\widetilde{\mathcal{D}} \to \mathcal{D}$ induces a map $H^i(G, \widetilde{\mathcal{D}}) \to H^i(G, \mathcal{D})$ for any $i \geq 0$. Since $H^i(G, \mathcal{C})$ and $H^{i+1}(G, \mathcal{C})$ are co-pseudo-null, the same will be true for both the kernel and the cokernel of that induced map. Proposition 3.3 then has the following consequence.

Proposition 3.9. *Suppose that $i \geq 0$. Suppose that $H^{i+1}(G, \alpha_k) = 0$ for $1 \leq k \leq t$. Then the map $H^i(G, \widetilde{\mathcal{D}}) \to H^i(G, \mathcal{D})$ is surjective, $H^i(G, \mathcal{D})$ is Λ-divisible, $H^i(G, \widetilde{\mathcal{D}})$ is Λ-coreflexive, and the Pontryagin dual of $H^i(G, \widetilde{\mathcal{D}})$ is precisely the reflexive hull of the Pontryagin dual of $H^i(G, \mathcal{D})$.*

Proof. Note that $H^{i+1}(G, \mathcal{C}) = 0$ by proposition 3.8 and corollary 3.1.1. This implies the surjectivity. The divisibility of $H^i(G, \mathcal{D})$ and coreflexivity of $H^i(G, \widetilde{\mathcal{D}})$ follow from propositions 3.8 and 3.3. The Pontryagin dual of $H^i(G, \mathcal{D})$ is a torsion-free Λ-module which is mapped injectively into the Pontryagin dual of $H^i(G, \widetilde{\mathcal{D}})$. The corresponding quotient Λ-module is a submodule of the Pontryagin dual of $H^i(G, \mathcal{C})$, and so it is pseudo-null. The final statement follows from this. ■

Remark 3.9.1. If $\mathcal{D}$ is not coreflexive, then $H^i(G, \mathcal{D})$ would often fail to be coreflexive too. Suppose, for example, that $i = 1$ and that both $H^0(G, \alpha_k)$ and

$H^2(G,\alpha_k)$ vanish for all k, $1 \le k \le t$. Then, if $H^1(G,\mathcal{D}[\mathfrak{m}]) \ne 0$, it follows that $H^1(G,\mathcal{C}) \ne 0$ and that the map $H^i(G,\widetilde{\mathcal{D}}) \to H^i(G,\mathcal{D})$ will have a nonzero kernel. In that case, proposition 3.9 implies that $H^i(G,\mathcal{D})$ is non-reflexive.

E. Relationship between $H^i(G,\mathcal{D})$ and $H^i_{cts}(G,\mathcal{T})$. Consider an arbitrary finitely generated R-module $\mathcal{T}$ on which a group G acts continuously and R-linearly. We assume that $H^i(G,\alpha)$ is finite for all $i \ge 0$ and all simple subquotients α of the finite G-module $\mathcal{T}/\mathfrak{m}\mathcal{T}$. Let $\mathcal{D} = \mathcal{T} \otimes_R \widehat{R}$.

Proposition 3.10. *We have* $\mathrm{rank}_R\big(H^i_{cts}(G,\mathcal{T})\big) = \mathrm{corank}_R\big(H^i(G,\mathcal{D})\big)$ *for all* $i \ge 0$.

Proof. The statement concerns $\mathcal{D} = \mathcal{D}_R$. Note that the simple subquotients α of the G-module $\mathcal{D}[\mathfrak{m}]$ are among those for $\mathcal{T}/\mathfrak{m}\mathcal{T}$ and so the corresponding cohomology groups are finite. To prove the equality, it is enough to consider the rank and corank over the subring Λ of R. We replace $\mathcal{D}_R$ by $\mathcal{D}_\Lambda = \mathcal{T} \otimes_\Lambda \widehat{\Lambda}$. This module is R-isogenous to $\mathcal{D}_R$ and so the corresponding cohomology groups will have the same coranks.

If Λ has Krull dimension 1, then the argument is straightforward. The maximal ideal $\mathfrak{m}_\Lambda$ of Λ is then principal. Letting $A_n = \mathcal{T}/\mathfrak{m}_\Lambda^n\mathcal{T}$, we have $A_n \cong \mathcal{D}[\mathfrak{m}_\Lambda^n]$ for any $n \ge 0$. One can relate the rank or corank in question to the growth of the finite groups $H^i(G,A_n)$ as $n \to \infty$. If Λ has Krull dimension > 1, there are infinitely many prime ideals of Λ of height 1. We then use an induction argument on the Krull dimension. Let $r = \mathrm{corank}_\Lambda\big(H^i(G,\mathcal{D})\big)$ and $s = \mathrm{rank}_\Lambda\big(H^i(G,\mathcal{T})\big)$. According to proposition 3.5, the (Λ/P)-corank of $H^i(G,\mathcal{D}[P])$ will be equal to r for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. As pointed out in part E of section 2, one has a surjective (Λ/P)-homomorphism

$$(\mathcal{T}/P\mathcal{T}) \otimes_{\Lambda/P} \widehat{(\Lambda/P)} \to \mathcal{D}[P]$$

For almost all P's, the (Λ/P)-coranks of these modules will be equal, the kernel will therefore be (Λ/P)-cotorsion, and hence $H^i\big(G,(\mathcal{T}/P\mathcal{T}) \otimes_{\Lambda/P} \widehat{(\Lambda/P)}\big)$ will also have (Λ/P)-corank equal to r. We can choose such a P so that Λ/P is also a formal power series ring. The Krull dimension will be reduced by 1 and so we assume, inductively, that the (Λ/P)-rank of $H^i(G,\mathcal{T}/P\mathcal{T})$ is equal to r too. This will be true for an infinite set of P's in $\mathrm{Spec}_{ht=1}(\Lambda)$. However, according to remark 3.5.1, $H^i(G,\mathcal{T}/P\mathcal{T})$ will have (Λ/P)-rank equal to s for all but finitely many such P's. Therefore, $r = s$. ■

Remark 3.10.1. We want to mention another argument for the case $i = 0$ based on proposition 2.8. Let $\mathcal{D} = \mathcal{D}_R$. We will assume that G is topologically finitely generated. Let $g_1, ..., g_t \in G$ generate a dense subgroup of G. Consider the map $\phi : \mathcal{T} \longrightarrow \mathcal{T}^t$ defined by $\phi(x) = \big((g_1-1)x, ..., (g_t-1)x\big)$ for all $x \in \mathcal{T}$. The induced map $\psi : \mathcal{D} \longrightarrow \mathcal{D}^t$, as defined in proposition 2.8, is given by the same formula, but for $x \in \mathcal{D}$ instead. This definition implies that $\ker(\phi) = H^0(G,\mathcal{T})$ and that $\ker(\psi) = H^0(G,\mathcal{D})$. Proposition 2.8 then implies the equality of the R-rank and R-corank for these two R-modules.

A similar argument implies that the R-rank of $\mathcal{T}_G$ is equal to the R-corank of $\mathcal{D}_G$. These modules are the maximal *quotients* on which G acts trivially. Consider the map $\phi' : \mathcal{T}^t \longrightarrow \mathcal{T}$ defined by $\phi'(x_1, ..., x_t) = \sum_{i=1}^t (g_i - 1)x_i$ for all $x \in \mathcal{T}^t$. The induced map $\psi' : \mathcal{D}^t \longrightarrow \mathcal{D}$ is again given by the same formula. It is easy to see that $\mathrm{coker}(\phi') = \mathcal{T}_G$ and $\mathrm{coker}(\psi') = \mathcal{D}_G$. The stated equality follows from proposition 2.8.

Remark 3.10.2. One can apply remark 2.1.2 to obtain a useful consequence if we assume that $\mathcal{T}$ is a free R-module. Then $\mathcal{T}^t$ is also a free R-module. Let ϕ be the map defined above. If $\mathcal{P}$ is a prime ideal of R, then $\phi_{\mathcal{P}}$ is defined by the same formula as ϕ. It follows that $\mathrm{rank}_{R/\mathcal{P}}\big((\mathcal{T}/\mathcal{P}\mathcal{T})^G\big) \geq \mathrm{rank}_R\big(\mathcal{T}^G\big)$ for *every* prime ideal $\mathcal{P}$ of R. According to proposition 2.1.1, equality holds on a nonempty Zariski-open subset of $\mathrm{Spec}(R)$. Also, note that if $(\mathcal{T}/\mathcal{P}\mathcal{T})^G = 0$ for some prime ideal $\mathcal{P}$, then it follows that $\mathcal{T}^G = 0$.

4 Coranks.

In this section we will prove theorems concerning Euler-Poincaré characteristics, lower bounds on the R-coranks of H^1 and H^2, and the relationship between the R-coranks of $Ш^1$ and $Ш^2$. Assume that R is a finite, integral extension of Λ. If X is a finitely generated R-module, then $\mathrm{rank}_\Lambda(X) = \mathrm{rank}_R(X)\mathrm{rank}_\Lambda(R)$. Hence we can derive the formulas for ranks or coranks by considering the various R-modules as Λ-modules. This simplifies the arguments since the prime ideals of height 1 in Λ are principal. Thus, we will formulate all the results for a discrete, cofinitely generated Λ-module $\mathcal{D}$ which has a Λ-linear action of the appropiate Galois groups. Proposition 3.2 implies that the Galois cohomology groups $H^i(K_\Sigma/K, \mathcal{D})$ and $H^i(K_v, \mathcal{D})$ are also cofinitely generated Λ-modules. Thus, we can consider their Λ-coranks.

A. Euler-Poincaré characteristics. We assume that $\mathcal{D}$ has a Λ-linear action of $\mathrm{Gal}(K_\Sigma/K)$. We will prove the following result.

Proposition 4.1. *Let* $m = \mathrm{corank}_\Lambda(\mathcal{D})$, $m_v^- = \mathrm{corank}_\Lambda(\mathcal{D}/\mathcal{D}^{G_{K_v}})$ *for each real prime* v *of* K*, and let* r_2 *denote the number of complex primes of* K*. Then*

$$\sum_{i=0}^{2}(-1)^i \mathrm{corank}_\Lambda\big(H^i(K_\Sigma/K, \mathcal{D})\big) = -\delta_\Lambda(K, \mathcal{D})$$

where $\delta_\Lambda(K, \mathcal{D}) = r_2 m + \sum_{v \text{ real}} m_v^-$.

For $i \geq 3$, we have $H^i(K_\Sigma/K, \mathcal{D}) = 0$ except possibly when $p = 2$. In fact, the global-to-local restriction maps induces an isomorphism for $i \geq 3$

$$H^i(K_\Sigma/K, \mathcal{D}) \cong \prod_{v|\infty} H^i(K_v, \mathcal{D})$$

(See [NSW], (8.6.13, *ii*).) This justifies our remark in the introduction that $Ш^i(K, \Sigma, \mathcal{D}) = 0$ for $i \geq 3$. The right-hand side is trivial if p is an odd prime. But suppose that $p = 2$. In that case, if $v|\infty$, then $H^i(K_v, \mathcal{D})$ is of exponent 2 and hence can be regarded as a module over $\Lambda/(2)$ for any such v. Thus, if Λ has characteristic 0, then $H^i(K_\Sigma/K, \mathcal{D})$ is a cotorsion Λ-module for $i \geq 3$. However, if Λ is a formal power series ring over $\mathbb{F}_2$, then $H^i(K_\Sigma/K, \mathcal{D})$ can have positive Λ-rank.

We will also state a formula for a local Euler-Poincaré characteristic for every non-archimedean prime v of K. The cofinitely generated Λ-module $\mathcal{D}$ is just assumed to have a Λ-linear action of G_{K_v}.

Proposition 4.2. *Let* $m = \mathrm{corank}_\Lambda(\mathcal{D})$. *Let v be any non-archimedean prime of K.*

(a) If v lies over p, then $\sum_{i=0}^{2}(-1)^i \mathrm{corank}_\Lambda\big(H^i(K_v, \mathcal{D})\big) = -m[K_v : \mathbb{Q}_p]$.

(b) If v does not lie over p, then $\sum_{i=0}^{2}(-1)^i \mathrm{corank}_\Lambda\big(H^i(K_v, \mathcal{D})\big) = 0$.

Both of these propositions will be proved by a specialization argument, reducing to the case where the Krull dimension of Λ is 1. That case is then rather easy, derived from the Poitou-Tate formula for the Euler-Poincaré characteristic of a finite Galois module. The Euler-Poincaré characteristic is additive for an exact sequence $0 \to \mathcal{D}_1 \to \mathcal{D}_2 \to \mathcal{D}_3 \to 0$. For any $\mathcal{D}$, we let $\mathcal{D}_{\Lambda-\mathrm{div}}$ denote its maximal Λ-divisible Λ-submodule. Then $\mathcal{D}/\mathcal{D}_{\Lambda-\mathrm{div}}$ is Λ-cotorsion. Also, the Euler-Poincaré characteristic for a Λ-cotorsion module is 0. Thus, we can assume for the proof that $\mathcal{D}$ is Λ-divisible. The proofs of the two propositions are virtually the same and so we will just give the proof of proposition 4.1.

Proof. If the Krull dimension of Λ is 1, then either $\Lambda = \mathbb{Z}_p$ or $\Lambda = \mathbb{F}_p[[T]]$. In the first case, the result is known. One determines the $\mathbb{Z}_p$-corank by reducing to the case of the finite modules $\mathcal{D}[p^n],\ n \geq 0$. In the second case, the argument would be similar, reducing to the case of the finite modules $\mathcal{D}[T^n],\ n \geq 0$. If the Krull dimension is at least 2, then there are infinitely many prime ideals P of height 1 such that (Λ/P) is also a formal power series ring, but with Krull dimension reduced by 1. By remark 2.1.3, we can choose such a P so that $\mathrm{corank}_{\Lambda/P}(\mathcal{D}[P]) = \mathrm{corank}_\Lambda(\mathcal{D})$ and $\mathrm{corank}_{\Lambda/P}(\mathcal{D}[P]^{G_{K_v}}) = \mathrm{corank}_\Lambda(\mathcal{D}^{G_{K_v}})$ for all archimedean primes v of K. Then $\delta_{\Lambda/P}(K, \mathcal{D}[P]) = \delta_\Lambda(K, \mathcal{D})$ for all such P. By proposition 3.5 and remark 2.1.3, we can also assume that P has the property that $\mathrm{corank}_{\Lambda/P}\big(H^i(G, \mathcal{D}[P])\big) = \mathrm{corank}_\Lambda\big(H^i(G, \mathcal{D})\big)$ for $i = 0, 1$, and 2. Choosing a P with all of these properties reduces the proof of proposition 4.1 to the corresponding result for $\mathcal{D}[P]$ considered as a module over the formal power series ring (Λ/P). By induction, we are done. ■

B. Lower bound on the Λ-corank of $H^1(K_\Sigma/K, \mathcal{D})$. We will derive a lower bound in terms of various local and global H^0's. First we do this for the Λ-corank of $H^2(K_\Sigma/K, \mathcal{D})$. Then applying proposition 4.1 gives a lower bound for the Λ-corank of $H^1(K_\Sigma/K,\mathcal{D})$. The theorems of Poitou-Tate determine the cokernel of the map

$$\gamma : H^2(K_\Sigma/K,\mathcal{D}) \to P^2(K,\Sigma,\mathcal{D})$$

where $P^2(K,\Sigma,\mathcal{D}) = \prod_{v\in\Sigma} H^2(K_v,\mathcal{D})$. Usually these theorems are stated for finite Galois modules. See [NSW], (8.6.13, *i*) for a complete statement in this case. But $\mathcal{D}$ is a direct limit of the finite Galois modules $\mathcal{D}[\mathfrak{m}^n]$ as $n\to\infty$, and one can therefore extend these theorems easily. In particular, we have

$$\operatorname{coker}(\gamma) \cong H^0(K_\Sigma/K,\mathcal{T}^*)^\wedge, \tag{6}$$

where $\mathcal{T}^* = \operatorname{Hom}(\mathcal{D},\mu_{p^\infty})$. This module is the inverse limit of the finite Galois modules $\operatorname{Hom}(\mathcal{D}[\mathfrak{m}_\Lambda^n],\mu_{p^\infty})$ as $n\to\infty$. One can also extend Tate's local duality theorem ([NSW], (7.2.6)), usually stated for finite Galois modules, to $\mathcal{D}$ obtaining, for example, the isomorphisms $H^2(K_v,\mathcal{D}) \cong H^0(K_v,\mathcal{T}^*)^\wedge$ for every non-archimedean prime v of K. When Λ has characteristic 2, it is also necessary to consider the real archimedean primes since $H^2(K_v,\mathcal{D})$ could then have a positive Λ-corank. If v is such a prime, then the Pontryagin dual of $H^2(K_v,\mathcal{D})$ is $\widehat{H}^0(K_v,\mathcal{T}^*) = (\mathcal{T}^*)^{G_{K_v}}/(1+\sigma_v)\mathcal{T}^*$, where σ_v is the nontrivial element of G_v.

We will use the following abbreviations for various ranks and coranks over Λ. For $i\geq 0$, let $h_i(K_\Sigma/K,\mathcal{D}) = \operatorname{corank}_\Lambda\big(H^i(K_\Sigma/K,\mathcal{D})\big)$. If $i=0$, we will usually write K in place of K_Σ/K since the group is then just the G_K-invariant elements. We let $h_0(K,\mathcal{T}^*)$ and $h_0(K_v,\mathcal{T}^*)$ denote the Λ-ranks of $H^0(K,\mathcal{T}^*)$ and $H^0(K_v,\mathcal{T}^*)$, respectively. If v is archimedean, we will let $\widehat{h}_0(K_v,\mathcal{T}^*)$ denote the Λ-rank of $\widehat{H}^0(K_v,\mathcal{T}^*)$. With this notation, we get the following lower bound for $\operatorname{corank}_\Lambda\big(H^2(K_\Sigma/K,\mathcal{D})\big)$:

$$h_2(K_\Sigma/K,\mathcal{D}) \;\geq\; \sum_{v\mid\infty}\widehat{h}_0(K_v,\mathcal{T}^*) \;+\; \sum_{v\in\Sigma,\,v\nmid\infty} h_0(K_v,\mathcal{T}^*) \;-\; h_0(K,\mathcal{T}^*) \tag{7}$$

Equality occurs precisely when $\text{Ш}^2(K,\Sigma,\mathcal{D}) = \ker(\gamma)$ has Λ-corank equal to 0.

The terms in the quantity $\delta_\Lambda(K,\mathcal{D})$ (defined in proposition 4.1) are mostly Λ-ranks of H^0's. For a complex prime v, one obviously has $m = h_0(K_v,\mathcal{T}^*)$. For a real prime v, one sees easily that $m_v^- = h_0(K_v,\mathcal{T}^*)$ if the characteristic of Λ is not 2. This is not necessarily so if Λ has characteristic 2. However, in all cases, one has the following result.

Proposition 4.3. *Let* $b_\Lambda^1(K,\Sigma,\mathcal{D}) = h_0(K,\mathcal{D}) + \sum_{v\in\Sigma} h_0(K_v,\mathcal{T}^*) - h_0(K,\mathcal{T}^*)$. *Then we have the inequality* $h_1(K_\Sigma/K,\mathcal{D}) \;\geq\; b_\Lambda^1(K,\Sigma,\mathcal{D})$. *Equality holds if and only if* $\text{Ш}^2(K,\Sigma,\mathcal{D})$ *is* Λ*-cotorsion.*

Of course, one can similarly define all the quantities in terms of R-ranks and coranks. The corresponding lower bound will be denoted by $b_R^1(K,\Sigma,\mathcal{D})$.

Proof. Assume first that either p is odd or, if $p=2$, that Λ has characteristic 0. Note that the sum is over all $v \in \Sigma$, finite and infinite. The contribution to this sum from the infinite primes is just $\delta_\Lambda(K, \mathcal{D})$. Indeed, each complex prime contributes an m. To check the contribution when v is a real prime, let σ_v be a generator of G_v. Let $\beta_v = 1 + \sigma_v$, the norm map. Then $(\mathcal{T}^*)^{G_{K_v}}/\beta_v\mathcal{T}^*$ has exponent 2 and is therefore a torsion Λ-module. Hence $(\mathcal{T}^*)^{G_{K_v}}$ and $\beta_v\mathcal{T}^*$ have the same Λ-ranks. Since σ_v acts by inversion on μ_{p^∞}, $\beta_v\mathcal{T}^*$ is the Pontryagin dual of $\mathcal{D}/\mathcal{D}^{G_{K_v}}$ as a Λ-module. Thus, the contribution from v will be m_v^-. It follows that the contribution from the infinite primes is just $\delta_\Lambda(K, \mathcal{D})$ and so the stated inequality then follows from proposition 4.1 together with (7). The fact that $\widehat{h}_0(K_v, \mathcal{T}^*) = 0$ implies that equality holds if and only if it holds in (7) and that is equivalent to the vanishing of the Λ-corank of $\text{Ш}^2(K, \Sigma, \mathcal{D})$.

Now assume that Λ has characteristic 2. For the complex primes and finite primes, everything is the same as before. If v is a real prime, then it is still true that $\beta_v\mathcal{T}^*$ is the Pontryagin dual of $\mathcal{D}/\mathcal{D}^{G_{K_v}}$ as a Λ-module. Thus, the Λ-rank of $\beta_v\mathcal{T}^*$ is m_v^-. It follows that $h_0(K_v, \mathcal{T}^*) = m_v^- + \widehat{h}_0(K_v, \mathcal{T}^*)$. Using that observation, the inequality in proposition 4.3 follows from proposition 4.1 and (7). Equality is again equivalent to the validity of hypothesis L. ■

Remark 4.3.1. One can express all the quantities occurring in the inequality of the above proposition in terms of the discrete Λ-modules $\mathcal{D}$ and $\mathcal{D}^* = \mathcal{T}^* \otimes_\Lambda \widehat{\Lambda}$. Then we have $h_0(K_v, \mathcal{T}^*) = \text{corank}_\Lambda\big(H^0(K_v, \mathcal{D}^*)\big)$ for each $v \in \Sigma$ and $h_0(K, \mathcal{T}^*) = \text{corank}_\Lambda\big(H^0(K, \mathcal{D}^*)\big)$. These equalities follow from proposition 3.10 or remark 3.10.1. Note that G_{K_v} is topologically finitely generated and that the action of $\text{Gal}(K_\Sigma/K)$ on $\mathcal{T}^*$ factors through a quotient group G satisfying that property.

In theorem 1, we assume that $H^0(K_{v_o}, \mathcal{T}^*) = 0$ for at least one non-archimedean $v_o \in \Sigma$. Since $\mathcal{T}^*$ is torsion-free Λ-module in that theorem, an equivalent assumption would be that $h_0(K_v, \mathcal{T}^*) = 0$ for some such v_o. Note that this assumption obviously implies that $H^0(K, \mathcal{T}^*) = 0$ or, equivalently, that $h_0(K, \mathcal{T}^*) = 0$.

C. The coranks of Ш^1 and Ш^2. Another part of the Poitou-Tate duality theorems gives a perfect pairing between Ш^2 for a finite Galois module A and Ш^1 for the *"Kummer dual"* $A^* = \text{Hom}(A, \mu_N)$, where $N = |A|$. See [NSW], (8.6.8). Taking direct and inverse limits gives a perfect pairing between $\text{Ш}^2(K, \Sigma, \mathcal{D})$ and $\text{Ш}^1(K, \Sigma, \mathcal{T}^*)$. As discussed in the introduction, both groups might be zero in important cases. We prefer to consider Ш^1 for a discrete module $\mathcal{D}^*$, but this may often be nonzero even if $\text{Ш}^1(K, \Sigma, \mathcal{T}^*) = 0$. We can only prove a relationship between the Λ-coranks. It is not even quite clear how one should define $\mathcal{D}^*$. We have some freedom because the Λ-corank of Ш^i is not changed by a Λ-isogeny of the coefficient module, as we show below. For the purpose of the following proposition, we define $\mathcal{D}^* = \mathcal{T}^* \otimes_\Lambda \widehat{\Lambda}$, although this may differ from $\mathcal{D}^*$, as defined in the introduction, by a Λ-isogeny.

Proposition 4.4. *The Λ-coranks of $\text{Ш}^2(K,\Sigma,\mathcal{D})$ and $\text{Ш}^1(K,\Sigma,\mathcal{D}^*)$ are equal.*

We will use the following lemma which is the analogue of proposition 3.5 for Ш^i.

Lemma 4.4.1. *Suppose that $\mathcal{D}$ is a cofinitely generated Λ-module. Let $i \geq 1$. Then, for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, both the kernel and the cokernel of the map*

$$\text{Ш}^i(K,\Sigma,\mathcal{D}[P]) \longrightarrow \text{Ш}^i(K,\Sigma,\mathcal{D})[P]$$

will be cotorsion as (Λ/P)-modules. Hence $\text{Ш}^i(G,\mathcal{D}[P])$ and $\text{Ш}^i(G,\mathcal{D})[P]$ will have the same (Λ/P)-coranks.

Proof. Applying proposition 3.5 to the global and local cohomology groups shows that the kernels and cokernels of the maps

$$H^i(K_\Sigma/K,\mathcal{D}[P]) \longrightarrow H^i(K_\Sigma/K,\mathcal{D})[P], \quad P^i(K,\Sigma,\mathcal{D}[P]) \longrightarrow P^i(K,\Sigma,\mathcal{D})[P]$$

are Λ-cotorsion for all but finitely many P's of height 1. A straightforward application of the snake lemma implies the result. One uses the fact that the kernels of both maps and the cokernel of the first map are Λ-cotorsion. ■

Now we show that the Λ-corank of Ш^i is unchanged by Λ-isogenies. Assume that $\mathcal{D}_1$ and $\mathcal{D}_2$ are cofinitely generated Λ-modules with a Λ-linear action of $\mathrm{Gal}(K_\Sigma/K)$ and that $\phi : \mathcal{D}_1 \to \mathcal{D}_2$ is a $\mathrm{Gal}(K_\Sigma/K)$-equivariant Λ-isogeny. Then ϕ induces maps on both the global and local cohomology groups and one has a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \text{Ш}^i(K,\Sigma,\mathcal{D}_1) \arrow[r] \arrow[d, dashed, "\alpha"] & H^i(K_\Sigma/K,D_1) \arrow[r] \arrow[d, "\kappa"] & P^i(K,\Sigma,\mathcal{D}_1) \arrow[d, "\lambda"] \\
0 \arrow[r] & \text{Ш}^i(K,\Sigma,\mathcal{D}_2) \arrow[r] & H^i(K_\Sigma/K,D_2) \arrow[r, "\sigma"] & P^i(K,\Sigma,\mathcal{D}_2)
\end{tikzcd}$$

The maps κ and λ are Λ-isogenies. It is clear that the image of $\text{Ш}^i(K,\Sigma,\mathcal{D}_1)$ under the map κ is contained in the kernel of σ and so the map α corresponding to the dashed arrow making the diagram commutative does exist. The fact that κ and λ are Λ-isogenies implies that α is a Λ-isogeny.

Let $s_2 = \mathrm{corank}_\Lambda\big(\text{Ш}^2(K,\Sigma,\mathcal{D})\big)$, $s_1^* = \mathrm{corank}_\Lambda\big(\text{Ш}^1(K,\Sigma,\mathcal{D}^*)\big)$. We prove the equality by induction. If the Krull dimension of Λ is 1, then proposition 4.4 is, as before, rather straightforward to derive from the Poitou-Tate duality theorems for finite Galois modules. In that case, let $\mathcal{V} = \mathcal{T} \otimes_\Lambda \mathcal{L}$, $\mathcal{V}^* = \mathcal{T}^* \otimes_\Lambda \mathcal{L}$, where $\mathcal{L}$ is the fraction field for Λ. Thus, $\mathcal{L} = \mathbb{Q}_p$ or $\mathcal{L} = \mathbb{F}_p((T))$. One then verifies that $s_2 = \dim_{\mathcal{L}}\big(\text{Ш}^2(K,\Sigma,\mathcal{V})\big)$ and $s_1^* = \dim_{\mathcal{L}}\big(\text{Ш}^1(K,\Sigma,\mathcal{V}^*)\big)$. Also, the duality theorem asserts that $\text{Ш}^2(K,\Sigma,\mathcal{V})$ and $\text{Ш}^1(K,\Sigma,\mathcal{V}^*)$ are dual vector spaces, and so the equality $s_2 = s_1^*$ follows.

If the Krull dimension d of Λ is at least 2, we reduce to the case of Krull dimension $d-1$ by using remark 2.1.3 and the above lemma. These imply that $s_2 = \mathrm{corank}_{\Lambda/P}\big(\text{Ш}^2(K,\Sigma,\mathcal{D}[P])\big)$ and $s_1^* = \mathrm{corank}_{\Lambda/P}\big(\text{Ш}^1(K,\Sigma,\mathcal{D}^*[P])\big)$ for all but finitely many P of height 1. We may assume, inductively, that $s_2 = \mathrm{corank}_{\Lambda/P}\big(\text{Ш}^1(K,\Sigma,\mathcal{D}[P]^*)\big)$. We can also assume that $\mathcal{D}$ is Λ-divisible, replacing $\mathcal{D}$ by its maximal Λ-divisible submodule if necessary. This doesn't change s_2. Then $\mathcal{T}^*$ will be a torsion-free Λ-module. Also, $\mathcal{D}^*$ and s_1^* will be unchanged.

To prove that $s_1^* = s_2$, it is now enough to show that $\mathcal{D}^*[P]$ is (Λ/P)-isogenous to $\mathcal{D}[P]^*$. Now $\mathrm{Hom}(\mathcal{D}[P],\mu_{p^\infty})$ is isomorphic to $\mathcal{T}^*/P\mathcal{T}^*$ and so, by definition,

$$\mathcal{D}[P]^* \cong (\mathcal{T}^*/P\mathcal{T}^*) \otimes_{\Lambda/P} \widehat{(\Lambda/P)}$$

According to (3), we therefore have a surjective map $\mathcal{D}[P]^* \to \mathcal{D}^*[P]$. The remark following (3) implies that this map is actually a (Λ/P)-isogeny. ■

The most interesting case is as described in the introduction. A somewhat different proof of proposition 4.4 works nicely in that case, which we will sketch here. Assume that $\mathcal{T}$ is a free R-module and that $\mathcal{D} = \mathcal{T} \otimes_R \widehat{R}$. As above, let $\mathcal{T}^* = \mathrm{Hom}(\mathcal{D},\mu_{p^\infty})$. We now take $\mathcal{D}^* = \mathcal{T}^* \otimes \widehat{R}$. Then, one can verify that $\mathcal{D}^*$ is canonically isomorphic to $\mathrm{Hom}(\mathcal{T},\mu_{p^\infty})$. Hence the theorems of Poitou and Tate can be applied to the dual pair $\mathcal{D}^*$ and $\mathcal{T}$.

One can define $\text{Ш}^2(K,\Sigma,\mathcal{T})$ for the compact R-module $\mathcal{T}$ as the kernel of the homomorphism

$$\gamma_{cpt} : H^2_{cts}(K_\Sigma,\mathcal{T}) \longrightarrow P^2_{cts}(K,\Sigma,\mathcal{T})$$

where $P^2(K,\Sigma,\mathcal{T}) = \prod_{v\in\Sigma} H^2_{cts}(K_v,\mathcal{T})$. The cokernel of γ_{cpt} is isomorphic to $H^0(K,\mathcal{D}^*)^\wedge$. If one applies proposition 3.10 to all the global and local terms, one deduces that the R-rank of $\ker(\gamma_{cpt})$ is equal to the R-corank of $\ker(\gamma)$. That is,

$$\mathrm{rank}_R\big(\text{Ш}^2(K,\Sigma,\mathcal{T})\big) \;=\; \mathrm{corank}_R\big(\text{Ш}^2(K,\Sigma,\mathcal{D})\big)$$

Now $\text{Ш}^1(K,\Sigma,\mathcal{D}^*)$ is isomorphic to the Pontryagin dual of $\text{Ш}^2(K,\Sigma,\mathcal{T})$ as an R-module and so its R-corank must indeed be equal to the R-corank of $\text{Ш}^2(K,\Sigma,\mathcal{D})$.

5 Local Galois cohomology groups.

Suppose that v is a prime of K and that p is any prime number. We assume that $\mathcal{D}$ is a cofinitely generated Λ-module with a Λ-linear action of G_{K_v}. Let $\mathcal{T}^* = \mathrm{Hom}(\mathcal{D},\mu_{p^\infty})$. We will consider first the local H^2 and then various properties for the local H^1. Most results will be for non-archimedean primes. We discuss the archimedean primes at the end of this section.

A. The structure of $H^2(K_v,\mathcal{D})$. If v is non-archimedean, then it is known that the p-cohomological dimension of G_{K_v} is equal to 2. (See theorem (7.1.8) in [NSW].) Proposition 3.3 therefore has the following immediate consequence:

Proposition 5.1. *Let v be a non-archimedean prime of K. If $\mathcal{D}$ is Λ-divisible, then $H^2(K_v, \mathcal{D})$ is Λ-divisible. If $\mathcal{D}$ is Λ-coreflexive, then $H^2(K_v, \mathcal{D})$ is Λ-coreflexive.*

The fact that the Λ-module $H^2(K_v, \mathcal{D})$ is coreflexive when $\mathcal{D}$ is coreflexive can also be seen as follows. Since the Λ-module $\mathcal{T}^*$ is reflexive, it follows that $(\mathcal{T}^*)^{G_{K_v}}$ is also reflexive, as observed in section 2, part C. But the Pontryagin dual of $(\mathcal{T}^*)^{G_{K_v}} = H^0(K_v, \mathcal{T}^*)$ is $H^2(K_v, \mathcal{D})$.

Remark 5.1.1. It is not difficult to give an example where $H^2(K_v, \mathcal{D})$ fails to be Λ-cofree even if $\mathcal{D}$ is assumed to be Λ-cofree. This is based on the example described in remark 2.6.3. We will use the same notation. There we exhibited a reflexive, but non-free, Λ-submodule Y of $X = \Lambda^r$ for some r assuming that the Krull dimension of Λ is at least 3. Suppose that $\Lambda = \mathbb{Z}_p[[T_1, T_2]]$. Recall that Y was the kernel of a Λ-module homomorphism $X \to Z$ where Z was torsion-free and of rank 1. If we choose any injective Λ-module homomorphism $Z \to X$, then we can regard Y as the kernel of a Λ-module homomorphism $\tau : X \to X$. Choose a basis for the Λ-module X. We will identify τ with the corresponding matrix. Multiplying τ by an element of Λ, if necessary, we can assume that τ has entries in $\mathfrak{m}_\Lambda$. The kernel will still be Y. Thus, $\sigma = 1 + \tau$ will be an invertible matrix over Λ. The closed subgroup $\overline{<\sigma>}$ of $GL_r(\Lambda)$ generated topologically by σ will be a pro-p group, either isomorphic to $\mathbb{Z}_p$ or to a finite cyclic group of p-power order. In either case, we can easily define a continuous, surjective homomorphism $G_{K_v} \to \overline{<\sigma>}$. Thus, G_{K_v} acts Λ-linearly on X. If we let $\mathcal{D} = \mathrm{Hom}(X, \mu_{p^\infty})$, then $\mathcal{D}$ has the desired properties. Note that this example arises from a representation of G_{K_v} over Λ of rank r. It is also easy to arrange for this representation to be the restriction to G_{K_v} of such a representation of $\mathrm{Gal}(K_\Sigma/K)$ if $v \in \Sigma$.

The next result holds for any prime of K, archimedean or non-archimedean.

Proposition 5.2. *Let v be any prime of K. Let $\mathcal{D}$ be a cofinitely generated Λ-module. Assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is Λ-reflexive. For almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, the map*

$$H^2(K_v, \mathcal{D}[P]) \to H^2(K_v, \mathcal{D})$$

is injective.

Proof. First assume that v is non-archimedean. We take P to be a prime ideal of height 1 in Λ. To prove injectivity of the map in question, we consider the adjoint map on the Pontryagin duals: $H^0(K_v, \mathcal{T}^*) \longrightarrow H^0(K_v, \mathcal{T}^*/P\mathcal{T}^*)$. If we let $X = \mathcal{T}^*$, then we must prove that the map $X^{G_{K_v}} \longrightarrow (X/PX)^{G_{K_v}}$ is surjective for all but finitely many P's. Let $Y = X^{G_{K_v}}$, the Pontryagin dual of $H^2(K_v, \mathcal{D})$.

According to proposition 3.5, both the kernel and cokernel of the map in question will be (Λ/P)-cotorsion for all but finitely many P's. Therefore, the same will be true for the adjoint map $Y/PY \to (X/PX)^{G_{K_v}}$. Let $Z = X/Y$. By assumption, Z is a reflexive Λ-module. Now we have an exact sequence of (Λ/P)-modules:

$$0 \to Y/PY \to X/PX \to Z/PZ \to 0 \tag{8}$$

and the image of $(X/PX)^{G_{K_v}}$ in Z/PZ is (Λ/P)-torsion. Since Z/PZ is a torsion-free (Λ/P)-module, it is clear that this image must be trivial, i.e. the map $Y/PY \to (X/PX)^{G_{K_v}}$ is surjective as we needed to prove.

Suppose now that v is a real prime of K. We again must prove the surjectivity of the adjoint map: $\widehat{H}^0(K_v, \mathcal{T}^*) \longrightarrow \widehat{H}^0(K_v, \mathcal{T}^*/P\mathcal{T}^*)$, involving the modified H^0's. But these Λ-modules are quotients of the Λ-modules $H^0(K_v, \mathcal{T}^*)$ and $H^0(K_v, \mathcal{T}^*/P\mathcal{T}^*)$ considered above. It follows that the adjoint maps will again be surjective for all but finitely many $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. ■

Remark 5.2.1. The assumption that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is a reflexive Λ-module is important. In the notation of the above proof, let's assume that $X = \mathcal{T}^*$ is itself reflexive, but that $Z = X/Y$ is not. Thus, the Krull dimension of Λ is at least 2. Let $\widetilde{Z}$ be the reflexive hull of the torsion-free Λ-module Z. Then $U = \widetilde{Z}/Z$ is nonzero. Corollary 2.5.1 asserts that there are infinitely many prime ideals $P = (\pi)$ of Λ such that $U[P] = U$. Since U is pseudo-null as a Λ-module, U is then a torsion (Λ/P)-module. Multiplication by π induces an isomorphism $U = \widetilde{Z}/Z \to \pi\widetilde{Z}/\pi Z$ which is a (Λ/P)-submodule of Z/PZ. Also, $Z/\pi\widetilde{Z}$ is a submodule of the (Λ/P)-module $\widetilde{Z}/\pi\widetilde{Z}$, which is torsion-free by proposition 2.6. Thus, the maximal torsion (Λ/P)-submodule of Z/PZ is isomorphic to U. Let $Z' = \pi\widetilde{Z}$ and let X' be the inverse image in X of Z' under the surjective map $X \to Z$. Then $Z'/PZ \cong U$ and we have an exact sequence derived from (8)

$$0 \to Y/PY \to X'/PX \to Z'/PZ \to 0$$

Since X/PX is a torsion-free (Λ/P)-module (by proposition 2.6) and the image of Y/PY is contained in $(X/PX)^{G_{K_v}}$, it follows that $X'/PX \subset (X/PX)^{G_{K_v}}$. Furthermore, if we exclude only finitely many P's, we can then assume that the (Λ/P)-ranks of Y/PY and $(X/PX)^{G_{K_v}}$ are both equal to $\mathrm{rank}_\Lambda(Y)$. Then we have $X'/PX = (X/PX)^{G_{K_v}}$. It follows that the map $Y \to (X/PX)^{G_{K_v}}$ will not be surjective for such P's. The cokernel will be isomorphic to U. These considerations imply the following statement.

If $\mathcal{T}^*$ is reflexive, but $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is not reflexive as Λ-modules, then there exist infinitely many prime ideals $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ such that the map $H^2(K_v, \mathcal{D}[P]) \to H^2(K_v, \mathcal{D})$ has a nonzero kernel.

The kernel of the map will be isomorphic to $\widehat{U}$ for infinitely many P's.

B. Almost divisibility of $H^1(K_v, \mathcal{D})$. Proposition 3.7 has the following consequence.

Proposition 5.3. *Suppose that v is a non-archimedean prime. If $\mathcal{D}$ is Λ-coreflexive and $H^2(K_v, \mathcal{D}) = 0$, then $H^1(K_v, \mathcal{D})$ is an almost divisible Λ-module.*

Here is a more general result. It follows from proposition 5.2 together with proposition 3.6.

Proposition 5.4. *Suppose that v is any prime of K. Assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is reflexive as a Λ-module. If $\mathcal{D}$ is an almost divisible Λ-module, then $H^1(K_v, \mathcal{D})$ is an almost divisible Λ-module.*

Remark 5.2.1 makes it clear that the assumption concerning $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is crucial. The following proposition makes this more precise when $\mathcal{D}$ is Λ-coreflexive and v is non-archimedean.

Proposition 5.5. *Let v be a non-archimedean prime. Assume that $\mathcal{D}$ is a coreflexive Λ-module. Then the maximal pseudo-null Λ-submodule of $H^1(K_v, \mathcal{D})^\wedge$ is isomorphic to $\widetilde{Z}/Z$, where $\widetilde{Z}$ denotes the reflexive hull of the Λ-module $Z = \mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$.*

Proof. Let $U = \widetilde{Z}/Z$. Let U' denote the maximal pseudo-null Λ-submodule of $H^1(K_v, \mathcal{D})^\wedge$. There is nothing to prove unless Λ has Krull dimension at least 2. Applying corollary 2.5.1 to the pseudo-null Λ-module $U \times U'$, we see that there exist prime ideals $P = (\pi)$ of Λ such that $\pi U = 0$ and $\pi U' = 0$. We can also assume that P is not an associated prime for the Λ-torsion submodule of $H^1(K_v, \mathcal{D})^\wedge$. It follows that $H^1(K_v, \mathcal{D})^\wedge[P] = U'$. We therefore have an isomorphism

$$H^1(K_v, \mathcal{D})/\pi H^1(K_v, \mathcal{D}) \cong \ker\big(H^2(K_v, \mathcal{D}[P]) \longrightarrow H^2(K_v, \mathcal{D})[P]\big)$$

since $\mathcal{D}$ is assumed to be Λ-divisible. The choice of P implies that the first group is precisely the Pontryagin dual of U' and, as explained in remark 5.2.1, the second group is the Pontryagin dual of U. Thus, indeed, $U \cong U'$. ■

C. Divisibility of $H^1(K_v, \mathcal{D})$. It is rather common for $H^1(K_v, \mathcal{D})$ to be a divisible Λ-module. Proposition 3.3 gives sufficient conditions. The assumption that $H^2(K_v, \alpha) = 0$ for a G_{K_v}-irreducible subquotient α of the $\mathbb{F}_p$-representation space $\mathcal{D}[\mathfrak{m}_\Lambda]$ means that $H^0(K_v, \mathrm{Hom}(\alpha, \mu_p)) = 0$, or, equivalently, that $\alpha \ncong \mu_p$. Thus, we need just assume that μ_p is not a subquotient of $\mathcal{D}[\mathfrak{m}_\Lambda]$ for the action of G_{K_v} to apply that proposition.

Proposition 5.6. *Suppose that v is non-archimedean. Assume that μ_p is not a G_{K_v}-subquotient of $\mathcal{D}[\mathfrak{m}_\Lambda]$ and that $\mathcal{D}$ is Λ-divisible. Then $H^1(K_v, \mathcal{D})$ is Λ-divisible.*

Even if μ_p is a subquotient of $\mathcal{D}[\mathfrak{m}_\Lambda]$, one can prove divisibility under other assumptions. Here is one such result.

Proposition 5.7. *Suppose that v is non-archimedean. Assume that $\mathcal{D}$ is Λ-coreflexive. Let $\mathcal{D}^* = \mathcal{T}^* \otimes_\Lambda \widehat{\Lambda}$. Assume that $H^0(K_v, \mathcal{D}^*)$ is a co-pseudo-null Λ-module. Then $H^1(K_v, \mathcal{D})$ is a divisible Λ-module.*

Note that the assumption about $H^0(K_v, \mathcal{D}^*)$ implies that $H^0(K_v, \mathcal{T}^*) = 0$ according to proposition 3.10, and hence that $H^2(K_v, \mathcal{D}) = 0$. Therefore, we already know that $H^1(K_v, \mathcal{D})$ is an almost divisible Λ-module.

Proof. Let $P = (\pi)$ be any prime ideal of Λ of height 1. Since $H^2(K_v, \mathcal{D}) = 0$, we must show that $H^2(K_v, \mathcal{D}[P]) = 0$ in order to conclude that $H^1(K_v, \mathcal{D})$ is divisible by π. (See (6) for $I = P$, $i = 2$.) Now $\mathcal{D}[P]$ is (Λ/P)-divisible and hence so is $H^2(K_v, \mathcal{D}[P])$. It therefore suffices to prove that its (Λ/P)-corank is 0. The Pontryagin dual of this group is $(\mathcal{T}^*/P\mathcal{T}^*)^{G_{K_v}}$. By proposition 3.10, the rank of this (Λ/P)-module is equal to the corank of the (Λ/P)-module $\big((\mathcal{T}^*/P\mathcal{T}^*) \otimes_{\Lambda/P} (\widehat{\Lambda/P})\big)^{G_{K_v}}$. As pointed out at the end of section 2, part E, the map $(\mathcal{T}^*/P\mathcal{T}^*) \otimes_{\Lambda/P} (\widehat{\Lambda/P}) \to \mathcal{D}^*[P]$ is a (Λ/P)-isogeny and so the submodules of G_{K_v}-invariant elements have the same (Λ/P)-coranks. Finally, note that $\mathcal{D}^*[P]^{G_{K_v}} = (\mathcal{D}^*)^{G_{K_v}}[P]$. The (Λ/P)-corank of this module is equal to 0 because the Pontryagin dual of the Λ-module $(\mathcal{D}^*)^{G_{K_v}}$ has no associated prime ideals of height 1. ■

D. Coreflexivity of $H^1(K_v, \mathcal{D})$. Proposition 3.3 immediately gives one simple sufficient condition for coreflexivity.

Proposition 5.8. *Suppose that v is a non-archimedean prime and that μ_p is not a G_{K_v}-subquotient of $\mathcal{D}[\mathfrak{m}_\Lambda]$. If $\mathcal{D}$ is Λ-coreflexive, then $H^1(K_v, \mathcal{D})$ is also Λ-coreflexive.*

A more subtle result is the following.

Proposition 5.9. *Suppose that v is non-archimedean. Assume that $\mathcal{D}$ is Λ-cofree. Let $\mathcal{D}^* = \mathcal{T}^* \otimes_\Lambda \widehat{\Lambda}$. Assume that every associated prime ideal for the Λ-module $H^0(K_v, \mathcal{D}^*)^\wedge$ has height at least 3. Then $H^1(K_v, \mathcal{D})$ is a coreflexive Λ-module.*

Proof. Let d denote the Krull dimension of Λ. Let $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ be fixed. We will denote Λ/P by R' and $\mathcal{D}[P]$ by $\mathcal{D}'$. Thus, $\mathcal{D}'$ is a cofree R'-module. Since P is a principal ideal, the ring R' is a complete intersection and is therefore a Cohen-Macaulay ring. (See section 2.3 in [B-H].) It follows that R' contains a subring Λ' such that: *(i)* Λ' is isomorphic to a formal power series ring and *(ii)* R' is a free, finitely generated Λ'-module. The Krull dimension of Λ' is $d-1$. Note that $\mathcal{D}[P]$ is cofree and hence coreflexive as a Λ'-module. We will apply proposition 5.7 to this Λ'-module. For that purpose, the role of $\mathcal{T}^*$ is played by $\mathcal{T}'^* = \mathcal{T}^*/P\mathcal{T}^*$ and $\mathcal{D}^*$ by $\mathcal{D}'^* = \mathcal{T}'^* \otimes_{\Lambda'} \widehat{\Lambda'}$.

Since $\mathcal{T}^*$ is Λ-free, the discussion at the beginning of section 2, part E, shows that $\mathcal{T}'^* \otimes_{R'} \widehat{R'}$ is isomorphic to $\mathcal{D}^*[P]$ as an R'-module. Since R' is free as a Λ'-module, $\mathcal{T}'^* \otimes_{R'} \widehat{R'}$ is isomorphic to $\mathcal{T}'^* \otimes_{\Lambda'} \widehat{\Lambda'}$ and so $\mathcal{D}'^*$ and $\mathcal{D}^*[P]$ are isomorphic. The isomorphisms are G_{K_v}-equivariant. The assumption about $H^0(K_v, \mathcal{D}^*)$ implies that $H^0(K_v, \mathcal{D}'^*) = H^0(K_v, \mathcal{D}^*)[P]$ is co-pseudo-null as an R'-module, and hence as a Λ'-module. Therefore, proposition 5.7 implies that $H^1(K_v, \mathcal{D}')$ is Λ'-divisible, and hence R'-divisible. That is, $H^1(K_v, \mathcal{D}[P])$ is a divisible (Λ/P)-module.

Now we have a surjective homomorphism $H^1(K_v, \mathcal{D}[P]) \to H^1(K_v, \mathcal{D})[P]$. Therefore, for all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$, the (Λ/P)-module $H^1(K_v, \mathcal{D})[P]$ is also divisible. Corollary 2.6.1 implies that $H^1(K_v, \mathcal{D})$ is indeed coreflexive as a Λ-module. ■

Remark 5.9.2. An example that we have in mind in propositions 5.7 and 5.9 arises from classical Iwasawa theory over the local field K_v. Suppose that $K_{\infty,v}/K_v$ is a $\mathbb{Z}_p^m$-extension where $m \geq 1$. Let $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_{\infty,v}/K_v]]$. If $v \nmid p$, then one can only have $m = 1$, but if $v|p$, then m could be as large as $[K_v : \mathbb{Q}_p] + 1$. If $D = V/T$ is a G_{K_v}-module isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^n$, let $\mathcal{D} = \mathrm{Ind}_{K_{\infty,v}/K_v}(D)$. There is a comparison theorem just as stated in the introduction, but for a local field. We have that $H^0(K_v, \mathcal{D}^*)$ is isomorphic as a Λ-module to $H^0(K_{\infty,v}, D^*) = D^*(K_{\infty,v})$. This module has finite $\mathbb{Z}_p$-corank and is often even finite.

Assume first that $D^*(K_{\infty,v})$ is finite. Then the only associated prime ideal will be $\mathfrak{m}_\Lambda$. In that case, propositions 5.7 and 5.9 imply that $H^1(K_{\infty,v}, D)$ is a divisible Λ-module for $m \geq 1$ and even coreflexive for $m \geq 2$. If $D^*(K_{\infty,v})$ is infinite, then $H^1(K_{\infty,v}, D)$ is Λ-divisible if $m \geq 2$ and Λ-coreflexive if $m \geq 3$.

This is not a new result. See lemma 5.4 in [O-V], which even applies to non-abelian p-adic Lie extensions of a local field. Also, for the case $m = 1$, more precise results can be found in section 3 of [Gr89].

E. Cofreeness of $H^1(K_v, \mathcal{D})$. We can prove cofreeness under suitable assumptions. Let $\mathbb{Z}/p\mathbb{Z}$ denote the one-dimension $\mathbb{F}_p$-vector space with trivial Galois action.

Proposition 5.10. *Suppose that v is a non-archimedean prime and that neither $\mathbb{Z}/p\mathbb{Z}$ nor μ_p are G_{K_v}-subquotients of $\mathcal{D}[\mathfrak{m}_\Lambda]$. If $\mathcal{D}$ is a cofree Λ-module, then $H^1(K_v, \mathcal{D})$ is also a cofree Λ-module.*

Proof. We can apply proposition 3.4 to conclude that the map

$$H^1(K_v, \mathcal{D}[\mathfrak{m}_\Lambda]) \longrightarrow H^1(K_v, \mathcal{D})[\mathfrak{m}_\Lambda]$$

is an isomorphism. The hypothesis about $\mathbb{Z}/p\mathbb{Z}$ nor μ_p means that for every G_{K_v}-irreducible subquotient α of the $\mathbb{F}_p$-representation space $\mathcal{D}[\mathfrak{m}_\Lambda]$, we have $H^0(K_v, \alpha) = H^2(K_v, \alpha) = 0$. Hence, by corollary 3.1.1, it follows that $H^0(K_v, \mathcal{D}) = 0$ and $H^2(K_v, \mathcal{D}) = 0$. We can then apply proposition 4.2 to determine the Λ-corank of $H^1(G_{K_v}, \mathcal{D})$, which will be either equal to 0 if $v \nmid p$ or equal to $[K_v : \mathbb{Q}_p]\mathrm{corank}_\Lambda(\mathcal{D})$ if $v|p$. However, we also have $H^0(K_v, \mathcal{D}[\mathfrak{m}_\Lambda]) = 0$

and $H^2(K_v, \mathcal{D}[\mathfrak{m}_\Lambda]) = 0$. The Euler-Poincaré characteristic formula for the finite G_{K_v}-module $\mathcal{D}[\mathfrak{m}_\Lambda]$ determines the $\mathbb{F}_p$-dimension of $H^1(K_v, \mathcal{D}[\mathfrak{m}_\Lambda])$. It will either equal 0 if $v \nmid p$ or equal $[K_v : \mathbb{Q}_p]\dim_{\mathbb{F}_p}(\mathcal{D}[\mathfrak{m}_\Lambda])$ if $v|p$.

If $\mathcal{D}$ is a cofree Λ-module, then $\operatorname{corank}_\Lambda(\mathcal{D}) = \dim_{\mathbb{F}_p}(\mathcal{D}[\mathfrak{m}_\Lambda])$. Thus, the above observations show that

$$\operatorname{corank}_\Lambda\big(H^1(G_{K_v}, \mathcal{D})\big) = \dim_{\mathbb{F}_p}\big(H^1(K_v, \mathcal{D}[\mathfrak{m}_\Lambda])\big) = \dim_{\mathbb{F}_p}\big(H^1(K_v, \mathcal{D})[\mathfrak{m}_\Lambda]\big)$$

We now use Nakayama's lemma. Let $r = \operatorname{corank}_\Lambda\big(H^1(G_{K_v}, \mathcal{D})\big)$. Let X be the Pontryagin dual of $H^1(G_{K_v}, \mathcal{D})$. Then X is a finitely generated Λ-module of rank r and the minimum number of generators of X is $\dim_{\mathbb{F}_p}(X/\mathfrak{m}_\Lambda X)$, which is also equal to r. Thus, there is a surjective Λ-module homomorphism $\Lambda^r \to X$. Comparing ranks, it is clear that this map is an isomorphism. Thus, X is free and so $H^1(G_{K_v}, \mathcal{D})$ is indeed cofree as a Λ-module. ■

Remark 5.10.1. If $v \nmid p$, then one could just assume that $\mathcal{D}$ is Λ-divisible. The assumption about $\mathbb{Z}/p\mathbb{Z}$ and μ_p implies that $H^i(G_{K_v}, \mathcal{D}) = 0$ for $i = 0$ and $i = 2$. Proposition 4.2 then implies that $H^1(G_{K_v}, \mathcal{D})$ is Λ-cotorsion. By proposition 5.6, $H^1(G_{K_v}, \mathcal{D})$ is also Λ-divisible and so we have $H^1(G_{K_v}, \mathcal{D}) = 0$, which is trivially Λ-cofree.

It is worthwhile to point out that the above proof applies with virtually no change if one assumes that $\mathcal{D}$ is a cofree R-module over a complete Noetherian local domain R. One concludes that, for any non-archimedean v, $H^1(G_{K_v}, \mathcal{D})$ is a cofree R-module under the same hypothesis about $\mathbb{Z}/p\mathbb{Z}$ nor μ_p.

F. Local assumptions *(a)* and *(b)*. Assume now that we are in the situation described in the introduction. Thus, $\mathcal{T}$ is a free R-module of rank n, $\mathcal{D} = \mathcal{D}_R$ is R-cofree, and $\mathcal{T}^*$ is R-free. We have several comments about the important assumption that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is also R-free. For many results proven in this section, it suffices to assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is Λ-reflexive, but we don't know how to verify such an assumption in itself. Freeness is more accessible.

As a first observation, note that if $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is a free R-module, then it follows that $\mathcal{T}^* \cong (\mathcal{T}^*)^{G_{K_v}} \oplus (\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}})$ as R-modules. Hence, $(\mathcal{T}^*)^{G_{K_v}}$ is a projective R-module and therefore must also be free. Let $r = \operatorname{rank}_R\big((\mathcal{T}^*)^{G_{K_v}}\big)$. It follows, furthermore, that the image of $(\mathcal{T}^*)^{G_{K_v}}$ in $\mathcal{T}^*/\mathfrak{m}\mathcal{T}^*$ will have dimension r over the residue field $k = R/\mathfrak{m}$. Conversely, if $(\mathcal{T}^*)^{G_{K_v}}$ is free of rank r and its image in $\mathcal{T}^*/\mathfrak{m}\mathcal{T}^*$ has dimension r, then $(\mathcal{T}^*)^{G_{K_v}}$ will be a direct summand of $\mathcal{T}^*$ and the complementary summand, which is isomorphic to $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ will also be R-free.

An important case to consider is $\mathcal{D} = \operatorname{Ind}_{K_\infty/K}(D)$, where K_∞/K is a $\mathbb{Z}_p^m$-extension and $D = V/T$ is a Galois module isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ for some $n \geq 1$. In this case, T is a free $\mathbb{Z}_p$-module of rank n and $\mathcal{T}^* \cong T^* \otimes_{\mathbb{Z}_p} \Lambda$, a free Λ-module of rank n. We take $R = \Lambda$. The action of $\operatorname{Gal}(K_\Sigma/K)$ on Λ in the tensor product is given by a homomorphism $\kappa : \operatorname{Gal}(K_\Sigma/K) \to \Gamma \to \Lambda^\times$ as described in the introduction. Now if v is a prime of K which splits completely in K_∞/K, including, in particular, all archimedean primes, then $\kappa|_{G_{K_v}}$ is trivial. Thus, the action of G_{K_v} on $\mathcal{T}^*$ is via the first factor T^* in the tensor product. One sees easily that

$$(\mathcal{T}^*)^{G_{K_v}} \cong (T^*)^{G_{K_v}} \otimes_{\mathbb{Z}_p} \Lambda, \quad \mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}} \cong \big(T^*/(T^*)^{G_{K_v}}\big) \otimes_{\mathbb{Z}_p} \Lambda \ .$$

Since $T^*/(T^*)^{G_{K_v}}$ is a torsion-free $\mathbb{Z}_p$-module, it is $\mathbb{Z}_p$-free. This implies that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is indeed a free Λ-module and hence local assumption *(a)* is satisfied if v splits completely. If v doesn't split completely in K_∞/K, then one can use remark 3.10.2 to verify that $(\mathcal{T}^*)^{G_{K_v}} = 0$.

In some cases, assumption *(a)* can be verify by considering just the residual representation $\overline{\rho}$. We illustrate this when $n = 2$. Thus, $\overline{\rho}$ is a 2-dimensional representation over the residue field k. There is nothing to show unless $\mathrm{rank}_R\big((\mathcal{T}^*)^{G_{K_v}}\big) = 1$ and so we assume this is the case. Suppose that $\overline{\rho}|_{G_{K_v}}$ is reducible and that the two $k^\times$-valued characters that occur are distinct. Then the same is true for $\overline{\rho}^*$ and so it follows that the k-subspace $(\mathcal{T}^*/\mathfrak{m}\mathcal{T}^*)^{G_{K_v}}$ of $\mathcal{T}^*/\mathfrak{m}\mathcal{T}^*$ has dimension 1 and that the action of G_{K_v} on the corresponding quotient is by a nontrivial character $\overline{\eta} : G_{K_v} \to k^\times$. One deduces easily that there exists a finite cyclic subgroup Δ of G_{K_v} such that $p \nmid |\Delta|$ and $\overline{\eta}|_\Delta$ is still nontrivial. Considering just the action of Δ on $\mathcal{T}^*$, we see that we have a direct sum decomposition

$$\mathcal{T}^* = (\mathcal{T}^*)^{\eta_o} \oplus (\mathcal{T}^*)^{\eta}$$

as R-modules, where η_o is the trivial character and η is a "lifting" of $\overline{\eta}$, both characters of Δ having values in $R^\times$. Since $(\mathcal{T}^*)^{G_{K_v}} \subseteq (\mathcal{T}^*)^\Delta = (\mathcal{T}^*)^{\eta_o}$ and $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is a torsion-free R-module, it follows that $(\mathcal{T}^*)^{G_{K_v}} = (\mathcal{T}^*)^{\eta_o}$, which is indeed a direct summand, verifying assumption *(a)*.

Note that if G_v acts on $\mathcal{T}^*$ through a finite quotient group Δ whose order is not divisible by p, then one has $(\mathcal{T}^*)^{G_{K_v}} = (\mathcal{T}^*)^\Delta$, which is again obviously a direct summand of $\mathcal{T}^*$. The idempotent e_o for the trivial character η_o of Δ is in the group ring $\mathbb{Z}_p[\Delta]$. One has $(\mathcal{T}^*)^{G_{K_v}} = e_o\mathcal{T}^*$ and the complementary direct summand is $(1 - e_o)\mathcal{T}^*$. In particular, assumption *(a)* is satisfied for archimedean primes if p is odd - an unimportant case because the groups $\widehat{H}^i(K_v, \mathcal{D})$ are then trivial.

Now suppose that v is a real prime of K and that $p = 2$. Otherwise, the corresponding cohomology groups are all trivial. Let σ_v denote the nontrivial element of G_{K_v}. Note that $\sigma_v(\zeta) = \zeta^{-1}$ for $\zeta \in \mu_{p^\infty}$. First assume that R has characteristic 0. Let $\alpha_v = \sigma_v - 1$ which we consider as an R-module endomorphism of $\mathcal{T}^*$. Thus $\ker(\alpha_v) = (\mathcal{T}^*)^{G_{K_v}}$ and so assumption *(a)* is equivalent to the statement that $\mathrm{im}(\alpha_v) = \alpha_v(\mathcal{T}^*)$ is R-free.

Let $\beta_v = \sigma_v + 1$ be the norm map on $\mathcal{T}^*$. The Pontryagin dual of $H^1(K_v, \mathcal{D})$ is $H^1(K_v, \mathcal{T}^*) = \ker(\beta_v)/\mathrm{im}(\alpha_v)$, a consequence of the local duality theorem but also easily verified directly from the definitions of these groups. Assume now that R is a finite, integral extension of Λ and is reflexive. Then $\mathcal{T}^*$ is a reflexive Λ-module. Since $\mathcal{T}^*/\ker(\beta_v)$ is a torsion-free Λ-module, it follows that $\ker(\beta_v)$ is reflexive and that $\mathrm{im}(\alpha_v)$ is reflexive if and only if $\ker(\beta_v)/\mathrm{im}(\alpha_v)$ has no nonzero pseudo-null Λ-submodules. That is, $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is a reflexive Λ-module if and only if $H^1(K_v, \mathcal{D})$ is an almost divisible Λ-module. Since this group has exponent 2, one can simply take $\theta = 2$ in the definition of almost divisibility, which then simply means that $H^1(K_v, \mathcal{D})$ is divisible when considered as a $\Lambda/(2)$-module.

It is easy to give an example where assumption *(a)* is not satisfied. Suppose that $R = \Lambda = \mathbb{Z}_2[[S]]$ and that $\mathcal{T}^* \cong \Lambda^2$. Suppose that σ_v acts on $\mathcal{T}^*$ by the matrix $\begin{bmatrix} -1 & S \\ 0 & 1 \end{bmatrix}$. Then $\mathrm{im}(\alpha_v)$ is isomorphic to $\mathfrak{m}_\Lambda$ and is not reflexive. Note that $H^1(K_v, \mathcal{D}) \cong \Lambda/\mathfrak{m}_\Lambda \cong \mathbb{F}_2$ in this example. We have just specified the action of G_{K_v}, but it is not hard to contrive a global representation ρ over Λ where G_{K_v} acts in this way.

Now assume that R has characteristic 2. Then $\alpha_v = \sigma_v - 1 = \beta_v$ and α_v^2 is the zero-map. We have $H^1(K_v, \mathcal{T}^*) \cong \ker(\alpha_v)/\mathrm{im}(\alpha_v)$. Also, $\mathrm{im}(\alpha_v)$ is the orthogonal complement of $\mathcal{D}^{G_{K_v}}$ under the pairing $\mathcal{D} \times \mathcal{T}^* \to \mu_2$. Therefore, using the notation from the introduction, we have

$$n_v^- = \mathrm{corank}_R(\mathcal{D}/\mathcal{D}^{G_{K_v}}) = \mathrm{rank}_R\big(\mathrm{im}(\alpha_v)\big) \ .$$

If we define $n_v^+ = \mathrm{corank}_R\big(\mathcal{D}^{G_{K_v}}\big)$, then $n = n_v^+ + n_v^-$. Since $\mathrm{im}(\alpha_v) \subseteq \ker(\alpha_v)$, it follows that $n_v^- \le n_v^+$ and $H^1(K_v, \mathcal{T}^*)$ has R-rank equal to $n_v^+ - n_v^-$. Almost anything could occur subject to these constraints. One could simply define α_v so that $\mathrm{im}(\alpha_v) \subseteq \ker(\alpha_v)$. It could be any R-submodule of $\mathcal{T}^*$ which has a generating set of n elements and has R-rank at most $n/2$. This submodule could certainly fail to be R-free or Λ-reflexive. Note that $(1 + \alpha_v)^2$ is the identity map and so we can define an action of G_{K_v} on $\mathcal{T}^*$ (and hence on $\mathcal{D}$) by letting $\sigma_v = 1 + \alpha_v$.

Finally, we will discuss the verification of assumption *(b)*. Suppose that v_o is a non-archimedean prime in Σ. Since $\mathcal{T}^*$ is a torsion-free R-module, so is $(\mathcal{T}^*)^{G_{K_{v_o}}}$. Hence $(\mathcal{T}^*)^{G_{K_{v_o}}} = 0$ if and only if its rank over R is equal to 0. According to remark 3.10.2, we have the inequality

$$\mathrm{rank}_R\big((\mathcal{T}^*)^{G_{K_{v_o}}}\big) \ \le \ \mathrm{rank}_{R_\mathcal{P}}\big((\mathcal{T}^*/\mathcal{P}\mathcal{T}^*)^{G_{K_{v_o}}}\big)$$

for every prime ideal $\mathcal{P}$ of R. Therefore, it suffices to find just one $\mathcal{P}$ such that $(\mathcal{T}^*/\mathcal{P}\mathcal{T}^*)^{G_{K_{v_o}}}$ has $(R/\mathcal{P})$-rank equal to 0, or equivalently, such that $\mathcal{D}^*[\mathcal{P}]^{G_{K_{v_o}}}$ has $(R/\mathcal{P})$-corank equal to 0. For example, this may occur for $\mathcal{P} = \mathfrak{m}$. In that case, one would have $(\mathcal{D}^*)^{G_{K_{v_o}}} = 0$. If the Krull dimension d of R is at least 2, then there are infinitely many prime ideals $\mathcal{P}$ of R of height $d-1$. Then $R/\mathcal{P}$ has Krull dimension 1. If $\mathcal{D}^{G_{K_{v_o}}}$ is indeed R-cotorsion, then remark 2.1.3 implies that $\mathcal{D}[\mathcal{P}]^{G_{K_{v_o}}} = \mathcal{D}^{G_{K_{v_o}}}[\mathcal{P}]$ is finite for infinitely many such $\mathcal{P}$'s. Exhibiting one such $\mathcal{P}$ is sufficient to verify assumption *(b)*.

6 Global Galois cohomology groups.

Assume that $\mathcal{D}$ is a cofinitely generated Λ-module and that $\mathrm{Gal}(K_\Sigma/K)$ acts Λ-linearly on $\mathcal{D}$, where Σ is a finite set of primes of K containing all primes above p and ∞. Let $\mathcal{T}^* = \mathrm{Hom}(\mathcal{D}, \mu_{p^\infty})$. This section will contain the proof of theorem 1. It will be a consequence of somewhat more general theorems. The heart of the matter is to study $H^2(K_\Sigma/K, \mathcal{D})$ and certain Λ-submodules obtained by requiring local triviality at some of the primes in Σ. The almost divisibility assertion in theorem 1 for $H^1(K_\Sigma/K, \mathcal{D})$ will follow easily.

A. The structure of $H^2(K_\Sigma/K, \mathcal{D})$ and certain submodules. Assume first that p is an odd prime. It is then known that $\mathrm{Gal}(K_\Sigma/K)$ has p-cohomological dimension 2 and so propositions 3.3 has the following immediate consequence.

Proposition 6.1. *Assume that p is an odd prime. If $\mathcal{D}$ is Λ-divisible, then $H^2(K_\Sigma/K, \mathcal{D})$ is Λ-divisible. If $\mathcal{D}$ is Λ-coreflexive, then $H^2(K_\Sigma/K, \mathcal{D})$ is Λ-coreflexive.*

We will prove a more general result. The arguments depend on the fundamental commutative diagram below. We assume that $\mathcal{D}$ is a cofinitely generated, divisible Λ-module. Suppose that Σ' is any subset of Σ. We make the following definition:

$$H^i_{\Sigma'}(K_\Sigma/K, \mathcal{D}) = \ker\big(H^i(K_\Sigma/K, \mathcal{D}) \to \prod_{v \in \Sigma'} H^i(K_v, \mathcal{D})\big)$$

for $i \geq 1$. Since $H^i_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ is clearly a Λ-submodule of $H^i(K_\Sigma/K, \mathcal{D})$, it must also be cofinitely generated. Note that if we take $\Sigma' = \Sigma$, then $H^i_{\Sigma'}(K_\Sigma/K, \mathcal{D}) = Ш^i(K, \Sigma, \mathcal{D})$. However, we will now assume from here on that there is at least one non-archimedean prime v_o in Σ which is not in Σ'. Thus Σ' will be a proper subset of Σ. We will also always make the assumption that $\mathcal{D}$ is a cofinitely generated, divisible Λ-module. Here is the fundamental diagram, where we take P to be any prime ideal of Λ of height 1.

$$\begin{tikzcd}
0 \arrow[r] & H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}[P]) \arrow[r] \arrow[d, dashed, "\delta"] & H^2(K_\Sigma/K, \mathcal{D}[P]) \arrow[r, "\sigma"] \arrow[d, "\kappa"] & \prod_{v \in \Sigma'} H^2(K_v, \mathcal{D}[P]) \arrow[r] \arrow[d, "\lambda"] & 0 \\
0 \arrow[r] & H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}) \arrow[r] \arrow[d, "\varphi"] & H^2(K_\Sigma/K, \mathcal{D}) \arrow[r] \arrow[d, "\chi"] & \prod_{v \in \Sigma'} H^2(K_v, \mathcal{D}) \arrow[r] \arrow[d, "\psi"] & 0 \\
0 \arrow[r] & H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}) \arrow[r] \arrow[d, "\epsilon"] & H^2(K_\Sigma/K, \mathcal{D}) \arrow[r] \arrow[d] & \prod_{v \in \Sigma'} H^2(K_v, \mathcal{D}) \arrow[r] \arrow[d] & 0 \\
 & 0 \arrow[r] & H^3(K_\Sigma/K, \mathcal{D}[P]) \arrow[r, "\tau"] & \prod_{v \in \Sigma'} H^3(K_v, \mathcal{D}[P]) \arrow[r] & 0
\end{tikzcd}$$

The 2nd and 3rd columns of maps in this diagram are induced by the exact sequence

$$0 \longrightarrow \mathcal{D}[P] \longrightarrow \mathcal{D} \xrightarrow{\pi} \mathcal{D} \longrightarrow 0$$

where we have chosen a generator π for P. Thus, those columns are certainly exact. The maps φ, χ and ψ are all just multiplication by π. As for the rows, the exactness of the last row is part of the Poitou-Tate theorems. (See [NSW], (8.6.13).) For the other rows, the only issue is the surjectivity of the global-to-local maps. This follows from the following general lemma since we are assuming that $\Sigma - \Sigma'$ contains at least one non-archimedean prime v_o.

Lemma 6.2. *Let v_o be any non-archimedean prime in Σ. Then the map*

$$H^2(K_\Sigma/K, \mathcal{D}) \longrightarrow \prod_{v \in \Sigma, v \neq v_o} H^2(K_v, \mathcal{D})$$

is surjective.

Proof. First consider the case where $\mathcal{D}$, and hence $\mathcal{T}^* = \mathrm{Hom}(\mathcal{D}, \mu_{p^\infty})$, are just finite $\mathrm{Gal}(K_\Sigma/K)$-modules. One has an exact sequence

$$H^2(K_\Sigma/K, \mathcal{D}) \xrightarrow{\gamma} P^2(K, \Sigma, \mathcal{D}) \xrightarrow{\alpha} H^0(K_\Sigma/K, \mathcal{T}^*)^\wedge,$$

where $P^2(K, \Sigma, \mathcal{D}) = \prod_{v \in \Sigma} H^2(K_v, \mathcal{D})$. The map γ is just the global-to-local restriction map. Let $\mathcal{G}$ denote its image. Let $\mathcal{H}_{v_o}$ denote the factor $H^2(K_{v_o}, \mathcal{D})$ in the product $P^2(K, \Sigma, \mathcal{D})$. The assertion to be proved is that $\mathcal{G}\mathcal{H}_{v_o} = P^2(K, \Sigma, \mathcal{D})$. The map α is the adjoint of the "diagonal" map

$$\beta : H^0(K_\Sigma/K, \mathcal{T}^*) \to P^0(K, \Sigma, \mathcal{T}^*)$$

where $P^0(K, \Sigma, \mathcal{T}^*) = \prod_{v | \infty} \widehat{H}^0(K_v, \mathcal{T}^*) \times \prod_{v \in \Sigma, v \nmid \infty} H^0(K_v, \mathcal{T}^*)$. Since $\mathcal{G}$ is the kernel of the map α, its orthogonal complement is the image of β. The orthogonal complement of $\mathcal{H}_{v_o}$ is just the kernel of the natural projection map $\pi_{v_o} : P^0(K, \Sigma, \mathcal{T}^*) \to H^0(K_{v_o}, \mathcal{T}^*)$. The assertion means that the intersection of these orthogonal complements is trivial. Since v_o is non-archimedean, the map $H^0(K_\Sigma/K, \mathcal{T}^*) \to H^0(K_{v_o}, \mathcal{T}^*)$ is injective. That is, the composite map $\pi_{v_o} \circ \beta$ is injective. This implies that $\mathrm{im}(\beta') \cap \ker(\pi_{v_o}) = 0$ which proves the assertion. In general, $\mathcal{D} = \bigcup_{n \geq 0} \mathcal{D}[\mathfrak{m}_\Lambda^n]$, a union of finite Galois modules, and the surjectivity therefore follows in general. ■

It remains to discuss the maps δ and ϵ. Under the assumptions that we are making, the equality $\mathrm{im}(\varphi) = \ker(\epsilon)$ is established. It amounts to proving Λ-divisibility.

Proposition 6.3. *If $\mathcal{D}$ is a divisible Λ-module, then $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ is a divisible Λ-module.*

Proof. We must show that φ is surjective. Applying the snake lemma to the 2nd and 3rd rows gives an exact sequence

$$\ker(\chi) \xrightarrow{a} \ker(\psi) \longrightarrow \operatorname{coker}(\varphi) \longrightarrow \operatorname{coker}(\chi) \xrightarrow{b} \operatorname{coker}(\psi)$$

Since σ is surjective, it follows that the map a is surjective too. Now τ is injective and so it follows that the map b is also injective. The exact sequence then implies that $\operatorname{coker}(\varphi) = 0$ as we want. ■

Finally, we consider the map δ in the fundamental diagram. The first two rows in that diagram can be rewritten as follows. We use the letters d, k and l for the vertical maps corresponding to δ, κ, and λ.

$$\begin{tikzcd}
0 \arrow[r] & H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}[P]) \arrow[r] \arrow[d, "d"] & H^2(K_\Sigma/K, \mathcal{D}[P]) \arrow[r, "\sigma"] \arrow[d, "k"] & \prod_{v\in\Sigma'} H^2(K_v, \mathcal{D}[P]) \arrow[r] \arrow[d, "l"] & 0 \\
0 \arrow[r] & H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})[P] \arrow[r] & H^2(K_\Sigma/K, \mathcal{D})[P] \arrow[r] & \prod_{v\in\Sigma'} H^2(K_v, \mathcal{D})[P] &
\end{tikzcd}$$

The maps k and l are surjective. Since k is surjective, the snake lemma gives us an exact sequence $\ker(l) \longrightarrow \operatorname{coker}(d) \longrightarrow 0$. We can now apply proposition 5.2 to deduce that d is at least sometimes surjective. If so, the first column of maps in the fundamental diagram will then be exact.

Proposition 6.4. *Assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is a reflexive Λ-module for all $v \in \Sigma'$. Then, for almost all $P \in \operatorname{Spec}_{ht=1}(\Lambda)$, we have $\operatorname{im}(\delta) = \ker(\varphi)$.*

Proof. The assumption concerning $\mathcal{T}^*$ implies that $\ker(l) = 0$ for almost all prime ideals of Λ of height 1. It would then follow that $\operatorname{coker}(d) = 0$ and so d is indeed surjective for those P's. ■

We can apply this proposition to obtain the following important result.

Proposition 6.5. *Assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is a reflexive Λ-module for all $v \in \Sigma'$. If $\mathcal{D}$ is a coreflexive Λ-module, then $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ is also a coreflexive Λ-module.*

Proof. Excluding just finitely many prime ideals $P \in \operatorname{Spec}_{ht=1}(\Lambda)$, the stated assumptions imply the following statements: The map d will be surjective and $\mathcal{D}[P]$ will be a cofinitely generated, divisible (Λ/P)-module. Proposition 6.3 implies that $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}[P])$ is (Λ/P)-divisible for all those P's. Therefore, its image $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})[P]$ under the map d will also be (Λ/P)-divisible. Corollary 2.6.1 implies that $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ is coreflexive. ■

The assumption about $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ in theorem 1 is due primarily to our need for that assumption in propositions 6.5. Since we assume that R is a cofree Λ-module, the assumption that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is R-free implies that this module is also Λ-reflexive. The other local assumption in theorem 1 is made for the following simple reason. If $(\mathcal{T}^*)^{G_{K_{v_o}}} = 0$ for some non-archimedean prime $v_o \in \Sigma$, then we have $H^2(K_{v_o}, \mathcal{D}) = 0$. If we then let $\Sigma' = \Sigma - \{v_o\}$, it is clear that $Ш^2(K, \Sigma, \mathcal{D}) = H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})$. We then can apply the above propositions to get the following result.

Proposition 6.6. *Assume that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is Λ-reflexive for all $v \in \Sigma$ and that $(\mathcal{T}^*)^{G_{K_{v_o}}} = 0$ for at least one non-archimedean prime $v_o \in \Sigma$. If $\mathcal{D}$ is Λ-divisible, then $Ш^2(K, \Sigma, \mathcal{D})$ is Λ-divisible. If $\mathcal{D}$ is Λ-coreflexive, then $Ш^2(K, \Sigma, \mathcal{D})$ is Λ-coreflexive.*

Thus, all but the final statement is theorem 1 has been proven.

It is interesting to consider the case where Σ' is as small as possible - just the set of archimedean primes of K. We will then denote $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ by $H^2_\infty(K_\Sigma/K, \mathcal{D})$. For any real prime v of K, we let σ_v denote the nontrivial element of G_{K_v}. Then propositions 6.3 and 6.5 give the following result. The content is the same as proposition 6.1 when $p \neq 2$. Note that the assumption about $(1+\sigma_v)\mathcal{D}$ is true when p is odd and is equivalent to the assumption that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is reflexive when $p = 2$.

Proposition 6.7. *If $\mathcal{D}$ is a divisible Λ-module, then $H^2_\infty(K_\Sigma/K, \mathcal{D})$ is a divisible Λ-module. If $\mathcal{D}$ is a coreflexive Λ-module and if $(1 + \sigma_v)\mathcal{D}$ is also coreflexive for every real prime v of K, then $H^2_\infty(K_\Sigma/K, \mathcal{D})$ is a coreflexive Λ-module.*

B. The cokernel of γ. The duality theorems of Poitou and Tate have some interesting and useful consequences concerning the cokernel of the map $\gamma: \ H^2(K_\Sigma/K, \mathcal{D}) \longrightarrow P^2(K, \Sigma, \mathcal{D})$, the map whose kernel is $Ш^2(K, \Sigma, \mathcal{D})$. According to (6), $\mathrm{coker}(\gamma)^\wedge \cong (\mathcal{T}^*)^{\mathrm{Gal}(K_\Sigma/K)}$ which is a Λ-submodule of $\mathcal{T}^*$. If $\mathcal{T}^*$ is Λ-reflexive, then so is $(\mathcal{T}^*)^{\mathrm{Gal}(K_\Sigma/K)}$. (See part C in section 2.) Furthermore, proposition 3.10 implies that the Λ-rank of $(\mathcal{T}^*)^{\mathrm{Gal}(K_\Sigma/K)}$ is equal to the Λ-corank of $H^0(K_\Sigma/K, \mathcal{D}^*)$. These remarks give us the following results.

Proposition 6.8. *If $\mathcal{D}$ is Λ-divisible, then* $\mathrm{coker}(\gamma)$ *is also Λ-divisible. If $\mathcal{D}$ is Λ-coreflexive, then* $\mathrm{coker}(\gamma)$ *is also Λ-coreflexive.*

Proposition 6.9. *Assume that $\mathcal{D}$ is Λ-divisible and that $H^0(K_\Sigma/K, \mathcal{D}^*)$ is Λ-cotorsion. Then γ is surjective. In general, $H^0(K_\Sigma/K, \mathcal{D}^*)$ and* $\mathrm{coker}(\gamma)$ *have the same Λ-corank.*

One simple case where γ is surjective is if $H^0(K_\Sigma/K, \mathcal{D}^*[\mathfrak{m}_\Lambda]) = 0$. Then, of course, $H^0(K_\Sigma/K, \mathcal{D}^*)[\mathfrak{m}_\Lambda] = 0$, and Nakayama's lemma implies that $H^0(K_\Sigma/K, \mathcal{D}^*) = 0$. Another important case is if $\mathcal{D}$ is induced from some $D = V/T$ via a $\mathbb{Z}_p^m$-extension K_∞/K, where $m \geq 1$. Then

$$H^0(K_\Sigma/K, \mathcal{D}^*) = H^0(K_\Sigma/K_\infty, D^*) = D^*(K_\infty)$$

has finite $\mathbb{Z}_p$-corank and so is clearly Λ-cotorsion since the Krull dimension of Λ is greater than 1. More generally, if assumption *(b)* in theorem 1 holds, then, as we pointed out in the introduction, it follows that $H^0(K_\Sigma/K, \mathcal{T}^*) = 0$ and hence that γ is surjective.

C. The structure of $H^1(K_\Sigma/K, \mathcal{D})$. We now complete the proof of theorem 1. The hypotheses are somewhat broader and so we state this as a proposition.

Proposition 6.10. *Assume that $\mathcal{D}$ is Λ-coreflexive, that $\mathcal{T}^*/(\mathcal{T}^*)^{G_{K_v}}$ is Λ-reflexive for all $v \in \Sigma$, that $(\mathcal{T}^*)^{G_{K_{v_o}}} = 0$ for some non-archimedean $v_o \in \Sigma$, and that $\text{Ш}^2(K, \Sigma, \mathcal{D}) = 0$. Then $H^1(K_\Sigma/K, \mathcal{D})$ is an almost divisible Λ-module.*

Proof. The assertion will follow from proposition 3.6 if we show that κ is an injective map for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. We have an exact sequence

$$0 \longrightarrow \ker(\delta) \longrightarrow \ker(\kappa) \longrightarrow \ker(\lambda)$$

Proposition 5.2 implies that $\ker(\lambda) = 0$ for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. Thus it suffices to prove the same statement for $\ker(\delta)$.

If $\Sigma' = \Sigma - \{v_o\}$, then we have $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}) = \text{Ш}^2(K, \Sigma, \mathcal{D}) = 0$. Hence, $\ker(\delta) = H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}[P])$. Now $\mathcal{D}[P]$ is a divisible (Λ/P)-module for all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ and hence proposition 6.3 implies that $H^2_{\Sigma'}(K_\Sigma/K, \mathcal{D}[P])$ is also (Λ/P)-divisible. Therefore, it suffices to prove that the (Λ/P)-corank of $\ker(\delta)$ is equal to 0 for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. It will then follow that $\ker(\delta) = 0$ and hence that κ is injective. Proposition 3.5 implies that the (Λ/P)-corank of $\ker(\kappa)$ is 0 for almost all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$ and therefore the same must be true for the submodule $\ker(\delta) = 0$. This argument proves that, under the stated assumptions, $H^1(K_\Sigma/K, \mathcal{D})$ is indeed an almost divisible Λ-module. ■

It is worth pointing out that $H^1(K_\Sigma/K, \mathcal{D})$ is not necessarily a divisible Λ-module as the following proposition shows. It is not hard to find examples satisfying the hypotheses and where at least one of the local factors $H^1(K_v, \mathcal{D})$ for $v \in \Sigma'$ fails to be Λ-divisible.

Proposition 6.11. *Assume that $\mathcal{D}$ is Λ-divisible, that p is odd, that $H^2(K_v, \mathcal{D}) = 0$ for all nonarchimedean $v \in \Sigma'$, and that $H^2(K_\Sigma/K, \mathcal{D}) = 0$. Then the natural map*

$$H^1(K_\Sigma/K, \mathcal{D})/H^1(K_\Sigma/K, \mathcal{D})_{\Lambda-div} \longrightarrow \prod_{v \in \Sigma'} H^1(K_v, \mathcal{D})/H^1(K_v, \mathcal{D})_{\Lambda-div}$$

is surjective.

If A is a discrete Λ-module, then $A_{\Lambda-div}$ denotes the maximal Λ-divisible submodule of A. If $X = \widehat{A}$, then the Pontryagin dual of $A/A_{\Lambda-div}$ is isomorphic to the torsion Λ-submodule of X.

Proof. Applying the snake lemma to the two-row commutative diagram above, it follows that the map $\ker(k) \to \ker(l)$ is surjective. That is, we have a surjective homomorphism

$$H^1(K_\Sigma/K, \mathcal{D})/PH^1(K_\Sigma/K, \mathcal{D}) \longrightarrow \prod_{v\in\Sigma'} H^1(K_v, \mathcal{D})/PH^1(K_v, \mathcal{D})$$

for *all* $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. In general, suppose that A and B are two cofinitely generated, cotorsion Λ-modules and that $\psi : A \to B$ is a Λ-module homomorphism with the property that the induced map $A/PA \to B/PB$ is surjective for all $P \in \mathrm{Spec}_{ht=1}(\Lambda)$. This means that $\psi(A) + PB = B$ for all such P's. Let $C = \mathrm{coker}(\psi)$, which is also a cotorsion Λ-module. It follows that $\pi C = C$ for all irreducible elements of Λ. Thus C is a divisible Λ-module and so $C = 0$. This proves the proposition. ■

D. A discussion of hypothesis L. One natural way to verify hypothesis L for a given Galois module $\mathcal{D}$ is to show that the inequality in proposition 4.3, which gives a lower bound $b^1_\Lambda(K, \Sigma, \mathcal{D})$ on the Λ-corank of $H^1(K_\Sigma/K, \mathcal{D})$, is actually an equality. One can often verify this by specialization. For example, suppose that Λ is a formal power series over $\mathbb{Z}_p$ in m variables, where $m \geq 1$. Consider a cofree, cofinitely generated Λ-module $\mathcal{D}$ with Λ-corank n. Suppose that P is a prime ideal such that $\Lambda' = \Lambda/P$ is isomorphic to a formal power series ring over $\mathbb{Z}_p$ or $\mathbb{F}_p$ in m' variable, where $0 \leq m' \leq m$. (If $m' = 0$, we mean that $\Lambda' \cong \mathbb{Z}_p$ or $\mathbb{F}_p$. In the latter case, $P = \mathfrak{m}_\Lambda$.) Since Λ' is a regular local ring, remark 3.4.2 can be applied. If the equality $\mathrm{corank}_{\Lambda'}\big(H^1(K_\Sigma/K, \mathcal{D}[P])\big) = b^1_\Lambda(K, \Sigma, \mathcal{D})$ can be verified for one such prime ideal P, then hypothesis L for $\mathcal{D}$ would follow. Of course, it may happen $b^1_{\Lambda'}(K, \Sigma, \mathcal{D}[P]) > b^1_\Lambda(K, \Sigma, \mathcal{D})$, in which case, the equality would be impossible. However, remark 3.10.2 implies that there exists a nonzero ideal I of Λ such that $b^1_{\Lambda'}(K, \Sigma, \mathcal{D}[P]) = b^1_\Lambda(K, \Sigma, \mathcal{D})$ for all $P \notin V(I)$.

We will discuss various special cases and give examples where hypothesis L fails to be true. But it will be clear that these examples are rather special.

Elliptic curves. Suppose that E is an elliptic curve defined over K and that the Mordell-Weil group $E(K)$ has rank $r > [K : \mathbb{Q}]$. Let $s_K = r - [K : \mathbb{Q}]$. Let p be any prime number and let Σ be a finite set of primes of K containing all primes lying above p or ∞ and the primes where E has bad reduction. The Kummer map defines an injective homomorphism

$$E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_\Sigma/K, E[p^\infty])$$

It follows that $\mathrm{corank}_{\mathbb{Z}_p}\big(H^1(K_\Sigma/K, E[p^\infty])\big) \geq r$. In the notation of proposition 4.1, we have $\delta_{\mathbb{Z}_p}(K, E[p^\infty]) = [K : \mathbb{Q}]$. The Euler-Poincaré characteristic formula then implies that $\mathrm{corank}_{\mathbb{Z}_p}\big(H^2(K_\Sigma/K, E[p^\infty])\big) > 0$. But

$H^2(K_v, E[p^\infty]) = 0$ for every non-archimedean prime v of K and is finite for the archimedean primes (trivial if $p > 2$). Hence it follows that $\mathrm{corank}_{\mathbb{Z}_p}\big(\text{Ш}^2(K, \Sigma, E[p^\infty])\big) > 0$. Thus hypothesis L fails if $R = \mathbb{Z}_p$ and $\mathcal{D} = E[p^\infty]$. This example corresponds to the representation ρ giving the action of $\mathrm{Gal}(K_\Sigma/K)$ on the Tate module $\mathcal{T} = T_p(E)$.

In this example, the Krull dimension of R is 1. However, one can simply extend scalars to obtain a *"constant"* deformation of $T_p(E)$ where R has arbitrary Krull dimension and hypothesis L still fails to be valid. For example, suppose that $\mathcal{T} = T_p(E) \otimes_{\mathbb{Z}_p} \Lambda$, where Λ is a formal power series ring over $\mathbb{Z}_p$ in m variables. We assume that the Galois action on Λ is trivial. Define $\mathcal{D} = \mathcal{T} \otimes_\Lambda \widehat{\Lambda}$. If $m \geq 1$, there are infinitely many homomorphism $\phi : \Lambda \to \mathbb{Z}_p$ and one has $T_\phi \cong T_p(E)$, $D_\phi \cong E[p^\infty]$ for all such ϕ. It follows easily (by using lemma 4.4.1 for example) that $\mathrm{corank}_\Lambda\big(\text{Ш}^2(K, \Sigma, \mathcal{D})\big) = \mathrm{corank}_{\mathbb{Z}_p}\big(\text{Ш}^2(K, \Sigma, E[p^\infty])\big)$.

One natural non-constant deformation to consider was described in the introduction. Suppose that K_∞/K is a $\mathbb{Z}_p^m$-extension, where $m \geq 1$, and let $\mathcal{D} = \mathrm{Ind}_{K_\infty/K}(E[p^\infty])$. It is known in certain cases that $\mathrm{rank}\big(E(K')\big)$ is unbounded as K' varies over the finite extensions of K contained in K_∞. One can find a discussion of this phenomenon in [M], [M-R], [Va], and [C], for example. To produce an example where Hypothesis L fails based on the above discussion, one would need $s_{K'} = \mathrm{rank}\big(E(K')\big) - [K' : \mathbb{Q}]$ to be unbounded above as K' varies. No such examples are known. It is hard to imagine that they could exist.

Suppose that $R = \Lambda \cong \mathbb{Z}_p[[T_1, ..., T_m]]$ and that $\mathcal{D}[P] \cong E[p^\infty]$ for some prime ideal P of Λ, as in the example in the previous paragraph. Note that both $b^1_\Lambda(K, \Sigma, \mathcal{D})$ and $b^1_{\mathbb{Z}_p}(K, \Sigma, E[p^\infty])$ equal $[K : \mathbb{Q}]$. Suppose further that $\mathrm{corank}_{\mathbb{Z}_p}\big(H^1(K_\Sigma/K, E[p^\infty])\big) = [K : \mathbb{Q}]$, i.e., that hypothesis L holds for $\mathcal{D}[P]$. Thus, by our initial remarks, hypothesis L would then hold for $\mathcal{D}$. One example where this happens is if $K = \mathbb{Q}$, $E(\mathbb{Q})$ has rank 1, and the p-primary subgroup of the Tate-Shafarevich group for $E/\mathbb{Q}$ is finite. (See [M-C] for a discussion of this case.)

As another example, suppose instead that $\mathcal{D}[P] \cong \mathrm{Ind}_{K_\infty^{cyc}/K}(E[p^\infty])$ for some prime ideal P of Λ, where K_∞^{cyc} denotes the cyclotomic $\mathbb{Z}_p$-extension of K. Assume also that E has ordinary reduction at all the primes of K lying above p. A conjecture of Mazur asserts that the p-Selmer group $\mathrm{Sel}_E(K_\infty^{cyc})$ for E over K_∞^{cyc} is a cotorsion module over $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty^{cyc}/K)]]$. Since $\text{Ш}^1(K_\infty^{cyc}, \Sigma, E[p^\infty]) \subseteq \mathrm{Sel}_E(K_\infty^{cyc})$, Mazur's conjecture would imply that $\text{Ш}^1(K_\infty^{cyc}, \Sigma, E[p^\infty])$ is also cotorsion. Now $E[p^\infty]^* \cong E[p^\infty]$ and so it would follow that conjecture L holds for $\mathcal{D}[P]$. It then would hold for $\mathcal{D}$. One special case is $\mathcal{D} = \mathrm{Ind}_{K_\infty/K}(E[p^\infty])$, where K_∞ is a $\mathbb{Z}_p^m$-extension of K containing K_∞^{cyc}.

A twist of $\mathbb{Q}_p/\mathbb{Z}_p$. Let K denote the maximal real subfield of $\mathbb{Q}(\mu_p)$. Assume that $p = 37$, an irregular prime. Let Σ be the set of primes of K lying above

p and ∞. Let M_∞ be the maximal abelian pro-p-extension of K_∞^{cyc} which is unramified outside of Σ. Then it is known that $X = \mathrm{Gal}(M_\infty/K_\infty^{cyc}) \cong \mathbb{Z}_p$. The action of $\Gamma = \mathrm{Gal}(K_\infty^{cyc}/K)$ on X is given by a nontrivial homomorphism $\phi : \Gamma \to 1 + p\mathbb{Z}_p$. We define $\rho : \mathrm{Gal}(K_\Sigma/K) \to GL_1(\mathbb{Z}_p)$ to be the composition of ϕ with the restriction map $\mathrm{Gal}(K_\Sigma/K) \to \Gamma$. Thus the corresponding Galois module $\mathcal{D}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ and $\mathrm{Gal}(K_\Sigma/K)$ acts via ρ. We denote this $\mathcal{D}$ by $(\mathbb{Q}_p/\mathbb{Z}_p)(\rho)$. Then we have

$$H^1(K_\Sigma/K, \mathcal{D}) \cong H^1(K_\Sigma/K_\infty^{cyc}, \mathcal{D})^\Gamma \cong \mathbb{Q}_p/\mathbb{Z}_p$$

The $\mathbb{Z}_p$-corank is 1. We have $\delta_{\mathbb{Z}_p}(K, \mathcal{D}) = 0$ and so it follows that $\mathrm{corank}_{\mathbb{Z}_p}\big(H^2(K_\Sigma/K, \mathcal{D})\big) > 0$. We again have $H^2(K_v, \mathcal{D}) = 0$ for all $v \in \Sigma$ and so, as in example 1, $Ш^2(K, \Sigma, \mathcal{D})$ fails to be a cotorsion module over $R = \mathbb{Z}_p$. Just as before, one can form a constant deformation of ρ over an arbitrary R to construct additional examples where hypothesis L also fails to hold. However, if instead one considers $\mathcal{D} = \mathrm{Ind}_{K_\infty^{cyc}/K}((\mathbb{Q}_p/\mathbb{Z}_p)(\rho))$, a cofree module over $R = \mathbb{Z}_p[[\Gamma]]$ of corank 1, then $H^1(K_\Sigma/K, \mathcal{D}) \cong \mathrm{Hom}(X, (\mathbb{Q}_p/\mathbb{Z}_p)(\rho))$, which is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a group and is a cotorsion R-module. Hypothesis L holds in this case.

Consider an arbitrary number field K. Let K_∞ denote the compositum of all $\mathbb{Z}_p$-extensions of K. Let $\Gamma = \mathrm{Gal}(K_\infty/K)$, which is isomorphic to $\mathbb{Z}_p^m$ for some $m \geq 1$. Let $\mathcal{D} = \mathrm{Ind}_{K_\infty/K}(D)$, where $D = \mu_{p^\infty}$. Thus D is simply the twist of $\mathbb{Q}_p/\mathbb{Z}_p$ by the cyclotomic character χ and $\mathcal{D}$ is a cofree module over $\Lambda = \mathbb{Z}_p[[\Gamma]]$ with corank 1. As we pointed out in the introduction, hypothesis L is true for $\mathcal{D}$ and $Ш^1(K, \Sigma, \mathcal{D}^*)$ is essential just the Pontryagin dual of the Galois group $Y = \mathrm{Gal}(L_\infty^{'}/K_\infty)$. It is conjectured that Y is a pseudo-null module over Λ. Thus, $Ш^1(K, \Sigma, \mathcal{D}^*)$ should even be a co-pseudo-null Λ-module. However, this module can be nontrivial and it is conceivable that examples where hypothesis L fails can arise by specialization.

Suppose that P is a prime ideal of Λ which is an associated prime ideal for Y. Then $Ш^1(K, \Sigma, \mathcal{D}^*)[P]$ will have positive corank over Λ/P. Consider the map

$$Ш^1(K, \Sigma, \mathcal{D}^*[P]) \longrightarrow Ш^1(K, \Sigma, \mathcal{D}^*)[P]$$

Thus, for such a P, either the cokernel of this map or $Ш^1(K, \Sigma, \mathcal{D}^*[P])$ will have a positive (Λ/P)-corank. If it is the latter, then hypothesis L would fail to be true for the (Λ/P)-module $\mathcal{D}[P]$. Virtually nothing is known about the associated prime ideals of Y in general. One can construct examples where Y has an associated prime ideal P such that Λ/P is of characteristic 0 and has arbitrarily large Krull dimension. However, the construction is an imitation of classical genus theory and it is probably the cokernel of the above map which has positive (Λ/P)-corank. This example illustrates the subtlety of hypothesis L.

Characteristic p. Let R be a formal power series ring over $\mathbb{F}_p$ in any number of variables. Let Σ' be a finite set of primes of K containing the primes above

p and ∞. Suppose that we have a representation $\rho : \mathrm{Gal}(K_{\Sigma'}/K) \to GL_n(R)$. Let $\mathcal{D}$ be the cofree R-module of corank n with Galois action given by ρ. We will make the following assumption: there exist infinitely many primes v of K such that *(i)* $\rho|_{G_v^{\Sigma'}}$ is trivial and *(ii)* $\mu_p \subset K_v$. Here $G_v^{\Sigma'}$ denotes the decomposition subgroup of $\mathrm{Gal}(K_{\Sigma'}/K)$ for any prime of $K_{\Sigma'}$ lying above v. For any prime v satisfying *(i)* and *(ii)*, it is clear that G_{K_v} acts trivially on $\mathcal{T}^* = \mathrm{Hom}(\mathcal{D}, \mu_p)$. Thus, the R-rank of $H_0(K_v, \mathcal{T}^*)$ is n and so the R-corank of $H^2(K_v, \mathcal{D})$ is equal to n. Suppose that $\Upsilon = \{v_1, ..., v_t\}$ is a set consisting of such primes. Let $\Sigma = \Sigma' \cup \Upsilon$. Then, by (7), we have the following inequality:

$$\mathrm{corank}_R\big(H^2(K_\Sigma/K, \mathcal{D})\big) \ \geq \ (t-1)n$$

If we assume that $H^0(K_{\Sigma'}/K, \mathcal{T}^*)$ is a torsion R-module, then we get the better lower bound tn instead. In either case, it follows that the lower bound $b_R^1(K, \Sigma, \mathcal{D})$ for the R-corank of $H^1(K_\Sigma/K, \mathcal{D})$ is unbounded as $t \to \infty$.

Now let c' denote the R-corank of $\prod_{v \in \Sigma'} H^1(K_v, \mathcal{D})$. The definition of $H^1_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ gives the following inequality:

$$\mathrm{corank}_R\big(H^1_{\Sigma'}(K_\Sigma/K, \mathcal{D})\big) \ \geq \ b_R^1(K, \Sigma, \mathcal{D}) - c'$$

We can make this corank positive by choosing a sufficiently large set Υ. We will assume that the primes in Υ do not lie over p. The elements of $H^1_{\Sigma'}(K_\Sigma/K, \mathcal{D})$ are locally trivial at all $v \in \Sigma'$, but could be nontrivial at the primes $v \in \Upsilon$. However, for each $v \in \Upsilon$, G_{K_v} acts trivially on $\mathcal{D}$. This module is just a vector space over $\mathbb{F}_p$ - a direct sum of copies of the trivial Galois module $\mathbb{Z}/p\mathbb{Z}$. Let L_v denote the maximal abelian extension of K_v such that $\mathrm{Gal}(L_v/K_v)$ has exponent p. Thus $[L_v : K_v] = p^2$. Every element of $H^1(K_v, \mathbb{Z}/p\mathbb{Z})$ becomes trivial when restricted to G_{L_v} and so the same thing is true for the elements of $H^1(K_v, \mathcal{D})$.

Choose a finite extension F of K such that, for each $v \in \Upsilon$ and for every prime η lying over v, the completion F_η contains L_v. We will also assume that F is chosen so that $F \cap K_\Sigma = K$. Such a choice is easily seen to be possible. Suppose that $\sigma \in H^1_{\Sigma'}(K_\Sigma/K, \mathcal{D})$. Let $\sigma|_F$ denote the image of σ under the restriction map $H^1(K_\Sigma/K, \mathcal{D}) \to H^1(F_{\Sigma_F}/F, \mathcal{D})$. Here Σ_F denotes the set of primes of F lying over those in Σ. This restriction map is easily seen to be injective. Then $\sigma|_F$ is locally trivial at *all* primes $\eta \in \Sigma_F$. That is, $\sigma|_F \in \text{Ш}^1(F, \Sigma_F, \mathcal{D})$. It follows that $\mathrm{corank}_R\big(\text{Ш}^1(F, \Sigma_F, \mathcal{D})\big)$ will be positive and so we do get examples where hypothesis L fails.

References

[B-H] W. Bruns, J. Herzog, Cohen-Macaulay Rings, Cambridge Studies in Advanced Math. 39, Cambridge University Press, 1998.

[C-M] J. Coates, G. McConnell, Iwasawa theory of modular elliptic curves of analytic rank at most 1, J. London Math. Soc. 50 (1994), 243-269.

[C-S] J. Coates, R. Sujatha, Fine Selmer groups of elliptic curves over p-adic Lie extensions, Math. Ann. 331 (2005), 809-839.

[C] C. Cornut, Mazur's conjecture on higher Heegner points, Invent. Math. 148 (2002), 495-523.

[D] J. Dieudonné, Topics in Local Algebra, Notre Dame Mathematical Lectures 10, University of Notre Dame Press, 1967.

[Gr73] R. Greenberg, The Iwasawa invariants of Γ-extensions of a fixed number field, Amer. J. of Math. XCV (1973), 204-214.

[Gr78] R. Greenberg, On the structure of certain Galois groups, Invent. Math. 47 (1978), 85-99.

[Gr89] R. Greenberg, Iwasawa theory for p-adic representations, Advanced Studies in Pure Math. 17 (1989), 97-137.

[Gr94] R. Greenberg, Iwasawa theory and p-adic deformations of motives, Proceedings of Symposia in Pure Math. 55 II (1994), 193-223.

[Gr97] R. Greenberg, The structure of Selmer groups, Proceedings Natl. Acad. of Science 94 (1997), 11125-11128.

[Hid] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Invent. Math. (1985), 545–613.

[Iw59] K. Iwasawa, On the theory of cyclotomic fields, Ann. Math. 70 (1959), 530-561.

[Iw73] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, Ann. Math. 98 (1973), 246-326.

[J] U. Jannsen, Iwasawa modules up to isomorphism, Advanced Studies in Pure Math. 17 (1989), 171-207.

[M] B. Mazur, Modular curves and arithmetic, Proceedings of the ICM, Warsaw, 1983, 185-211.

[M-R] B. Mazur, K. Rubin, Studying the growth of Mordell-Weil, Documenta Math, Volume in honor of K. Kato, (2003) 586-607.

[McC] G. McConnell, On the Iwasawa theory of CM elliptic curves at supersingular primes, Ph.D. thesis,1993, Cambridge University.

[Nek] J. Nekovar, Selmer complexes, to appear in Astérisque

[NQD] T. Nguyen Quang-Do, Formations de classes et modules d'Iwasawa, Lecture notes in Math. 1068 (1984), 167-185.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Grundlehren der Math. Wissenschaften 323 (2000), Springer.

[O-V] Y. Ochi, O. Venjakob, On the structure of Selmer groups over p-adic Lie extensions, J. Algebraic Geom. 11 (2002), 547–580.

[Pe84] B. Perrin-Riou, Arithmetique des courbes elliptiques et théorie d'Iwasawa, Mem. Soc. Math. France 17, Vol. 112 (1984).

[Pe95] B. Perrin-Riou, Fonctions L p-adiques des representations p-adiques, Astérisque 229, (1995).

[Sch] P. Schneider, p-Adic height pairings II, Inv. Math. 79 (1985), 329-374.

[Va] V. Vatsal, Uniform distribution of Heegner points, Invent. Math. 148, (2002), 1-46.

[Ve] O. Venjakob, On the Iwasawa theory of p-adic Lie extensions, Compositio Math. 138, (2003), 1-54.

Ralph Greenberg
Department of Mathematics
Box 354350
University of Washington
Seattle WA 98195-4350 USA
greenber@math.washington.edu

p-Adic L-Functions for Unitary Shimura Varieties I: Construction of the Eisenstein Measure

To John Coates, with admiration

Michael Harris[1], Jian-Shu Li[2], Christopher M. Skinner[3]

Received: September 30, 2005
Revised: November 15, 2006

Abstract. We construct the Eisenstein measure in several variables on a quasi-split unitary group, as a first step towards the construction of p-adic L-functions of families of ordinary holomorphic modular forms on unitary groups. The construction is a direct generalization of Katz' construction of p-adic L-functions for CM fields, and is based on the theory of p-adic modular forms on unitary Shimura varieties developed by Hida, and on the explicit calculation of non-degenerate Fourier coefficients of Eisenstein series.

2000 Mathematics Subject Classification: Primary 11F33, 11R23; Secondary 14G35

Introduction

This is the first of a projected series of papers devoted to studying the relations between p-adic L-functions for $GL(n)$ (and unitary groups), congruences between stable and endoscopic automorphic forms on unitary groups, and Selmer groups for p-adic representations. The goals of these papers are outlined in the survey article [HLS]. The purpose of the present installment is to prepare the ground for the construction of p-adic L-functions in sufficient generality for the purposes of subsequent applications to congruences and Selmer groups.

[1] Institut de Mathématiques de Jussieu, U.M.R. 7586 du CNRS; Member, Institut Universitaire de France

[2] Partially supported by RGC-CERG grants HKUST6115/02P, HKUST601805 and a grant from the Chinese Academy of Science

[3] Partially supported by a grant from the National Science Foundation and a fellowship from the David and Lucile Packard Foundation

The first general conjectures on the construction of p-adic L-functions for ordinary motives were elaborated by Coates in [Co]. The conjectured p-adic analytic functions of [Co] interpolate the quotients of normalized values of L-functions at critical points, in the sense of Deligne. The normalization proceeds in two steps. The critical values are first rendered algebraic, by dividing by their Deligne periods. Next, they are p-stabilized: the Euler factors at p and ∞ are modified according to a complicated but explicit recipe. Coates' conjecture is that the resulting values are p-adically interpolated by a p-adic analytic function of Iwasawa type, associated to a p-adic measure. In our setting, the Deligne period is generally replaced by a certain Petersson norm or an algebraic multiple thereof; the relation of this Petersson norm to the Deligne period is discussed at length in [H3]. In [Pa], Panchishkin points out that Coates' recipe can be adapted unchanged for motives satisfying a condition weaker than ordinarity, which he calls *admissibility* and which Perrin-Riou and Greenberg have called the *Panchishkin condition.* Although this is somewhat obscured by the automorphic normalization, we work in the generality of Panchishkin's admissibility condition. Panchishkin also conjectures the existence of more general p-adic L-functions in the absence of admissibility; we do not address this question.

We work with automorphic forms on the unitary groups of hermitian vector spaces over a CM field $\mathcal{K}$, with maximal totally real subfield E. We assume every prime of E dividing p splits in $\mathcal{K}$; we also impose a hypothesis (1.1.2) linking primes above p to signatures of the unitary group at real places of E. Unitary groups, unlike $GL(n)$, are directly related to Shimura varieties. We show that the special values of L-functions of automorphic forms on unitary groups satisfy the congruences needed for the construction of p-adic L-functions by appealing to the fact that the corresponding Shimura varieties are moduli spaces for abelian varieties of PEL type. In this our approach is directly modeled on Katz's construction [K] of p-adic L-functions for Hecke characters of CM fields; indeed, for groups of type $U(1)$ our results reduce to those of Katz. The starting point of Katz's construction is Damarell's formula and its generalizations due to Shimura, which relate the values of arithmetic Eisenstein series at CM points to special values of L-functions of arithmetic Hecke characters. A generalization of Damerell's formula in higher dimensions is the construction of standard L-functions of unitary groups by the doubling method. This was first developed systematically in the article [PSR] of Piatetski-Shapiro and Rallis, though special cases had been discovered independently by Garrett, and a more thorough development in classical language is contained in the books [S97, S00] of Shimura. The local theory for unitary groups was ignored in [PSR] but was worked out in [L2] and [HKS].

Our p-adic L-functions are actually attached to Hida families of nearly ordinary modular forms on a unitary group $G = U(V)$. As in [K], the main step is the construction of an Eisenstein measure on a large unitary group H, attached to the sum of two copies $V \oplus (-V)$ of V. The hermitian form on $-V$ has been multiplied by -1, so that H is quasi-split and its associated Shimura variety has a point boundary component, stabilized by a maximal parabolic subgroup, the *Siegel parabolic.* The Eisenstein series attached to the Siegel parabolic are the direct generalizations of the classical Eisenstein series on $GL(2)$. The Eisenstein measure is a p-adic measure on a product T of copies of $\mathbb{Z}_p^\times$ with values in the algebra of p-adic modular forms on H interpolating such Eisenstein series. The theory of p-adic modular forms on H was developed by Hida in [Hi04, Hi05]. As in [K], these forms belong to the algebra of functions on the Igusa tower, which is a rigid analytic étale covering of the ordinary locus of the Shimura variety attached to H. The existence of the Eisenstein measure relies crucially on the irreducibility of the Igusa tower; this was established in some generality by Hida, though easier arguments due to Chai and Hida himself suffice for the case at hand (cf. [Ch, Hi06]).

The Eisenstein measure associates, by integrating over T with respect to this measure, p-adic modular forms to continuous functions on T. The integrals of characters of T of finite order, which determine the measure, are classical holomorphic (Siegel) Eisenstein series on H and as such are associated to explicit functions ("sections") belonging to degenerate principal series induced from characters of the Siegel parabolic. These sections factor as tensor products of local sections over the primes of E. At almost all finite primes the local sections are unramified and present no difficulty, and we simplify the theory by choosing local sections at ramified primes, other than those dividing p, that are insensitive to p-adic variation of the character of T. With our choice of data, the Fourier coefficients of the Eisenstein series at a chosen point boundary component also factor over primes. All the work in constructing the Eisenstein measure then comes down to choosing local data at primes above p such that the corresponding local coefficients satisfy the necessary Kummer congruences. Our strategy for choosing local data follows [K] in making use of a partial Fourier transform. Unlike in [K], our construction is systematically adelic and isolates the local considerations at p. The Eisenstein measure is designed to pair with Hida families – on $G \times G$, not on G itself – and thus depends on several variables, considerably complicating the calculations.

The doubling method was used by Böcherer and Schmidt in [BS] to construct standard p-adic L-functions for Siegel modular forms. They do not use p-adic modular forms; their approach is to construct the p-adic measure directly in terms of normalized special values of complex L-functions. Their approach applies to all critical values, unlike the present paper, which avoids reference to non-holomorphic differential operators (and their p-adic analogues). Presumably their techniques work for quasi-split unitary groups as well. We have not attempted to compare our results where they can be compared, namely in the local analysis at the prime p, since our group is locally isomorphic to $GL(2n)$, in principle much simpler than a symplectic group.

As predicted by Coates, the shape of the modified Euler factor at a prime v dividing p depends on the p-adic valuations of the eigenvalues of Frobenius at v. On the other hand, as in [H3], the fact that a critical value of the standard L-function is an algebraic multiple of a period of an arithmetic modular form on the doubled group $G \times G$ – in other words, the Petersson norm of an arithmetic modular form on G – can be expressed in terms of Hodge numbers. Then the Panchishkin condition, applied to the standard L-function for $GL(n)_{\mathcal{K}}$, roughly states that, for each v dividing p, the modified Euler factor at v is given by a natural partition of the Frobenius eigenvalues at v that corresponds to the signature of the unitary group at real places assigned to v by Hypothesis (1.1.2). The form of the modified Euler factor at p is thus linked to the real form of G. This is reflected in the fact that the natural embedding of the Shimura variety attached to $G \times G$ in that attached to H in general does not define a map of Igusa towers. In order to pair p-adic modular forms on H with p-adic modular forms on $G \times G$, the natural embedding has to be replaced by a p-adic translation (cf. (2.1.11)), which is exactly what is needed to provide the expected modification of the Euler factor.

The main innovation of our construction concerns the zeta integral at p. As in [K], the use of a partial Fourier transform to define local data at p with the appropriate congruence properties to construct the Eisenstein measure is precisely what is needed to obtain the modified Euler factor at p directly as a local zeta integral, up to some volume factors. For $U(1)$, this was proved by Katz by direct computation. In general, we obtain the result as an immediate application of the local functional equation for the Godement-Jacquet integral representation of the standard L-function of $GL(n)$. These calculations are presented in Part II.

Why the present construction is not altogether satisfactory. The first reasons have to do with somewhat arbitrary restrictions on the scope of our result. We have only constructed the p-adic L-function for holomorphic automorphic forms of scalar weight. Moreover, for any fixed scalar weight, we have only studied the p-adic interpolation of the critical values at a fixed point s_0, though we allow the inertial characters at p to vary freely. Relaxing these restrictions would require the construction of the p-adic analogues of the classical non-holomorphic weight-raising operators of Maass, as in [K]. There is no doubt that Katz's constructions can be generalized, but the paper was already quite long without this additional generality, which is not necessary for our intended applications to Selmer groups. Moreover, although Garrett has determined the special values of the archimedean zeta integrals up to rational factors in general, his method does not permit identification up to p-adic units in general.[4]

As mentioned above, our choice of Eisenstein measure is insensitive to p-adic variation at ramified primes not dividing p, and the resulting p-adic L-function is missing its local Euler factors at the corresponding primes. A construction taking ramification away from p into account would probably require at the very least a p-integral version of the Godement-Jacquet theory of local zeta integrals

[4] Shimura calculates the archimedean zeta integrals precisely in [S97], but only for forms of scalar weight. His scalar weights, unlike those treated here, are non-constant functions on the set of real primes; thus he is forced to work with Maass operators.

(at primes not dividing p), based on Vignéras' modular representation theory of $GL(n)$ over local fields. We hope to return to this question in the future. Ignoring a finite number of Euler factors at places prime to p introduces a bounded error in expected applications to Selmer groups.

There are also local restrictions at primes dividing p. Working with general r-dimensional Hida families, we expect the values of our p-adic L-functions at algebraic (classical) points to be explicitly related to normalized special values of archimedean L-functions. The normalization involves dividing by a complex period invariant, to which we return momentarily. Our main results assert this to be the case under certain restrictions: at algebraic points corresponding to r-tuples of characters lying in a certain positive cone (the *regular* case); or when $r = 1$, where the Hida family is just the family of twists by characters composed with the determinant; or finally when $r \leq 2$ but only along an "anticyclotomic" direction. This is sufficient for our intended applications but is certainly less than optimal, and we hope to be able to relax at least the anticyclotomic condition in the final version of Part II. The restrictions allow us to identify the specialization of the Hida family at an algebraic point as an explicit vector in a principal series representation, which can then be used as a test vector in a local zeta integral.

The most serious defect of our construction is global. The conjectures of [Co] and [Pa] are expressed in the language of motives, and relate the special values of the p-adic L-function to the special values of the quotient of an archimedean L-function by a complex period invariant attached to the motive. In order for this relation to make sense, one needs to know that this quotient is an algebraic number, and so the statements of the conjectures of [Co] and [Pa] require Deligne's conjecture on the critical values of motivic L-functions as a preliminary hypothesis.[5] Our archimedean L-functions are attached to automorphic forms rather than to motives, and the period invariants are defined, as in Shimura's work, as (suitable algebraic multiples of) Petersson norms of arithmetic holomorphic modular forms on the appropriate Shimura varieties. The conjectural relation of these Petersson norms to Deligne's motivic periods, up to rational factors, is discussed in [H3], at least when the ground field is $\mathbb{Q}$. Partial results in this direction are obtained in [H4, H5], using an elaborate inductive argument, based on the theta correspondence, for establishing period relations between automorphic forms on unitary groups of different signatures. It is not beyond the realm of imagination that such techniques can eventually provide relations between Petersson norms up to integral factors, though it may well be beyond the limits of anyone's patience. Even the relatively favorable case of Shimura curves, where no products of periods are involved, required extraordinary efforts on the part of Prasanna [Pr]. However, and this is the most important point, even assuming integral period relations for Petersson norms, we still need to compare products of Petersson norms to motivic periods. When

[5] The more general conjectures of Perrin-Riou concern non-critical values of motivic L-functions, and the normalizing periods are defined by Beilinson's conjectures; in general, this is far beyond the scope of the automorphic theory as it presently stands.

$n = 2$ and the ground field is $\mathbb{Q}$, Hida realized long ago that the ratio of the Petersson norm to the motivic period generates the congruence ideal, and is itself the specialization of a p-adic L-function. When $n > 2$ we do not know how to use the automorphic theory to study the analogous ratios.

Contents of this paper.

To keep this first paper in the series to a reasonable length we have decided to break it into two parts. Part I, by recalling the theory of p-adic modular forms on unitary groups and constructing the Eisenstein measure, sets up the ground work for the construction of the p-adic L-functions.

More precisely, §1 recalls the theory of modular forms on unitary Shimura varieties, a theory ultimately due to Shimura but presented here in the setting of [H1]. We present the theory of p-adic modular forms on unitary Shimura varieties in §2, following Hida's generalization of the constructions of Deligne and Katz for $GL(2)$. Most of these results are at least implicitly due to Hida, but we have highlighted some special features adapted to the embedding of Igusa towers mentioned above. The calculation of the local coefficients at p of Eisenstein series occupies the greater part of §3, the rest of which is concerned with the local coefficients at the remaining places, and the relation of local to global coefficients, due essentially to Shimura. We conclude §3 with the construction of the Eisenstein measures.

Part II will develop Hida theory for p-adic modular forms on unitary groups G, carry out the related zeta-integral calculations from the doubling method, and complete the construction of p-adic L-functions. It will also establish a dictionary between the motivic and automorphic normalizations, and in particular will verify that the modified Euler factors at p are as predicted in [Co] and [Pa].

Acknowledgments

The authors, working on three separate continents, are grateful to the institutions that have provided us the opportunity to meet occasionally. Harris began working on this project in 2001, while visiting the Centre de Recerca Matemàtica at the Universitat Autònoma de Barcelona, and continued as a guest of the Hong Kong University of Science and Technology in 2001. Li and Skinner were guests of the Institut de Mathématiques de Jussieu in 2002 and 2003, respectively. Harris and Skinner were both invited to Harvard University in the spring of 2004.

It remains to express our thanks to the colleagues who have encouraged this project in its various manifestations. We thank Eric Urban, who corrected some of our initial misconceptions and thereby incited us to consider more general p-adic L-functions than we had originally intended to construct. Ching-Li Chai has patiently answered our many questions related to the theory of p-adic modular forms. We are especially grateful to Haruzo Hida, who has generously and unhestitatingly shared his expertise and advice since the beginning of our collaboration, and has been a permanent source of encouragement, while warning us that the project would be with us longer than we might have expected.

Finally, it is a special privilege and pleasure to dedicate this article to John Coates. His insights and taste have shaped our field for a generation; his generosity, especially in supporting young researchers, is unparalleled; and his personal charm is in large part responsible for making number theory a most enviable profession.

0. Notation and Conventions

Let G be a reductive algebraic group over the number field F. If v is a place of F we let $G_v = G(\mathbb{Q}_v)$; if v is archimedean we let $\mathfrak{g}_v = Lie(G_v)_{\mathbb{C}}$. We let G_∞ denote $\prod_{v|\infty} G_v$, the product being over all archimedean places of F, and let $\mathfrak{g}_\infty = \prod_{v|\infty} \mathfrak{g}_v$. In practice we will denote by K_∞ a subgroup of G_∞ which is maximal compact modulo the center of G.
We let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Thus for any number field L we identify the set Σ_L of complex embeddings of L with the set $Hom(L, \overline{\mathbb{Q}})$. Let $\mathbb{C}_p$ denote the completion of an algebraic closure of $\mathbb{Q}_p$, with integer ring $\mathcal{O}_{\mathbb{C}_p}$. We choose once and for all an embedding $incl_p : \overline{\mathbb{Q}} \rightarrow \mathbb{C}_p$, and let $\bar{\mathbb{Z}}_{(p)} = incl_p^{-1}(\mathcal{O}_{\mathbb{C}_p})$, the corresponding valuation ring. When necessary, we denote by $incl_\infty$ the given inclusion of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. Via this pair of inclusions, any embedding $\tau : L \rightarrow \mathbb{C}$ of a number field L gives rise to an embedding $\tau_p = incl_p \circ \tau : L \rightarrow \mathbb{C}_p$.

(0.1) Unitary groups over CM fields.

Let E be a totally real number field of degree d over $\mathbb{Q}$ and let $\mathcal{K}$ be a totally imaginary quadratic extension of E, with ring of integers $\mathcal{O}$. Let $c \in Gal(\mathcal{K}/E)$ denote the non-trivial automorphism, and $\varepsilon_{\mathcal{K}}$ the character of the idele classes of E associated to the quadratic extension $\mathcal{K}$. We fix a CM type of $\mathcal{K}$, i.e. a subset $\Sigma \subset \Sigma_{\mathcal{K}}$ such that $\Sigma \coprod \Sigma c = \Sigma_{\mathcal{K}}$.
Let V be an n-dimensional $\mathcal{K}$-vector space, endowed with a non-degenerate hermitian form $< \bullet, \bullet >_V$ relative to the extension $\mathcal{K}/E$. For each $\sigma \in \Sigma_{\mathcal{K}}$, $< \bullet, \bullet >_V$ defines a hermitian form $< \bullet, \bullet >_\sigma$ on the complex space $V_\sigma = V \otimes_{\mathcal{K},\sigma} \mathbb{C}$. We let (a_σ, b_σ) denote the signature of the form $< \bullet, \bullet >_\sigma$. Note that $(a_{c\sigma}, b_{c\sigma}) = (b_\sigma, a_\sigma)$ for all $\sigma \in \Sigma_{\mathcal{K}}$.
The hermitian pairing $< \bullet, \bullet >_V$ defines an involution $\tilde{c}$ on the algebra $End(V)$ via

$$< a(v), v' >_V = < v, a^{\tilde{c}}(v') >, \tag{0.1.1}$$

and this involution extends to $End(V \otimes_{\mathbb{Q}} R)$ for any $\mathbb{Q}$-algebra R. We define $\mathbb{Q}$-algebraic groups $U(V) = U(V, < \bullet, \bullet >_V)$ and $GU(V) = GU(V, < \bullet, \bullet >_V)$ over $\mathbb{Q}$ such that, for any $\mathbb{Q}$-algebra R,
(0.1.2)

$$U(V)(R) = \{g \in GL(V \otimes_{\mathbb{Q}} R) \mid g \cdot \tilde{c}(g) = 1\};$$
$$GU(V)(R) = \{g \in GL(V \otimes_{\mathbb{Q}} R) \mid g \cdot \tilde{c}(g) = \nu(g) \text{ for some } \nu(g) \in R^\times\}.$$

Thus $GU(V)$ admits a homomorphism $\nu : GU(V) \rightarrow \mathbb{G}_m$ with kernel $U(V)$. There is an algebraic group $U_E(V)$ over E such that $U(V) \xrightarrow{\sim} R_{E/\mathbb{Q}} U_E(V)$,

where $R_{E/\mathbb{Q}}$ denotes Weil's restriction of scalars functor. This isomorphism identifies automorphic representations of $U(V)$ and $U_E(V)$.
The groups $U(V)$ (resp. $GU(V)$) are all inner forms of the same quasi-split unitary group (resp. unitary similitude group), denoted U_0 (resp. GU_0). The group U_0 is of the form $U(D_0, \tilde{\chi}(*)_0)$ where D_0 is the matrix algebra and $\tilde{\chi}(*)_0$ is an appropriate involution. Then $U_{0,\infty} \cong U(\frac{n}{2}, \frac{n}{2})^{[E:\mathbb{Q}]}$ if n is even, $U_{0,\infty} \cong U(\frac{n-1}{2}, \frac{n+1}{2})^{[E:\mathbb{Q}]}$ if n is odd.

(0.2) Haar measures.
The bulk of this article and its companion, Part II, is devoted to calculations involving Fourier transforms, zeta integrals, and Petersson inner products of automorphic forms on the groups $U(V)$ of (0.1). The integrals are defined with respect to local and adelic Haar measures. The natural adelic Haar measure on $G = U_E(V)$ is Tamagawa measure $d^\tau g$, associated to an invariant top differential ω rational over E on G. Let $\delta(E)$ denote the discriminant of E. The adelic Tamagawa measure $d^\tau g$ factors up to normalization as a product of local measures

$$(0.2.1) \qquad d^\tau g = |\delta(E)|^{-\frac{\dim G}{2}} L(1, \varepsilon_{\mathcal{K}})^{-1} \prod_v d^\tau g_v$$

where $d^\tau g_v$ is the measure defined by ω_v if v is real and by $L_v(1, \varepsilon_{\mathcal{K}})\omega_v$ if v is finite. The Tamagawa number $\tau(G)$ of G is $vol(G(\mathbb{Q})\backslash G(\mathbf{A}), d^\tau g) = 2$. For finite v the volume of any compact open set with respect to $d^\tau g_v$ is always a rational number.
An alternative measure, traditionally used in the calculation of zeta integrals, is $dg = \prod_v dg_v$ where $dg_v = d^\tau g_v$ for archimedean v but dg_v is chosen to give volume 1 to a hyperspecial maximal compact subgroup K_v at almost all finite primes. Let S_G be the set of finite places v of E where ω_v is not an $\mathcal{O}_{E,v}$ generator of the module of top differentials; in particular, the group G is unramified at $v \notin S_G$ and so $G(E_v)$ has hyperspecial maximal compacts. The relation is

$$(0.2.2) \qquad d^\tau g_v = L_v(1, \varepsilon_{\mathcal{K}}) \cdot A_v(n) dg_v, \ A_v(n) = (q_v)^{-\dim G} \cdot |G_v(k_v)|$$

where G_v is the smooth reductive group scheme over $Spec(\mathcal{O}_{E,v})$ associated to the hyperspecial subgroup K_v. If for $v \in S_G$ (which includes the finite places where G has no hyperspecial maximal compact) we arbitrarily set $d^* g_v = dg_v$ for $v \in S_G$, then

$$(0.2.3) \quad vol(G(\mathbb{Q})\backslash G(\mathbf{A}), dg))/vol(G(\mathbb{Q})\backslash G(\mathbf{A}), d^\tau g) =$$
$$= |\delta(E)|^{\frac{\dim G}{2}} \cdot \prod_{v \notin S_G} A_v(n)^{-1} = \prod_{j=1}^{n} L^{S_G}(j, \varepsilon_{\mathcal{K}}^j)$$

where L^{S_G} denotes the partial L-function with the factors at S_G removed.

Given an open compact subgroup $K \subset G(\mathbf{A}_f)$, we let $d\mu_K(g)$ be the Haar measure that gives each connected component of ${}_KS(G) = G(\mathbb{Q})\backslash G(\mathbf{A})/K_\infty K$ total volume 1, for any maximal compact subgroup $K_\infty \subset G(\mathbb{R})$. When V is totally definite, so $G(\mathbb{R}) = K_\infty$, $d\mu_K(g)$ is counting measure on the finite set ${}_KS(G)$. In general,

$$d\mu_K(g) = \frac{\mathcal{C}(G,K)}{2} d^\tau g \tag{0.2.4}$$

where the class number $\mathcal{C}(G,K) = |\pi_0({}_KS(G)|$ can be determined explicitly.

1. Automorphic forms on unitary groups

(1.1) Ordinary primes for unitary groups.

Let $(V, < \bullet, \bullet >_V)$ be a hermitian pairing as in (0.1). Let p be a rational prime which is unramified in $\mathcal{K}$ (hence in particular in the associated reflex field $E(V)$), and such that every divisor of p in E splits completely in $\mathcal{K}$. Choose an inclusion $incl_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ as above. Composition with $incl_p$ defines an identification $\Sigma_{\mathcal{K}} \xrightarrow{\sim} Hom(\mathcal{K}, \mathbb{C}_p)$, hence for every $\tau \in Hom(\mathcal{K}, \mathbb{C}_p)$ we can define a signature

$$(a_\tau, b_\tau) = (a_\sigma, b_\sigma) \text{ if } \tau = incl_p \circ \sigma. \tag{1.1.1}$$

We assume the triple $(\Sigma, incl_p, (a_\sigma, b_\sigma)_{\sigma\in\Sigma_{\mathcal{K}}})$ to be *ordinary* in the following sense:

(1.1.2) Hypothesis. *Suppose $\sigma, \sigma' \in \Sigma$ have the property that $incl_p \circ \sigma$ and $incl_p \circ \sigma'$ define the same p-adic valuations. Then $a_\sigma = a_{\sigma'}$.*

When $a_\sigma = n$ for all $\sigma \in \Sigma$ – this is the *definite case*, to be described in detail later – or more generally, when $a_\sigma = a$ for all $\sigma \in \Sigma$ is constant, this comes down to the following hypothesis, used by Katz in the case $n = 1$:

(1.1.3) Hypothesis. *For $\sigma, \sigma' \in \Sigma$, the p-adic valuations defined by $incl_p \circ \sigma$ and $incl_p \circ \sigma' c$ are* distinct.

As Katz observes in [K], our hypotheses on p guarantee that Σ's satisfying (1.1.2) exist.

We let Σ_p denote the set $incl_p \circ \sigma \mid \sigma \in \Sigma\}$ of $\mathbb{C}_p$-embeddings of $\mathcal{K}$. Complex conjugation c acts on the set of primes of $\mathcal{K}$ dividing p, and the set of all such primes of $\mathcal{K}$ is the disjoint union

$$Hom(\mathcal{K}, \mathbb{C}_p) = \Sigma_p \coprod \Sigma_p c. \tag{1.1.4}$$

Hypothesis (1.1.2) was suggested by Fargues, who observed that it is equivalent to the condition that the completion of the reflex field of the Shimura variety attached to G (see §1.2) at the place defined by $incl_p$ is $\mathbb{Q}_p$. This is in turn equivalent, by a criterion of Wedhorn [We], to the condition that the ordinary locus of the completion of the Shimura variety at $incl_p$ is non-empty (see (2.1.7), below). We reformulate the elementary condition (1.1.2) in equally elementary terms. We have a canonical isomorphism $V_p \xrightarrow{\sim} \oplus_{w|p} V_w$ where $V_w = V \otimes_{\mathcal{K}} \mathcal{K}_w$. Let V_{p,Σ_p} and $V_{p,\Sigma_p c}$ be, respectively, the preimages of the subspaces $\oplus_{w|p,w\in\Sigma_p} V_w$ and $\oplus_{w|p,w\in\Sigma_p c} V_w$, where the notation $w \in \Sigma_p$ designates those w such that w is the valuation determined by some $\sigma_p \in \Sigma_p$. In particular,

$$(1.1.5) \qquad V_{p,\Sigma_p} \xrightarrow{\sim} \oplus_{w|p,w\in\Sigma_p} V_w.$$

The fact that all primes of E above p split in $\mathcal{K}/E$ is equivalent to the condition that the $\mathbb{Q}_p$-vector space $V_p = R_{\mathcal{K}/\mathbb{Q}} V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ decomposes $\mathbb{Q}_p$-rationally as $V_p = V_{p,\Sigma_p} \oplus V_{p,\Sigma_p c}$. The decomposition (1.1.5) is tautologically $\mathbb{Q}_p$-rational. For any w dividing p, let

$$\Sigma_w = \{\sigma \in \Sigma_{\mathcal{K}} \mid \sigma_p = w\}.$$

Equivalent to (1.1.2) is the hypothesis:

(1.1.6) Hypothesis. *There is a $\mathbb{Q}_p$-rational $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$-submodule $W(sig) \subset V_{p,\Sigma_p}$ (resp. $F^0 V_p \subset V_p$) such that $W(sig) = \oplus_{w|p,w\in\Sigma_p} W(sig)_w$ (resp. $F^0 V_p = \oplus_{w|p} F^0 V_w$) with $\dim W(sig)_w = a_\sigma$ for any $\sigma \in \Sigma$ (resp. $\dim F^0 V_w = a_\sigma$ for any $\sigma \in \Sigma_w$).*

In the definite case we just have $W(sig) = V_{p,\Sigma_p}$. Under hypothesis (1.1.2) we write $(a_w, b_w) = (a_\sigma, b_\sigma)$ for any $\sigma \in \Sigma_w$.

(1.2) Shimura varieties and automorphic vector bundles.

Let $(V, <\bullet,\bullet>_V)$ be an n-dimensional hermitian space over $\mathcal{K}$ as above. As in [H4], we let $-V$ denote the space V with hermitian form $<\bullet,\bullet>_{-V} = -<\bullet,\bullet>_V$ and $2V$ denote the doubled hermitian space $V \oplus (-V)$ with hermitian form the sum of $<\bullet,\bullet>_V$ and $<\bullet,\bullet>_{-V}$. We define $U(2V)$ and $GU(2V)$ as in (1.1); in particular, $GU(2V)$ denotes the *rational* similitude group.
The stabilizer in $U(2V)$ of the direct sum decomposition $2V = V \oplus (-V)$ is naturally isomorphic to the product $U(V) \times U(-V)$, embedded naturally in $U(2V)$. Similarly, the stabilizer in $GU(2V)$ is isomorphic to the subgroup $G(U(V) \times U(-V)) \subset GU(V) \times GU(-V)$, defined by

$$(1.2.1) \quad G(U(V) \times U(-V)) = \{(g, g') \in GU(V) \times GU(-V) \mid \nu(g) = \nu(g')\}.$$

Let $(W, <\bullet,\bullet>_W)$ be any hermitian space over $\mathcal{K}$. To the group $G = GU(W)$ one can canonically attach a Shimura datum (G, X), and hence a Shimura variety $Sh(W) = Sh(G, X)$, as follows. For each $\sigma \in \Sigma$, let (a_σ, b_σ) denote the signature of the hermitian form induced by $<\bullet,\bullet>_W$ on the complex space $W_\sigma = W \otimes_{\mathcal{K},\sigma} \mathbb{C}$. Let $GU(a_\sigma, b_\sigma) = GU(W_\sigma)$ denote the real unitary similitude group, and let X^{a_σ, b_σ} denote the $GU(a_\sigma, b_\sigma)(\mathbb{R})$-conjugacy class of homomorphisms $R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{m,\mathbb{C}} \rightarrow GU(a_\sigma, b_\sigma)$ defined in [H4, p. 143]. The product $X = X(W) = \prod_{\sigma\in\Sigma} X^{a_\sigma,b_\sigma}$ is naturally a $G(\mathbb{R})$-conjugacy class of homomorphisms $R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{m,\mathbb{R}} \rightarrow G_\mathbb{R}$, and the pair (G, X) satisfies the axioms of [D] defining a Shimura variety – unless W_σ is definite for all σ, in which case one can attach a zero-dimensional Shimura variety to (G, X) all the same, as in [H3]. We recall that the complex-valued points of $Sh(G, X)$ are given by

$$(1.2.2) \qquad Sh(G,X)(\mathbb{C}) = \varprojlim_K G(\mathbb{Q})\backslash X \times G(\mathbf{A}_f)/K,$$

where K runs over open compact subgroups of $G(\mathbf{A}_f)$. We let ${}_KSh(G, X)$ denote the associated variety whose complex points are given by $G(\mathbb{Q})\backslash X \times G(\mathbf{A}_f)/K$.

If W' is a second hermitian space, the above construction applies to groups of the form $G(U(W) \times U(W'))$, defined by analogy with (1.2.1), yielding a Shimura datum $(G(U(W) \times U(W')), X(W, W'))$. With the above conventions, it is immediate that the natural map $G(U(W) \times U(W')) \rightarrow GU(W \oplus W')$ defines a map of Shimura data $(G(U(W) \times U(W')), X(W, W')) \rightarrow G(U(W \oplus W')), X(W \oplus W'))$, hence a morphism of Shimura varieties

$$(1.2.3) \quad Sh(W,W') = Sh((G(U(W) \times U(W')), X(W,W'))) \rightarrow Sh(W \oplus W').$$

When $E = \mathbb{Q}$, this is worked out in detail in [H4]. In particular, we obtain a map

$$(1.2.4) \qquad Sh(V, -V) \rightarrow Sh(2V).$$

The group $GU(2V)$ is always quasi-split; in particular, up to isomorphism, it does not depend on the choice of V of dimension n. The corresponding Shimura variety always has a canonical model over $\mathbb{Q}$. The more general Shimura varieties $Sh(W)$, $Sh(W, W')$ are defined over reflex fields $E(W)$, $E(W, W')$, respectively, of which one can only say in general that they are contained in the Galois closure of $\mathcal{K}$ over $\mathbb{Q}$. It is easy to see, however, that $E(V, -V) = E(V)$, and the general theory of canonical models implies that the map (1.2.4) is rational over $E(V)$. If $E = \mathbb{Q}$ then $\mathcal{K}$ is a quadratic imaginary field, and $E(V) = \mathcal{K}$ unless V is quasi-split, in which case $E(V) = \mathbb{Q}$. When V is a definite hermitian space, $E(V)$ is the reflex field $E(\mathcal{K}, \Sigma)$ of the CM type $(\mathcal{K}, \Sigma)$.

We will be working with holomorphic automorphic forms on G, when G is of the form $G = GU(W)$ or $GU(W, W')$. These are constructed as follows; for details, see [H1]. Let $K_\infty \subset G(\mathbb{R})$ be the stabilizer of a point $x \in X$ $(= X(W)$ or $X(W, W'))$; thus K_∞ contains a maximal connected compact subgroup of $G(\mathbb{R})$, as well as the real points of the center Z_G of G. In fact, K_∞ is the group of real points of an algebraic subgroup, also denoted K_∞, of G, the centralizer of the torus $x(R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{m,\mathbb{C}})$. Moreover, the derived subgroup of G is simply connected, hence K_∞ is connected. Hence one can speak of algebraic representations of K_∞ and their extreme weights. If $\tau : K_\infty \rightarrow GL(W_\tau)$ is an algebraic representation, then there exists a holomorphic vector bundle $[W_\tau]$ on $Sh(G,X)$; more precisely, there exists a canonical holomorphic structure on the C^∞ vector bundle

$$[W_\tau] = \varprojlim_K G(\mathbb{Q})\backslash G(\mathbb{R}) \times W_\tau \times G(\mathbf{A}_f)/K_\infty K, \tag{1.2.5}$$

where K_∞ acts on the right on $G(\mathbb{R})$ and on the left on W_τ, yielding a natural map to

$$\varprojlim_K G(\mathbb{Q})\backslash G(\mathbb{R}) \times G(\mathbf{A}_f)/K_\infty K = \varprojlim_K G(\mathbb{Q})\backslash X \times G(\mathbf{A}_f)/K = Sh(G,X)(\mathbb{C}).$$

A holomorphic automorphic form on G of type τ is a global section $f \in H^0(Sh(G,X),[W_\tau])$; when G contains a rational normal subgroup isogenous to $SL(2)_{\mathbb{Q}}$ one needs to add a growth condition at infinity. The representation τ is included in the notation for $[W_\tau]$, but is superfluous; $[W_\tau]$ can be defined without reference to a choice of K_∞ (or, equivalently, a choice of $p \in X$), and has a canonical model rational over a number field $E(W_\tau)$, containing the reflex field $E(G,X)$, and attached canonically to the set of extreme weights of W_τ. In particular, the space $H^0(Sh(G,X),[W_\tau])$ has a canonical rational structure over $E(W_\tau)$. However, since we have chosen K_∞, we can also realize holomorphic automorphic forms of type τ as W_τ-valued functions on the adèle group of G via (1.2.5). Let $\mathcal{A}(G)$ denote the space of automorphic forms on $G(\mathbb{Q})\backslash G(\mathbf{A})$. Then

(1.2.6)

$$H^0(Sh(G,X),[W_\tau]) \xrightarrow{\sim} \mathcal{A}_{hol,\tau}(G) := \{f \in (\mathcal{A}(G)\otimes W_\tau)^{K_\infty} \mid \mathfrak{p}^- f = 0\},$$

canonically. Here

$$\mathfrak{g}_\infty = Lie(K_\infty)_{\mathbb{C}} \oplus \mathfrak{p}^- \oplus \mathfrak{p}^+ \tag{1.2.7}$$

is the Harish-Chandra decomposition, and the choice a base point $x \in X$, and hence K_∞ and the decomposition (1.2.7), is implicit in the notation $\mathcal{A}_{hol,\tau}(G)$. We also write the right-hand side of (1.2.6) as

$$(\mathcal{A}(G)\otimes W_\tau)^{K_\infty}[\mathfrak{p}^-],$$

the $\mathfrak{p}^-$-torsion in $(\mathcal{A}(G)\otimes W_\tau)^{K_\infty}$.

If $X = X(V,-V)$ with V a definite hermitian space, then $K_\infty = GU(V,-V)(\mathbb{R})$. If $X = X(2V)$, with V again definite, we can take K_∞ to be $GU(V,-V)(\mathbb{R}) \subset GU(2V)$. With this choice, the Harish-Chandra decomposition (1.2.7) is rational over $E(V,-V) = E(V) = E(\mathcal{K},\Sigma)$.

Restricting forms.

Let $G = GU(V,-V)$, $X = X(V,-V)$, $G' = GU(2V)$, and $X' = X(2V)$. Pick $x \in X(V,-V)$. This determines a base point in X' and hence $K'_\infty \subseteq G'_\infty$

in addition to K_∞, with K_∞ being identified with a subgroup of K'_∞ via the canonical embedding of G into G'.
Suppose τ is a one-dimensional representation of K'_∞. This then determines a one-dimensional representation of K_∞ by restriction, and we obtain holomorphic vector bundles $[W\tau]$ and $[W'_\tau]$ on $Sh(V,-V) = Sh(G,X)$ and $Sh(2V) = Sh(G',X')$, respectively, having canonical models over the respective fields $E(W_\tau)$ and $E(W'_\tau)$. There is canonical map from the pull-back of $[W'_\tau]$ under the morphism (1.2.4) to $[W_\tau]$ and therefore a homomorphism:

$$(1.2.8) \qquad \mathrm{res}_{V,\tau} : H^0(Sh(2V), [W'_\tau]) \to H^0(Sh(V,-V), [W_\tau]).$$

This is rational over $E(W_\tau)$. Over the complex numbers (1.2.8) is compatible in the obvious way with the isomorphisms in (1.2.6) and the restriction of forms in $\mathcal{A}_{hol,\tau}(G')$ to $G(\mathbf{A})$, which gives forms in $\mathcal{A}_{hol,\tau}(G)$.

Connected components.

We let $G = GU(V)$. Let C denote the algebraic group G/G^{der} over $\mathbb{Q}$. Let $G(\mathbb{R})^+$ denote the identity component of $G(\mathbb{R})$, $G(\mathbb{Q})^+ = G(\mathbb{Q}) \cap G(\mathbb{R})^+$. For any open compact subgroup $K \subset G(\mathbf{A}_f)$, the set $\pi_0({}_KSh(G,X)(\mathbb{C}))$ of connected components of ${}_KSh(G,X)(\mathbb{C})$ is given by $\overline{G(\mathbb{Q})^+}\backslash G(\mathbf{A}_f)/K$, where $\overline{G(\mathbb{Q})^+}$ denotes the closure of $G(\mathbb{Q})^+$ in $G(\mathbf{A}_f)$. Let $C_K \subset C(\mathbf{A}_f)$ denote the image of K under the natural map; let $C^+ \subset C(\mathbf{A}_f)$ denote the image of $G(\mathbb{Q})^+$. Now G^{der} is an inner form of the simply-connected group $SL(n)$, hence satisfies strong approximation. It follows (cf. [D, (2.1.3.1)]) that

$$(1.2.9) \qquad \pi_0({}_KSh(G,X)(\mathbb{C})) = C(K) \overset{def.}{=} C(\mathbf{A}_f)/C_K \cdot C^+.$$

We can define a Shimura datum $(C, X(C))$ to be the quotient of (G,X) by G^{der}. The corresponding Shimura variety $Sh(C,X(C))$ also has a modular interpretation in terms of level structures on certain direct factors of rank one over $\mathcal{K}$ of certain tensor powers of the Tate modules of abelian varieties with CM by $\mathcal{K}$. The tensor power in question depends on the signatures (a_σ, b_σ). The natural map ${}_KSh(G,X)(\mathbb{C}) \to C(K) = \pi_0({}_KSh(G,X)(\mathbb{C}))$ becomes a morphism of moduli spaces. This interpretation will not be used in the sequel.

(1.3) PEL STRUCTURES.

Let $G = GU(V)$. Notation is as in the previous section. Write

$$\mathcal{K} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = \oplus_{\sigma\in\Sigma_{\mathcal{K}}} \overline{\mathbb{Q}}\sigma,$$

and let $e_\sigma \in \mathcal{K} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ be the corresponding orthogonal idempotents. We decompose $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ as a $\mathcal{K} \otimes \mathbb{Q}\overline{\mathbb{Q}}$-module as $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = V_\Sigma \oplus \mathcal{V}_{\Sigma c}$, where $\mathcal{V}_\Sigma$ is the sum of the spaces $V_\sigma = e_\sigma(V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})$ for $\sigma \in \Sigma$, and similarly for $V_{\Sigma c}$. Inside $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ we consider a variable $\mathcal{K} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$- submodule F^0V satisfying

(1.3.0) Property. *For any $\sigma \in \Sigma_{\mathcal{K}}$, the projection $F^0V_\sigma = e_\sigma F^0V$ of F^0V on V_σ is of dimension a_σ.*

Let T be an indeterminate and, for $x \in \mathcal{K}$, let $P_0(x,T) \in \overline{\mathbb{Q}}[T]$ denote the characteristic polynomial of x, acting on F^0V. It follows from the definition of the reflex field $E(V)$ that $P_\Sigma(x,T) \in E(V)[T]$, independently of the choice of F^0V. Indeed, Shimura defined $E(V)$ to be the field generated by traces of elements of $\mathcal{K}$ acting on F^0V.

Choose a purely imaginary element $\beth \in \mathcal{K}$, i.e. an element such that $Tr_{\mathcal{K}/E}(\beth) = 0$. The form $< \bullet, \bullet >_{V,\beth} = \beth \cdot < \bullet, \bullet >_V$ is skew-hermitian. When we fix a prime p we will always assume $\beth$ to be a unit at p. Fix a compact open subgroup $K \subset GU(V)(\mathbf{A}_f)$. We consider the following functor from the category of schemes over $E(V)$ to the category of sets:

$$S \mapsto {}_K\mathcal{A}_V(S) = {}_K\mathcal{A}_{V,\beth}(S) = \{(A, \lambda, \iota, \alpha)\} \tag{1.3.1}$$

where

(1.3.1.1) A is an abelian scheme over S, viewed as an abelian scheme up to isogeny;

(1.3.1.2) $\lambda : A \to \hat{A}$ is a polarization;

(1.3.1.3) $\iota : \mathcal{K} \to End_S(A) \otimes \mathbb{Q}$ is an embedding of $\mathbb{Q}$-algebras;

(1.3.1.4) $\alpha : V(\mathbf{A}_f) \xrightarrow{\sim} V^f(A)$ is an isomorphism of $\mathcal{K}$-spaces, modulo K.

Here $V^f(A) = \prod_\ell T_\ell(A) \otimes \mathbb{Q}$ is the adelic Tate module, viewed as a ind-pro-étale sheaf over S; it's $\mathcal{K}$-structure comes from (1.2.1.3). The level K structure of (1.3.1.4) is understood in the sense of Kottwitz [Ko]. These data satisfy the usual compatibility conditions:

(1.3.1.5) The Rosati involution on $End_S(A) \otimes \mathbb{Q}$ defined by λ fixes $\iota(\mathcal{K})$ and acts as complex conjugation;

(1.3.1.6) The isomorphism α identifies the Weil pairing on $V^f(A)$ with an ${\mathbf{A}_f}^\times$-multiple of the skew-symmetric pairing on $V(\mathbf{A}_f)$ defined by $tr_{\mathcal{K}/\mathbb{Q}} < \bullet, \bullet >_{V,\beth}$.

Finally, the action induced by ι on $Lie_{A/S}$ satisfies Shimura's trace condition, which we state here in the equivalent formulation due to Kottwitz. Let $P_\iota(x,T) \in \mathcal{O}_S[T]$ denote the characteristic polynomial of x, acting on $Lie(A/S)$. We view $E(V)[T]$ as a subalgebra of $\mathcal{O}_S[T]$. The Shimura-Kottwitz condition is

$$P_\iota(x,T) = P_0(x,T) \in \mathcal{O}_S[T], \ \forall x \in \mathcal{K}. \tag{1.3.1.7}$$

Two quadruples $(A, \lambda, \iota, \alpha)$ and $(A', \lambda', \iota', \alpha')$ are identified if and only if there is an isogeny $\phi : A \to A'$, commuting with ι', prime to the level K in the obvious sense and taking α to α', and identifying λ' with a positive rational multiple of λ.

(1.3.2) THEOREM (SHIMURA). *For K sufficiently small, the functor (1.3.1) is representable by a quasi-projective scheme over $E(V)$, and this is precisely the canonical model of ${}_KSh(V)$. As K varies, the natural maps between these functors induce the natural maps between the various ${}_KSh(V)$. The action of $GU(V)(\mathbf{A}_f)$ on the tower ${}_KSh(V)$ preserves the $E(V)$-rational structure.*

For $U \subset GU(V)(\mathbf{A}_f)$ a closed compact subgroup, we write ${}_USh(V) = \varprojlim_{K\supset U} {}_KSh(V)$, as K runs over compact open subgroups of $GU(V)(\mathbf{A}_f)$. This is simply a shorthand for referring to the full tower of the ${}_KSh(V)$ for $K \subset U$, and we will not need to worry about the nature of the projective limit.

The above theory applies in particular to the Shimura varieties $Sh(2V)$ and $Sh(V) \times Sh(-V)$. The Shimura variety $Sh(V, -V)$ is defined as the subvariety of $Sh(V) \times Sh(-V)$, which parametrizes pairs of quadruples $((A, \lambda, \iota, \alpha), (A^-, \lambda^-, \iota^-, \alpha^-))$, determined by compatibility of polarizations in the obvious sense. As a subvariety of $Sh(2V)$, $Sh(V) \times Sh(-V)$ is then the set of quadruples (B, μ, ι_2, β) which decompose as a product

$$(B, \mu, \iota_2, \beta) \xrightarrow{\sim} (A \times A^-, \lambda \times \lambda^-, \iota \times \iota^-, \alpha \times \alpha^-).$$

In particular, β respects the $\mathbf{A}_{\mathcal{K},f}$-decomposition $2V(\mathbf{A}_f) = V(\mathbf{A}_f) \oplus (-V)(\mathbf{A}_f)$. The most important level structures β for our purposes do not, however, respect this decomposition. In other words, in the applications, we will not be working with the Shimura variety $Sh(V, -V)$ via its natural embedding in $Sh(2V)$, but rather with a translate of the latter, cf. (2.1.11).

For the remainder of this section, let $G = GU(V)$, $X = X(V)$, $Sh = Sh(G, X)$. We identify

$$GU(V)(\mathbb{Q}_p) = U(V)(\mathbb{Q}_p) \times {\mathbb{Q}_p}^\times \xrightarrow{\sim} U_E(V)(E \otimes_{\mathbb{Q}} \mathbb{Q}_p) \times {\mathbb{Q}_p}^\times,$$

where the map to ${\mathbb{Q}_p}^\times$ is the similitude factor and $U_E(V)$ is as in (0.1). The ordinarity hypothesis (1.1.2) allows us to define subspaces V_{p,Σ_p} and $V_{p,c\cdot\Sigma_p}$ of V_p as in (1.1.5). The hermitian pairing

$$V_p \times V_p \to E \otimes \mathbb{Q}_p$$

determines, and is determined by, a perfect duality $V_{p,\Sigma_p} \otimes V_{p,c\cdot\Sigma_p} \to E \otimes_{\mathbb{Q}} (\mathbb{Q}_p)$ of free $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{w\in\Sigma_p} \mathcal{K}_w$-modules. There is thus a natural isomorphism

$$G(\mathbb{Q}_p) \xrightarrow{\sim} GL(V_{p,\Sigma_p}) \times {\mathbb{Q}_p}^\times \xrightarrow{\sim} \prod_{w,\Sigma_w\subset\Sigma_p} GL(n, \mathcal{K}_w) \times \mathbb{Q}_p^\times \tag{1.3.3}$$

The indexing by w such that $\Sigma_w \subset \Sigma_p$ is a reminder of the fact that several elements of Σ_p can correspond to the same divisor w of p. This is just a way of saying, somewhat more carefully than usual, that the unitary group at a split place is isomorphic to a general linear group. We identify $G_{\mathbb{Q}_p}$ with the product of algebraic groups $G_0 \times GL(1)$, where $G_0 = GL(V_{p,\Sigma_p})$ as algebraic groups and the map to $GL(1)$, as before, is the similitude factor ν.

Fix a compact open subgroup $K = K_p \times K^p \subset G(\mathbf{A}_f)$, with $K_p \subset G(\mathbb{Q}_p)$, $K^p \subset G(\mathbf{A}_f^p)$, and let ${}_KSh$ denote the Shimura variety at level K. Our hypotheses imply that $G_{\mathbb{Q}_p}$ is an unramified group over $\mathbb{Q}_p$, hence that $G(\mathbb{Q}_p)$ contains hyperspecial maximal compact subgroups; we assume that K_p is one such. Then K_p is the group of $\mathbb{Z}_p$-points of an extension of G to a smooth group scheme, also denoted G, over $Spec(\mathbb{Z}_p)$. The choice of K_p is equivalent to the choice of a self-dual $\mathcal{O} \otimes \mathbb{Z}_p$-lattice $M_V \subset V_p$. Let $M_{V,\Sigma_p} \subset V_{p,\Sigma_p}$ be the projection of M_V. We can extend G_0 to a group scheme over $\mathbb{Z}_p$ as $G_0 = GL(M_{V,\Sigma_p})$. Then there are isomorphisms

$$(1.3.4) \qquad K_p = G(\mathbb{Z}_p) \xrightarrow{\sim} G_0(\mathbb{Z}_p) \times GL(1, \mathbb{Z}_p) = \prod_{w, \Sigma_w \subset \Sigma_p} GL(n, \mathcal{O}_w) \times \mathbb{Z}_p^\times$$

compatible with the factorization (1.3.3). We also assume K^p is sufficiently small, in a sense we will make precise later.

When $G = G(2V) \supset G(V, -V)$, we choose K_p so that $M_{2V} = M_V \oplus M_{-V}$ with $M_V \subset V \otimes \mathbb{Q}_p$ and $M_{-V} \subset (-V) \otimes \mathbb{Q}_p$ self-dual lattices; this is equivalent to the assumption that $K_p \cap G(V, -V)(\mathbb{Q}_p)$ is a hyperspecial maximal compact subgroup of $G(V, -V)(\mathbb{Q}_p)$. In (2.1) we will impose additional conditions on the choice of M_V in the general case.

(1.4) Automorphic vector bundles on unitary Shimura varieties, again.

Notation is as in the previous sections: $G = GU(2V)$, resp. $GU(V, -V)$, $X = X(2V)$, resp. $X(V, -V)$, and $[W_\tau]$ is an automorphic vector bundle on $Sh(G, X)$.

In (1.2) we have fixed the stabilizer $K_\infty \subset G(\mathbb{R})$ of a point $x \in X$. Choose a maximal torus $T_\infty \subset K_\infty$, an algebraic subgroup over $\mathbb{R}$ necessarily containing the image of x. Then T_∞ is also a maximal torus in G. A specific choice of pair (T_∞, K_∞) can be obtained as follows. Decompose $(V, < \bullet, \bullet >_V)$ as an orthogonal direct sum of one-dimensional hermitian spaces over $\mathcal{K}$:

$$(1.4.1) \qquad (V, < \bullet, \bullet >_V) = \oplus_{i=1}^n (V_i, < \bullet, \bullet >_i).$$

We assume the V_i are numbered so that, for any $\sigma \in \Sigma$, $V_{i,\sigma} = V_i \otimes_{\mathcal{K},\sigma} \mathbb{C}$ has signature $(1,0)$ for $i \leq r_\sigma$ and signature $(0,1)$ for $i > r_\sigma$. Let $-V_i$ denote V_i with the hermitian form $- < \bullet, \bullet >_i$. Let $GU^{\oplus_i}(V, -V)$ denote the subgroup of the torus $\prod_i GU(V_i) \times \prod_i GU(-V_i)$ defined by equality of similitude factors. We obtain embeddings of Shimura data

(1.4.2)

$$(GU^{\oplus_i}(V, -V), \prod_i (X_i \times X_i')) \hookrightarrow (GU(V, -V), X(V, -V)) \hookrightarrow (GU(2V), X(2V))$$

where $\prod_i (X_i \times X_i')$ is an appropriate product of point symmetric spaces determined by the signatures of each V_i and $-V_i$. We write

$$Sh^{\oplus_i}(V,-V) = Sh(GU^{\oplus_i}(V,-V), \prod_i (X_i \times X_i')),$$

the superscript ${}^{\oplus_i}$ serving as a reminder of the choice of direct sum decomposition above. Define $(GU^{\oplus_i}(V), \prod_i X_i) \subset (GU(V), X(V))$, $GU^{\oplus_i}(-V), \prod_i X_i') \subset (GU(-V), X(-V))$ analogously. The groups $GU^{\oplus_i}(V)$, $GU^{\oplus_i}(-V)$, and $GU^{\oplus_i}(V,-V)$, defined over $\mathbb{Q}$, are maximal $\mathbb{R}$-elliptic tori in $GU(V)$, $GU(-V)$, and $GU(V,-V)$ or $GU(2V)$, and we take T_∞ to be the group of real points of one of these tori. We can of course find K_∞ containing T_∞, though K_∞ will in general not be defined over $\mathbb{Q}$. The Shimura data $(GU^{\oplus_i}(V), \prod_i X_i)$, etc., define CM points of the corresponding unitary Shimura varieties.

The group T_∞ is a maximal torus in a reductive group of type A, and we parametrize its roots in the usual way. In the case $G = GU(V)$, $G_{\mathbb{C}}$ is naturally isomorphic to $\prod_{\sigma\in\Sigma} GL(n,\mathbb{C}) \times GL(1,\mathbb{C})$, the last term coming from the similitude factor. Thus the group $X(T_\infty)$ of characters λ of the algebraic torus T_∞ consists of d-tuples $(a_{1,\sigma},\dots,a_{n,\sigma})_{\sigma\in\Sigma}$ of n-tuples of integers, indexed by $\sigma \in \Sigma$, together with a single integer a_0 for the similitude factor. The $(a_{j,\sigma})$ are given by the restriction of the character λ to $T_\infty \cap U(V)$, whereas a_0 is given by the restriction of λ to the maximal $\mathbb{R}$-split torus in $T_\infty \cap Z_G$: if $tI_n \in G(\mathbb{R})$ is a real central element then $\lambda(tI_n) = t^{a_0}$. The parameters satisfy the relation

$$a_0 \equiv \sum_{j,\sigma} a_{j,\sigma} \pmod 2. \tag{1.4.3}$$

Given an ordering on the roots of the maximal torus $T_\infty \subset G$, the dominant weights are then the characters parametrized as above, with $a_{i,\sigma} \geq a_{i+1,\sigma}$, for all σ and $i = 1,\dots,n-1$. We choose a set of positive roots containing the roots in $\mathfrak{p}^-$. The n-tuple corresponding to σ will often be written with a semi-colon $(a_{1,\sigma},\dots,a_{a_\sigma,\sigma}; -b_{b_\sigma,\sigma},\dots,-b_{1,\sigma})$ or occasionally $(a_{1,\sigma},\dots,a_{a_\sigma,\sigma}; -b_{b_\sigma,\sigma},\dots,-b_{1,\sigma}; a_0)$ when the term a_0 needs to be stressed, in such a way that it gives a dominant weight of the σ-factor of $K_\infty \cap U(V)_\infty$, $U(V)_\infty \equiv \prod_\sigma U(a_\sigma, b_\sigma)$ if and only if

$$a_{1,\sigma} \geq \cdots \geq a_{a_\sigma,\sigma},\ b_{1,\sigma} \geq \cdots \geq b_{b_\sigma,\sigma} \tag{1.4.4}$$

The parametrization in $G = GU(2V)$ is the same as above, except that n is replaced by $2n$ and $a_\sigma = b_\sigma = n$. For $G = GU(V,-V)$, we place the parameters for $GU(V)$ and $GU(-V)$ side by side.

If K is sufficiently small, ${}_KSh(V)$ carries a universal abelian scheme ${}_KA$ endowed with PEL structure of the appropriate type. Let $p_K : {}_KA \to {}_KSh(V)$ denote the structure map and put

$$\omega = \omega_V = p_{K,*}\Omega^1_{{}_KA/{}_KSh(V)}.$$

This is a locally-free sheaf on ${}_KSh(V)$ of rank $dn = [E : \mathbb{Q}]\dim_{\mathcal{K}} V$ with a natural action of $\mathcal{O}_{{}_KSh(V)} \otimes_{\mathbb{Q}} \mathcal{K}$, the $\mathcal{K}$-action coming from (1.3.1.3). If we extend the ground field to contain E, then ω breaks up as $\omega = \oplus_{\sigma\in\Sigma}\omega_\sigma$ corresponding to the canonical decomposition $E \otimes_{\mathbb{Q}} \mathcal{K} = \oplus_{\sigma\in\Sigma}\mathcal{K}$. Each ω_σ is a locally-free $\mathcal{O}_{{}_KSh(V)}$-sheaf of rank n. The sheaf $\otimes_{\sigma\in\Sigma}\omega_\sigma$ is the canonical bundle associated to $(0, ..., 0; 1, 0, ..., 0; 1)_{\sigma\in\Sigma}$.

The canonical bundles for other τ's can be constructed as follows, again assuming the ground field contains E. Let $Fl(\omega_\sigma)_{{}_KSh(V)}$ be the scheme representing the functor

$$S \mapsto (\mathcal{E}_1 = \omega_{\sigma/S} \supset \mathcal{E}_2 \supset \cdots \supset \mathcal{E}_n \supset \mathcal{E}_{n+1} = 0 \; ; \qquad \phi_i : \mathcal{E}_i/\mathcal{E}_{i+1} \xrightarrow{\sim} \mathcal{O}_S, i = 1, ..., n).$$

There is an obvious action of $D_\sigma = \mathbb{G}^n_{m/{}_KSh(V)}$ on $FL(\omega_\sigma)$: $d = (d_1, ..., d_n)$ acts by multiplying ϕ_i by d_i. Let $\pi_\sigma : FL(\omega_\sigma) \to {}_KSh(V)$ be the structure map. For each $\tau_\sigma \in X(D_\sigma)$ we define a locally-free sheaf ρ_{τ_σ} on ${}_KSh(V)$ by $H^0(U, \rho_{\tau_\sigma}) = H^0(\pi_\sigma^{-1}(U), \mathcal{O}_{FL(\omega_\sigma)})[\tau_\sigma]$, where the $[\tau_\sigma]$ signifies the submodule on which D_σ acts through τ_σ. We identify each τ_σ with an n-tuple of integers $(m_{1,\sigma}, ..., m_{n,\sigma})$ in the usual way and say that such a τ_σ is dominant if $m_{1,\sigma} \geq \cdots \geq m_{n,\sigma}$. Given a d-tuple $\tau = (\tau_\sigma)_{\sigma\in\Sigma}$ of dominant characters, let $\rho_\tau = \otimes_{\sigma\in\Sigma}\rho_{\tau_\sigma}$. Then we can naturally identify ρ_τ with $[W_\tau]$, where the character of T_∞ associated to τ is $(m_{1,\sigma}, ..., m_{a_\sigma,\sigma}; m_{a_\sigma+1,\sigma}, ..., m_{n,\sigma})$. These identifications respect the maps in (1.2.8) in the obvious way.

(1.5) Fourier expansions of modular forms.

In this section we consider the Shimura datum $(GU(2V), X(2V))$. The symmetric domain $X(2V)$ is holomorphically isomorphic to the product of $[E : \mathbb{Q}] = |\Sigma|$ copies of the irreducible tube domain $X_{n,n}$ of dimension n^2 attached to the group $U(n, n)$. Let $P = P_\Delta \subset G$ be the maximal parabolic defined in §1.5. The group of real points of P stabilizes the 0-dimensional boundary component of this product of tube domains. Fourier expansion with respect to $U(\mathbb{R})$ defines the q-expansion of a holomorphic automorphic form on X relative to a congruence subgroup of $GU(2V, \mathbb{Q})$. By work of Fujiwara [F], extending the results of Chai and Faltings, one can also define q-expansions for sections of the automorphic vector bundles $[W_\tau]$ over ${}_K\mathbb{S}$ when K_p is hyperspecial. In [Hi04, Hi05], Hida defined q-expansions on the closed Igusa tower. We will formulate this theory in an adelic version analogous to the characteristic zero formulation in [H1, §6] and [P].

In [H1, §6] we attach a Shimura datum (G_P, X_P) to the rational parabolic subgroup $P \subset GU(2V)$. The domain X_P is a version of the point boundary component mentioned above, and G_P is a torus; specifically, G_P is contained in the center of the standard Levi component of P. Recall the definition of G_P: the standard rational representation of G on $R_{\mathcal{K}/\mathbb{Q}}(2V)$ carries a family of Hodge structures of type $(-1, 0) + (0, -1)$, corresponding to the family of abelian varieties of PEL type over $Sh(2V)$. In a neighborhood of the boundary component corresponding to P, this family degenerates to a mixed Hodge structure of type $(0,0)+(-1,-1)$.

Actually, the formulation in [H1] is not quite correct: in general the boundary Shimura datum should be defined as in [Pink], where X_P is a homogeneous space for $G_P(\mathbb{R})$ finitely fibered over a $G_P(\mathbb{R})$ conjugacy class of homomorphisms $R_{\mathbb{C}/\mathbb{R}} \to G_{P,\mathbb{R}}$. In the present case, $G_P(\mathbb{R})$ has two connected components, corresponding to upper and lower hermitian half-spaces, and X_P consists of two points. The Shimura variety $Sh(G_P, X_P)$ is zero-dimensional, and one easily verifies it is of PEL type.

Indeed, it parametrizes pairs $(\alpha_\Sigma, \alpha_m)$ where α_Σ is a complete level structure on the abelian variety with complex multiplication type $(\mathcal{K}, \Sigma)$, and α_m is an isomorphism

$$\alpha_m : \prod_q \mathbb{Q}_q/\mathbb{Z}_q \xrightarrow{\sim} \prod_q \mu_{q^\infty}$$

Thus as long as one works in finite level K_P prime to p, there is no difficulty defining an integral model ${}_{K_P}\mathbb{S}(G_P)$ of ${}_{K_P}Sh(G_P, X_P)$. For general level K_P, there is a unique normal integral model, and we define this to be ${}_{K_P}\mathbb{S}(G_P)$.

We let U_P denote the unipotent radical of P, and let $U^* = Hom(U_P(\mathbb{Q}), \mathbb{Q})$. This is the vector space denoted $\mathfrak{g}^{-2}(\mathbb{Q})^*$ in [H1,]. The space $U^* \otimes \mathbb{R}$ contains a self-adjoint cone, homogeneous under $P(\mathbb{R})/U_P(\mathbb{R})$, and denoted C in [H1, 5.1]; we let $U^*(C) = U^* \cap C$. Let $[W_\tau]$ be an automorphic vector bundle over $\bar{S}$, as above. There is an automorphic vector bundle $[W_{\tau_P}]$ over $Sh(G_P, X_P)$, and a map

$$F.J.^{P,0} : \Gamma(Sh(2V), [W_\tau]) \to \hat{\bigoplus_{\beta \in U^*}} \Gamma(Sh(G_P, X_P), [W_{\tau_P}]) \tag{1.5.1}$$

defined, with slightly different notation, in [H1, (6.3.3)], and in [Pink, §12]. Here $\hat{\bigoplus}$ is understood as the subset (f_β) of the direct product over $\beta \in U^*$ such that $f_\alpha = 0$ for all but finitely many $\beta \notin U^*(C)$. If $F.J.^{P,0}(f) = (f_\beta)$ for some $f \in \Gamma(Sh(2V), [W_\tau])$, then the usual Fourier expansion is written $\sum f_\beta q^\beta$. The Koecher principle asserts that, for $n > 0$, $F.J.^{P,0}$ is supported on $U^*(C)$, and even for $n = 0$ one takes care only to consider f with that property.

Since C is self-adjoint, it can also be viewed as a cone in $U_P(\mathbb{R})$. One obtains a more reassuring variant of the q-expansion in the following way. Let $N = \dim U_P$, and let

$$\Lambda = \Lambda(K^p) = U_P(\mathbb{Q}) \cap K(U, m) \subset U_P(\mathbb{Q}). \tag{1.5.2}$$

Note that Λ is a lattice in $U_P(\mathbb{Q})$ and does not depend on m. We choose a polyhedral cone $\mathfrak{c} \subset C$ generated by a basis $\{\lambda_1, \ldots, \lambda_N\}$ of Λ:

$$\mathfrak{c} = \{\sum_{i=1}^N a_i \lambda_i \mid a_i \geq 0\}$$

and let $\mathfrak{c}^* \supset U^*(C)$ be the dual cone:

$$\mathfrak{c}^* = \{v \in U^*(C) \mid v(\lambda_i) \geq 0, i = 1, \ldots N\}.$$

Let $\Lambda^* = Hom(\Lambda, \mathbb{Z})$, viewed as a subgroup of $U^*(C)$. Let R be a $\mathcal{O}_v$-algebra and $\mathcal{M}$ a free R-module. The intersection $\Lambda^* \cap \mathfrak{c}^*$ is a free monoid on N generators β_i, $i = i, \ldots, N$, and the ring of formal series

$$R[[q^{\Lambda^* \cap \mathfrak{c}^*}]] = \{\sum_{\beta \in \Lambda^* \cap \mathfrak{c}^*} f_\beta q^\beta\}, \tag{1.5.3}$$

with $f_\beta \in R$, and with the usual multiplication rule $q^\beta \cdot q^{\beta'} = q^{\beta + \beta'}$, is then isomorphic to $R[[q^{\beta_1}, \ldots q^{\beta_N}]]$. We define the $R[[q^{\Lambda^* \cap \mathfrak{c}^*}]]$-module

$$\mathcal{M}[[q^{\Lambda^* \cap \mathfrak{c}^*}]] = \mathcal{M} \otimes_R R[[q^{\Lambda^* \cap \mathfrak{c}^*}]] = \{\sum_{\beta \in \Lambda^* \cap \mathfrak{c}^*} f_\beta q^\beta\}$$

where now $f_\beta \in \mathcal{M}$ for all β. Taking

$$\mathcal{M}^0 = \mathcal{M}^0([W_{\tau_P}], K_P(m)) = \Gamma({}_{K_P(m)}\mathbb{S}(G_P), [W_{\tau_P}])$$

for appropriate m, $F.J.^{P,0}$ can be regarded as a map

$$F.J.^{P,0} : \Gamma({}_{K(U,m)}Sh(2V), [W_\tau]) \to \mathcal{M}^0([W_{\tau_P}], K_P(m))[[q^{\Lambda^* \cap \mathfrak{c}^*}]]. \tag{1.5.4}$$

Letting K^p run over a fundamental set of open subgroups of $G(\mathbf{A}_f^p)$ corresponds to letting Λ^* grow to a $\mathbb{Z}_{(p)}$-lattice in $U_P(\mathbb{Q})$, or equivalently to adding nth roots of the generators q^{β_i} of $R[[q^{\Lambda^* \cap \mathfrak{c}^*}]]$ for all n prime to p.

(1.5.5) *One-dimensional τ's.*

In the present article we will mainly consider W_τ of dimension one. More precisely, $[W_{\tau_P}]$ is the automorphic vector bundle associated to an algebraic character, say τ_P, of the torus G_P. Fix a base point $x \in {}_{K_P(m)}\mathbb{S}(G_P)(\mathbb{C})$; for instance, we can take x to be the image of the element $1 \in GU(2V)(\mathbf{A})$ under the isomorphism $G_P(\mathbb{Q})\backslash G_P(\mathbf{A})/K_P(m) \xrightarrow{\sim} {}_{K_P(m)}\mathbb{S}(G_P)(\mathbb{C})$. Let W_{τ_P} be the stalk at x of $[W_{\tau_P}]$. Then $H^0(\mathbb{S}(G_P), [W_{\tau_P}])$ can be canonically identified with the space $\mathcal{M}(W_{\tau_P}(\mathbb{C}), K_P(m))$ of $W_{\tau_P}(\mathbb{C})$-valued automorphic forms on G_P of infinity type τ_P^{-1}; i.e., the space of functions

$$c : G_P(\mathbb{Q})\backslash G_P(\mathbf{A})/K_P(m) \to W_{\tau_P}(\mathbb{C})$$

such that $c(g_\infty g) = \tau_P(g_\infty)^{-1} c(g)$ for all $g \in G_P(\mathbf{A})$ and all $g_\infty \in G_P(\mathbb{R})$. Choosing a basis of $W_{\tau_P}(\mathbb{C})$ identifies $\mathcal{M}(W_{\tau_P}(\mathbb{C}), K_P(m))$ with the space

$$\begin{aligned} X_{\tau_P}(G_P; K_P(m)) &= \\ &= \{c : G_P(\mathbb{Q})\backslash G_P(\mathbf{A})/K_P(m) \to \mathbb{C} \mid c(g_\infty g) = \tau_P(g_\infty)^{-1} c(g)\} \end{aligned} \tag{1.5.5.1}$$

spanned by $\mathbb{C}$-valued Hecke characters of the indicated infinity type. This in turn identifies the Fourier expansion of a holomorphic modular form with an element of $X_{\tau_P}(G_P; K_P(m))[[q^{\Lambda^* \cap \mathfrak{c}^*}]]$. In this notation we can regard $\mathbb{C}$ as a $\mathcal{O}_v$-algebra or, more prudently, regard both $\mathbb{C}$ and $\mathcal{O}_v$ as algebras over the ring of integers of some number field.

(1.5.6) *Comparison with the transcendental theory*

Let $\psi : \mathbf{A}/\mathbb{Q} \rightarrow \mathbb{C}^\times$ be a non-trivial additive character, with local component ψ_v at the place v of $\mathbb{Q}$, such that $\psi_\infty(x) = e^{2\pi i x}$. For any $\beta \in U^*(\mathbb{Q})$ we define the character

$$\psi_\beta : U(\mathbb{Q})\backslash U(\mathbf{A}) \rightarrow \mathbb{C}^\times \mid \psi_\beta(u) = \psi(\beta(u)), u \in U(\mathbf{A}). \tag{1.5.6.1}$$

A section $f \in \Gamma(Sh(2V), [W_\tau])$ can be identified with a $W_\tau(\mathbb{C})$-valued automorphic form on $GU(2V)(\mathbf{A})$, belonging to the space on the right-hand side of (1.2.6), which This automorphic form will again be denoted f. We assume we are given an isomorphism of $W_\tau(\mathbb{C})$ with $\mathbb{C}$, so that f is viewed as a complex-valued automorphic form. The Fourier coefficients of such an f are then defined, classically, as functions on $GU(2V, \mathbf{A})$ by

$$f_\beta(h) = \int_{U(\mathbb{Q})\backslash U(\mathbf{A})} f(uh)\psi_{-\beta}(u)du \tag{1.5.6.2}$$

For $h = (h_\infty, h_f) \in GU(2V, \mathbf{A})$, the holomorphy of f implies a factorization $f_\beta(h) = f_{\beta,\infty}(h_\infty)f_{\beta,f}(h_f)$ where $f_{\beta,\infty}$ depends only on τ and β. Explicitly, if we write $h_\infty = p_\infty k_\infty$ with $p_\infty \in P(\mathbb{R})$ and $k_\infty \in K_\infty$, we have

$$f_{\beta,\infty}(p_\infty k_\infty) = \tau(k_\infty)^{-1} e^{2\pi i \beta(Z(p_\infty))} \tag{1.5.6.3}$$

where $Z(p_\infty) = p_\infty(x) \in U(\mathbb{C})$, with x the fixed point of K_∞ in $X(2V)$ and $X(2V)$ is realized as the tube domain $U(\mathbb{C})$ over the self-adjoint cone C in $U(\mathbb{R})$ and the action of $P(\mathbb{R})$ on the tube domain is the standard one. For more details, see [H1, II].

We write $q^\beta(h_\infty) = f_{\beta,\infty}(h_\infty)$. The function f can be recovered from the Fourier coefficients by Fourier inversion, to which we add Koecher's principle:

$$f(h) = \sum_{\beta \in U^* \cap C} f_\beta(h) = \sum_{\beta \in U^* \cap C} q^\beta(h_\infty) f_{\beta,f}(h_f). \tag{1.5.6.4}$$

It follows that the finite parts $f_{\beta,f}$ of f_β, as β varies, suffice to determine the form f. Suppose f is invariant under the compact open subgroup $K \subset GU(2V)(\mathbf{A}_f)$. Now the derived subgroup $GU(2V)^{der}$ is simply-connected, hence strong approximation is valid, and it follows that the coefficients $f_{\beta,f}$ are uniquely determined by their values on any subset $C' \subset GU(2V)(\mathbf{A}_f)$ which maps surjectively onto the quotient $C(K)$ defined as in (1.2). Let $L_P \subset P$ be the standard Levi component, the centralizer of G_P. Then we can take $C' = L_P(\mathbf{A}_f^p)$. It follows that

(1.5.6.5) Transcendental q-expansion principle. *A form* $f \in \mathcal{A}_{hol,\tau}(GU(2V))$ *is determined by the values* $f_{\beta,f}(h_f)$ *for* $h_f \in L_P(\mathbf{A}_f^p)$.

To simplify the comparison of the algebraic and transcendental theories, we introduce the "Shimura variety" $Sh(L_P, X_P)$ attached to L_P:

$$Sh(L_P, X_P) = Sh(G_P, X_P) \times^{G_P(\mathbf{A}_f)} L_P(\mathbf{A}_f). \tag{1.5.6.6}$$

This can be interpreted as an inductive limit of profinite schemes over $E(G_P, X_P) = \mathbb{Q}$, with natural $L_P(\mathbf{A}_f)$-action. The normal integral model $\mathbb{S}(G_P)$ extends similarly to an $L_P(\mathbf{A}_f)$-equivariant normal integral model $\mathbb{S}_P$ of $Sh(L_P, X_P)$. The automorphic vector bundles $[W_{\tau_P}]$ on $Sh(G_P, X_P)$ extend trivially to $L_(\mathbf{A}_f)$-equivariant vector bundles on $Sh(L_P, X_P)$. As in (1.5.5), we can write

$$\mathcal{M} = \mathcal{M}([W_{\tau_P}], K_{L(P)}(m)) = \Gamma({}_{K_{L(P)}(m)}\mathbb{S}_P, [W_{\tau_P}])$$

for an appropriate compact open subgroup $K_{L(P)}(m) \subset L_P(\mathbf{A}_f)$, and identify the latter with

$$\begin{aligned}&(1.5.6.7)\quad X_{\tau_P}(L_P; K_{L_P}(m)) = \\ &= \{c : G_P(\mathbb{Q})\backslash G_P(\mathbb{R}) \cdot L_P(\mathbf{A}_f)/K_{L(P)}(m) \to \mathbb{C} \mid c(g_\infty h) = \tau_P(g_\infty)^{-1}c(h)\}\end{aligned}$$

where now $h \in L_P(\mathbf{A}_f)$ but $g_\infty \in G_P(\mathbb{R})$. Ignoring the level structure, the Fourier expansion (1.5.6.4), with h_f restricted to $L_P(\mathbf{A}_f^p)$, then corresponds to a map

$$F.J.^P : \Gamma(Sh(2V), [W_\tau]) \to \widehat{\bigoplus_{\beta \in U^*}} \Gamma(Sh(L_P, X_P), [W_{\tau_P}]) \tag{1.5.6.8}$$

defined over $\mathbb{Q}$. By (1.5.6.5), this map is injective.

(1.5.7) *Trivializations.*

A good choice of basis of W_{τ_P} is provided by the theory of degenerating abelian varieties of type ${}_{K(U,m)}\mathcal{A}_{2V}$ (1.3.1); cf. [K, p. 212 ff.], [H1, Lemma 6.6], and [Pink,12.20]. The automorphic vector bundle W_{τ_P} is some power, say the kth, of the relative canonical sheaf (bundle of top differentials) on the universal degenerating abelian scheme over the toroidal compactification. Its natural basis is then the product

$$(\bigwedge_{j=1}^{N} dq^{\beta_j}/q^{\beta_j})^{\otimes k} = (2\pi i)^{Nk}(\bigwedge_j dz_j)^k, \tag{1.5.7.1}$$

where the tube domain coordinate z_j on $X(2V)$ is defined by $q^{\beta_j} = e^{2\pi i z_j}$. This basis is defined over $\mathbb{Z}_{(p)}$ because the coordinates q^{β_j} are used to define the toroidal compactification over $\mathbb{Z}_{(p)}$ in [F]. Thus the trivialization (1.5.7.1) is compatible with the theory of p-adic modular forms, just as in [K], and allows us to identify

$$F.J.^P(f)_\beta(h) = q^\beta(h_\infty) f_{\beta,f}(h_f),\ h = (h_\infty, h_f) \in L_P(\mathbf{A}) \tag{1.5.7.2}$$

where the left-hand term is (1.5.6.8) and the right-hand expression is from (1.5.6.4).

(1.6) p-INTEGRAL MODELS AND p-INTEGRAL SECTIONS.

Let p be a rational prime, and assume hypothesis (1.1.2) is satisfied. Let L' be a finite extension of $\mathbb{Q}$ containing $E(V)$ and let $\mathcal{O}'$ be the ring of integers of L'. For simplicity we will assume that L' also contains E. Fix a sufficiently small compact open subgroup $K = K_p \times K^p \subset G(\mathbf{A}_f)$, as in §1.3. Then it is known (cf. [Ko]) that ${}_KSh(G,X)$ admits a smooth integral model ${}_K\mathbb{S} = {}_K\mathbb{S}(G,X)$ over the valuation ring $\mathcal{O}'_{(p)}$ that is a moduli space for abelian varieties with additional structure of PEL type (the moduli problem is that of (1.3.1) but with ι now an embedding $\mathcal{O}_{(p)} \rightarrow End_S(A) \otimes \mathbb{Z}_{(p)}$). Moreover, if L' also contains $E(W_\tau)$ for every τ (a finite set of τ suffices) then the automorphic vector bundles $[W_\tau]$ extend naturally to locally free sheaves over ${}_K\mathbb{S}$. In particular, the construction of the ρ_τ's from §1.4 can be carried out over ${}_K\mathbb{S}$; these then provide integral structures on the various $[W_\tau]$'s. Both ${}_K\mathbb{S}$ and the integral structures on the $[W_\tau]$'s are functorial with respect to change of the level subgroup K^p away from p. In particular, we occasionally drop the notation K in what follows.

By our hypotheses on p, and by an elementary approximation argument, the decomposition (1.4.1) can be taken integral over $\mathcal{O}_{(p)}$. We assume that K is so defined so that $K_p \cap GU^{\oplus_i}(V,-V)(\mathbb{Q}_p)$ is again a maximal compact. Then ${}_KSh^{\oplus_i}(V,-V)$ (where the subscript ${}_K$ has the obvious meaning) also has a model over $\mathcal{O}'_{(p)}$, which we denote ${}_K\mathbb{S}^{\oplus_i} = {}_K\mathbb{S}^{\oplus_i}(V,-V)$. The natural map ${}_KSh^{\oplus_i}(V,-V) \rightarrow {}_KSh(G,X)$ (which is just the inclusion of certain CM points) extend to a map ${}_K\mathbb{S}^{\oplus_i} \rightarrow {}_K\mathbb{S}$, which can be uses to detect p-integrality of sections of the $[W_\tau]$'s, as we now explain.

Let A_Σ be an abelian variety over $\overline{\mathbb{Q}}$, of dimension $2d$, with complex multiplication by $\mathcal{K}$ of type Σ, and assume $End(A_\Sigma) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = \mathcal{O}_{(p)}$. In other words, $\mathcal{O}_{(p)}$ acts on the object "$A_\Sigma \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$" defined by A_Σ in the category of abelian varieties up to prime-to-p isogeny. One knows A_Σ extends to an abelian scheme, also denoted A_Σ, over the valuation ring $\bar{\mathbb{Z}}_{(p)}$, also with action by $\mathcal{O}_{(p)}$ up to prime-to-p isogeny. There is a decomposition

$$H^1_{DR}(A_\Sigma/\bar{\mathbb{Z}}_{(p)}) \xrightarrow{\sim} \oplus_{\sigma \in \Sigma_{\mathcal{K}}} \Omega(\Sigma)_\sigma, \tag{1.6.1}$$

with each $\Omega(\Sigma)_\sigma$ a free $\bar{\mathbb{Z}}_{(p)}$-module of rank one. Choose $\bar{\mathbb{Z}}_{(p)}$-generators $\omega_\sigma, \sigma \in \Sigma_{\mathcal{K}}$ of $\Omega(\Sigma)_\sigma$. On the other hand, the topological (Betti) homology

$H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)})$ is a free rank one $\mathcal{O} \otimes_{\mathbb{Z}} \bar{\mathbb{Z}}_{(p)}$-module, hence admits a decomposition

$$H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)}) \xrightarrow{\sim} \oplus_{\sigma \in \Sigma_{\mathcal{K}}} (\bar{\mathbb{Z}}_{(p)})_\sigma \tag{1.6.2}$$

where $(\bar{\mathbb{Z}}_{(p)})_\sigma$ is the submodule of $H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)})$, isomorphic to $\bar{\mathbb{Z}}_{(p)}$, on which $\mathcal{O}$ acts via σ. Choose $\bar{\mathbb{Z}}_{(p)}$-generators $\gamma_{\sigma'} \in (\bar{\mathbb{Z}}_{(p)})_{\sigma'}$, for $\sigma' \in \Sigma_{\mathcal{K}}$. The natural pairing (integration)

$$Int : H^1_{DR}(A_\Sigma/\bar{\mathbb{Z}}_{(p)}) \otimes H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)}) \to \mathbb{C}$$

defines invariants

$$p_{\mathcal{K}}(\sigma, \Sigma) = Int(\omega_\sigma, \gamma), \ \sigma \in \Sigma_{\mathcal{K}}, \gamma \in H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)}) \tag{1.6.3}$$

where γ is taken to be a free $\mathcal{O} \otimes_{\mathbb{Z}} \bar{\mathbb{Z}}_{(p)}$ generator of $H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)})$. It is easy to see that $Int(\omega_\sigma, \gamma)$ depends only on the projection of γ on $(\bar{\mathbb{Z}}_{(p)})_{c\sigma}$, hence that the complex number $p_{\mathcal{K}}(\sigma, \Sigma)$ is well defined up to multiplication by units in $(\bar{\mathbb{Z}}_{(p)})^\times$. Indeed, both $H_1(A_\Sigma(\mathbb{C}), \bar{\mathbb{Z}}_{(p)})$ and $H^1_{DR}(A_\Sigma/\bar{\mathbb{Z}}_{(p)})$ are invariants of the prime-to-p isogeny class of A_Σ, so the invariants $p_{\mathcal{K}}(\sigma, \Sigma)$ are independent of the choice of base point in the prime-to-p isogeny class of A_Σ, up to $(\bar{\mathbb{Z}}_{(p)})^\times$-multiples. It is well-known that any two choices of A_Σ can be related by a prime-to-p isogeny (concretely, any idèle class of $\mathcal{K}$ mod $\mathcal{K}_\infty^\times$ can be represented by an idèle trivial at p). Thus the $p_{\mathcal{K}}(\sigma, \Sigma)$ can be considered well-defined invariants of Σ, once a base point in the isogeny class is chosen. Now the elements of $\Sigma_{\mathcal{K}}$ generate the character group of the torus $R_{\mathcal{K}/\mathbb{Q}}\mathbb{G}_m$, hence their restrictions to the subtorus $GU(V_i)$, for any V_i as above, generate the character group of the latter. We only consider characters of $R_{\mathcal{K}/\mathbb{Q}}\mathbb{G}_m$ trivial on the Zariski closure of a sufficiently small congruence subgroup of the units in $\mathcal{K}$. These are characters of the Serre group, and can be identified with the formal linear combinations $\sum_{\sigma \in \Sigma_{\mathcal{K}}} n_\sigma \sigma$ with $n_\sigma \in \mathbb{Z}$ such that $n_\sigma + n_{\sigma c}$ is independent of σ. For such characters we define

$$p_{\mathcal{K}}(\sum_\sigma n_\sigma \sigma, \Sigma, V_i) = \prod_\sigma p_{\mathcal{K}}(\sigma e(i,\sigma), \Sigma)^{n_\sigma} \tag{1.6.4}$$

where $e(i,\sigma) = 1$ if $i \leq a_\sigma$ and $e(i,\sigma) = c$ otherwise. More generally, if κ is a character of $\prod_i GU(V_i) \times \prod_i GU(-V_i)$, written as an n-tuple of pairs of formal linear combinations

$$(\sum_{\sigma \in \Sigma_{\mathcal{K}}} n_{i,\sigma}\sigma, \sum_{\sigma \in \Sigma_{\mathcal{K}}} n^-_{i,\sigma}\sigma)$$

we define

$$p_{\mathcal{K}}(\kappa, \Sigma, 2V) = \prod_i p_{\mathcal{K}}(\sum_\sigma n_{i,\sigma}\sigma, \Sigma, V_i) \cdot \prod_i p_{\mathcal{K}}(\sum_\sigma n^-_{i,\sigma}\sigma, \Sigma, -V_i). \tag{1.6.5}$$

Here $p_{\mathcal{K}}(\sum_\sigma n_{i,\sigma}\sigma, \Sigma, -V_i)$ is defined as in (1.6.4) but with a_σ replaced by $n-a_\sigma$ The subgroup $T = GU^{\oplus_i}(V,-V)_\infty \subset \prod_i GU(V_i) \times \prod_i GU(-V_i)$ is a maximal torus in K_∞ (maximal compact mod center in $G = GU(2V)$). The formalism of CM periods implies that the product on the right in (1.6.5) depends only on the restriction of the algebraic character κ to the subgroup T. Indeed, if the restriction of κ to $\prod_i U(V_i) \times \prod_i U(-V_i)$ is trivial, then in particular $n_{i,\sigma} = n_{i,\sigma c}$ for all i and all σ. Since $n_{i,\sigma} + n_{i,\sigma c}$ is independent of σ for each i, it follows that $n_i = n_{i,\sigma}$ is independent of σ for each i, and one can define n_i^- likewise. One then has

$$p_{\mathcal{K}}(\sum_\sigma n_\sigma\sigma, \Sigma, V_i) = p_{\mathcal{K}}(\sum_\sigma \sigma, \Sigma, V_i)^{n_i} = p_{\mathcal{K}}(||\bullet||, 1)^{n_i} = (2\pi i)^{-dn_i}$$

as in [H2,Lemma 1.8.3]. If moreover $\kappa|_T \equiv 1$, then $\sum_i n_i + n_i^- = 0$, and so the product of powers of $2\pi i$ is in fact algebraic. Hence the statement of the following Proposition makes sense:

(1.6.6) Proposition. *Let $G = GU(2V)$. Let κ be a character of the torus T that extends to a one-dimensional representation of K_∞. Let $[W_\tau]$ be the corresponding automorphic line bundle over ${}_K\mathbb{S}$. Let $D \subset Sh^{\oplus_i}(V,-V)(\overline{\mathbb{Q}})$ be a set of points with the following property: the $G(\mathbf{A}_f^p)$ orbit of the image of D under specialization is Zariski dense in the special fiber of ${}_K\mathbb{S}$. Then $f \in H^0({}_K\mathbb{S}, [W_\tau]) \otimes_{L'} \mathbb{C}$ belongs to $H^0({}_K\mathbb{S}, [W_\tau]) \otimes_{O'} \bar{\mathbb{Z}}_{(p)}$ if and only if, for all $g \in G(\mathbf{A}_f^p)$, the weight κ component $f^g[\kappa]$ of the restriction of the g translate f^g of f to D satisfies*

$$p_{\mathcal{K}}(\kappa, \Sigma, 2V)^{-1} f^g[\kappa](x) \in \bar{\mathbb{Z}}_{(p)} \tag{1.6.7}$$

for all $x \in D$. Here the section $f^g \in H^0({}_K\mathbb{S}, [W_\tau]) \otimes_{L'} \mathbb{C}$ is identified with a classical automorphic form on $X(2V) \times G(\mathbf{A}_f)$ via (1.2.6). *The same holds with $\mathbb{C}$ replaced by $\mathbb{C}_p$ and $\bar{\mathbb{Z}}_{(p)}$ replaced by $\mathcal{O}_{\mathbb{C}_p}$.*

Remark. There is an analogous proposition for $[W_\tau]$ of arbitrary dimension, but we will not be needing it in the present paper.

Proof. Write $H = H^0({}_K\mathbb{S}, [W_\tau])$, $\bar{H} = H \otimes_{\mathcal{O}'_{(p)}} \overline{\mathbb{Q}}$. Our hypothesis on D implies that $D \cdot G(\mathbf{A}_f^p)$ is Zariski dense in the generic fiber ${}_K Sh(G,X)$. Then (1.6.7), with $\bar{\mathbb{Z}}_{(p)}$ replaced by $\overline{\mathbb{Q}}$, is a version of Shimura's criterion for f to belong to $\bar{H}$ (cf. ([H1,§5.3], cf. [H3, III, Lemma 3.10.2] for an explicit statement when $\mathcal{K}$ is imaginary quadratic). Then there is a number field L, containing L, such that $f \in H \otimes_{L'} L$. Let $H_p = H \otimes_{\mathcal{O}'_{(p)}} \mathcal{O}_{L,(p)}$. Thus H_p is a free $\mathcal{O}_{L,(p)}$-module of finite rank, and $\bar{H} = H_p \otimes_{\mathcal{O}_{L,(p)}} \overline{\mathbb{Q}}$.
Let $\mathfrak{p}$ be a prime of $\mathcal{O}_{L,(p)}$, necessarily dividing p, and let ϖ be a uniformizer of $\mathfrak{p}$. Thus for some positive integer m we have $\varpi^m f \in H_p$. Write $F = \varpi^m f$. Condition (1.6.7) asserts that

$$p_{\mathcal{K}}(\kappa, \Sigma, 2V)^{-1} F^g[\kappa](x) \equiv 0 \pmod{\mathfrak{p}^m}, \forall x \in D \tag{1.6.8}$$

The proposition then comes down to showing that any F satisfying (1.6.8) belongs to $\mathfrak{p}^m H_p$.
Since belonging to $\mathfrak{p}^m H_p$ is a local condition on ${}_K\mathbb{S} \times \mathcal{O}_{L,p}$, we can replace the latter by an affine open subset $U = Spec(A)$ flat over $\mathcal{O}_{L,p}$, and H_p by a free A-module M_p; F is an element of M_p. By induction we reduce to the case $m = 1$. Let $\bar{U} = Spec(A/pA)$ denote the special fiber of U; for a geometric point y of $\bar{U}$ let $I_y \subset A$ denote the maximal ideal at y. Condition (1.6.8) is the condition that $F \in I_y \cdot M_p$ for y in a Zariski dense subset $\bar{D}$ of $\bar{U}$; this is essentially the obvious p-integal version of the results of [H3, (3.10)]. By definition, the intersection $\bigcap_{\bar{D}} I_y = \mathfrak{p} \cdot A$. Since M_p is free of finite rank over the noetherian ring A, the proposition is clear.
A simple continuity argument now provides the proof in the case where $\bar{\mathbb{Z}}_{(p)}$ is replaced by $\mathcal{O}_{\mathbb{C}_p}$.

2. p-adic automorphic forms on unitary groups

(2.1) The Igusa tower, I: Definitions.

Notation is as in §1. Recall the $\mathbb{Q}_p$-rational $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$-submodule $F^0V_p \subset V_p$, defined in (1.1.6), and the $\mathcal{K} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$-submodule subspace $F^0V \subset V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ introduced at the beginning of (1.3). The flag variety $\hat{X}$ of $\mathcal{K}$-linear subspaces of V satisfying (1.3.0) has a natural $E(V)$-rational structure. Hypothesis (1.1.6) is equivalent to the condition that the completion $E(V)_{w_0}$ of $E(V)$ at the place w_0 of $E(V)$ corresponding to $incl_p$ is isomorphic to $\mathbb{Q}_p$, and the $\mathcal{K}$-linear subspace $F^0V_p \subset V_p$ is indeed a $\mathbb{Q}_p = E(V)_{w_0}$-rational point of $\hat{X}$.
The skew-hermitian pairing $tr_{\mathcal{K}/\mathbb{Q}} < \bullet, \bullet >_{V,\daleth}$ on $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ defines a perfect duality

$$V_{p,\Sigma_p} \otimes V_{p,c\Sigma_p} \to \mathbb{Q}_p. \tag{2.1.1}$$

This duality identifies

$$V_w/F^0V_w \xrightarrow{\sim} Hom(F^0V_{c\cdot w}, \mathbb{Q}_p)$$

for any w dividing p. In this way

$$\prod_{w|p} GL(F^0V_w) \xrightarrow{\sim} \prod_{w,\Sigma_w \subset \Sigma_p} GL(F^0V_w) \times GL(V_w/F^0V_w), \tag{2.1.2}$$

is naturally isomorphic to the Levi quotient L^0 of the parabolic

$$P^0 = \prod_{w,\Sigma_w \subset \Sigma_p} Stab(F^0V_w).$$

Here P^0 is a viewed as a parabolic subgroup of the unitary group G_0 rather than the unitary similitude group G. Bear in mind that the action of L^0 on V_w/F^0V_w is dual to that on $F^0V_{c\cdot w}$.

We return to the situation of (1.3.1), and let $K = K^p \times K_p$ where $K_p = G_0(\mathbb{Z}_p) \times GL(1,\mathbb{Z}_p)$ is the hyperspecial maximal compact subgroup of (1.3.4), viewed as the group of $\mathbb{Z}_p$-points of a smooth reductive group scheme $\mathbb{K}$ over $\mathbb{Z}_p$ with generic fiber $G \times_{\mathbb{Q}} \mathbb{Q}_p$. We assume the subspace F^0V_p and K_p are chosen compatibly, in the sense that P^0 is the $\mathbb{Q}_p$-points of a parabolic subgroup $\mathbb{P}^0 \subset \mathbb{K}$ (parabolic in the subgroup of $\mathbb{K}$ corresponding to $G_0(\mathbb{Z}_p)$), and we can define $\mathbb{L}^0$ to be the Levi quotient of $\mathbb{P}^0$ so that $L^{)} = (L)^0(\mathbb{Q}_p)$. Equivalently, V_p and F^0V_p contain compatible $\mathcal{O}_p$-stable lattices M and M^0, respectively, with K_p the stabilizer of M, and the decomposition $F^0V_p = \oplus_{w|p}F^0V_w$ of (1.1.6) is obtained by extension of scalars from a decomposition $M^0 = \oplus_{w|p}M^0_w$; $\mathbb{P}^0$ is then the stabilizer in $\mathbb{K}$ of M^0. Where necessary, we write $M = M(V)$, $M^0 = M(V)^0$, etc., to emphasize the relation with the hermitian space V defining the moduli problem.

We write

$$M^0_{\Sigma_p} = \oplus_{w,\Sigma_w\subset\Sigma_p}M^0_w,\ M^{-1}_{\Sigma_p} = \oplus_{w,\Sigma_w\subset\Sigma_p}M_w/M^0_w \tag{2.1.3}$$

As in the preceding paragraph, the skew-hermitian form $tr_{\mathcal{O}/\mathbb{Z}} < \bullet, \bullet >_{V,\beth}$ can be normalized to define a natural skew-hermitian perfect duality.

$$M^0 \otimes M/M^0 \to \mathbb{Z}_p. \tag{2.1.4}$$

There is also a natural isomorphism

$$M^0 \xrightarrow{\sim} M^0_{\Sigma_p} \oplus Hom^c(M^{-1}_{\Sigma_p}, \mathbb{Z}_p), \tag{2.1.5}$$

where

$$Hom^c(M^{-1}_{\Sigma_p}, \mathbb{Z}_p) = \mathcal{O}_p \otimes_{\mathcal{O}_p,c} Hom(M^{-1}_{\Sigma_p}, \mathbb{Z}_p)$$

i.e. the natural action of $\mathcal{O}_p$ on $Hom(M^{-1}_{\Sigma_p}, \mathbb{Z}_p)$ is composed with complex conjugation.

Let ${}_{K^p}\mathcal{A}^p = {}_{K^p}\mathcal{A}^p_{V,\beth}$ be the functor

$$S \mapsto \{(A, \lambda, \iota, \alpha^p)\}$$

where A is now an abelian scheme over S up to *prime-to* p-isogeny, λ is a polarization of degree prime to p, $\iota : \mathcal{O}_{(p)} \to End_S(A) \otimes \mathbb{Z}_{(p)}$ is an embedding of $\mathbb{Z}_{(p)}$-algebras, and $\alpha^p : V(\mathbf{A}^p_f) \xrightarrow{\sim} V^{f,p}(A)$ is a prime-to-p $\mathcal{O}_{(p)}$-linear level structure modulo K^p. The forgetful map ${}_K\mathcal{A} \to {}_{K^p}\mathcal{A}^p$ is obviously an isomorphism. The functor ${}_{K^p}\mathcal{A}^p$ is representable over the integer ring $\mathcal{O}_{w_0}$ of $E(V)_{w_0}$ by a scheme we will denote ${}_K\mathbb{S}$, as in (1.4).

(2.1.6) *Igusa Schemes*

The following constructions are compatible with change of the level subgroup K^p, and with passage to the limit over all K^p. Hence we drop the subscript ${}_{K^p}$ for the time being. We view $\mathcal{A}^p$ as a functor on the category of schemes over $\mathcal{O}_{w_0}$. Points of $\mathcal{A}^p(S)$ will be denoted $\underline{A}$. Define three families of functors above $\mathcal{A}^p$, indexed by non-negative integers m:

$$(2.1.6.1) \qquad Ig_{1,m}(S) = \{(\underline{A}, j^{et})\}, \quad j^{et} : A[p^m] \twoheadrightarrow (M/M^0) \otimes \mathbb{Z}/p^m\mathbb{Z}.$$

$$(2.1.6.2) \quad Ig_{2,m}(S) = \{(\underline{A}, j^o)\},\ \underline{A} = (A, \lambda, \iota, \alpha^p), \quad j^o : M^0 \otimes \mu_{p^m} \hookrightarrow A[p^m].$$

$$(2.1.6.3) \quad Ig_{3,m}(S) = \{(\underline{A}, j^0, j^{(-1)})\},$$
$$j^0 : M^0_{\Sigma_p} \otimes \mu_{p^m} \hookrightarrow A[p^m]_{\Sigma_p},\ j^{(-1)} : A[p^m]_{\Sigma_p} \twoheadrightarrow M^{-1}_{\Sigma_p} \otimes \mathbb{Z}/p^m\mathbb{Z}.$$

In each case $\underline{A}$ designates a quadruple $(A, \lambda, \iota, \alpha^p) \in \mathcal{A}^p(S)$. The maps j^0, j^{et}, j^0, and $j^{(-1)}$ are all assumed $\mathcal{O}/p^m\mathcal{O}$-linear.

(2.1.6.4) Lemma. *The functors $Ig_{i,m}$, $i = 1, 2, 3$, are all relatively representable over $\mathcal{A}^p$, and are canonically isomorphic for all m. These isomorphisms are compatible with the natural forgetful projection maps $Ig_{i,m+1} \to Ig_{i,m}$ for all i; moreover, these projection maps are étale for all m.*

Proof. Since the polarization λ is assumed of degree prime to p, we can use it to identify $\hat{A}[p^m] \xrightarrow{\sim} A[p^m]$. The isomorphism $Ig_{1,m} \xrightarrow{\sim} Ig_{2,m}$ is then obtained by combining the duality (2.1.4) with Cartier duality $A[p^m] \times \hat{A}[p^m] \to \mu_{p^m}$. The isomorphism between $Ig_{2,m}$ and $Ig_{3,m}$ is obtained in a similar way from (2.1.5). Compatibility of these isomorphisms with the forgetful projection maps is obvious. Finally, the projection $Ig_{1,m+1} \to Ig_{1,m}$ is obviously étale, since it corresponds to lifting a trivialization of the étale quotient of $A[p^m]$ to one of the étale quotient of $A[p^{m+1}]$.

Since the isomorphisms in (2.1.6) are canonical, we write Ig_m for $Ig_{i,m}$, $i = 1, 2, 3$, or $Ig(V)_m$ when we need to emphasize V. For any $m > 0$, the natural forgetful map $Ig_m \to \mathbb{S}$ obviously factors through the inclusion of the ordinary locus $\mathbb{S}^{ord} \subset \mathbb{S}$. The limit $Ig_\infty = \varprojlim_m Ig_m$ is an étale Galois covering of $\mathbb{S}^{ord}$ with covering group

$$\mathbb{L}^0(\mathbb{Z}_p) = Aut(M^0) \xrightarrow{\sim} Aut(M^0_{\Sigma_p}) \times Aut(M^{-1}_{\Sigma_p}).$$

Let $\mathbb{F}$ denote the algebraic closure of the residue field of $\mathcal{O}_{w_0}$, and let $\bar{S} = {}_K\mathbb{S} \times_{\mathcal{O}_{w_0}} \mathbb{F}$ denote the geometric special fiber of the moduli scheme ${}_K\mathbb{S}$. Let $\bar{S}^{ord} = \mathbb{S}^{ord} \times_{Spec(\mathcal{O}_{w_0})} \bar{S} \subset \bar{S}$ denote the ordinary locus of the special fiber. The following theorem is a special case of a result of Wedhorn [We]:

(2.1.7) THEOREM. *The ordinary locus $\bar{S}^{ord}$ contains an open dense subscheme of every irreducible component of $\bar{S}$.*

(2.1.8) *Modular interpretation of the Igusa tower in the limit*

In the limit as m tends to infinity we can reformulate the definition of the Igusa tower in terms of abelian varieties up to isogeny. We prefer to use the models $Ig_{3,m}$. Let $T(\mathbb{G}_m) = \varprojlim_m \mu_{p^m}$ denote the Tate module of the multiplicative group, viewed as a profinite flat group scheme over $Spec(\mathbb{Z}_p)$. For any vector space W over $\mathbb{Q}_p$ we let $W(1) = W \otimes_{\mathbb{Z}_p} T(\mathbb{G}_m)$. Consider the functor on schemes over $\mathcal{O}_{w_0}$:
(2.1.8.1)

$$Ig'_{3,\infty}(S) = \{(\underline{A}, j^0, j^{-1})\},$$
$$j^0 : F^0V_{\Sigma_p}(1) \hookrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} A[p^\infty]_{\Sigma_p},\ j^{-1} : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} A[p^\infty]_{\Sigma_p} \twoheadrightarrow V/F^0V_{\Sigma_p}.$$

Here $\underline{A} = (A, \lambda, \iota, \alpha^p)$ as above, but now A is an abelian variety up to isogeny, and $A[p^\infty]$ is a p-divisible group up to isogeny, or rather quasi-isogeny (cf. [RZ], 2.8). For fixed m we define $Ig'_{3,m}$ by the same functor as $Ig'_{3,\infty}$ but with j^0 and j^{-1} defined only modulo the principal congruence subgroups modulo p^m of $GL(M^0_{\Sigma_p})$ and $GL(M^{-1}_{\Sigma_p})$, respectively. The usual argument shows that

(2.1.8.2) LEMMA. *There are canonical isomorphisms $Ig'_{3,m} \xrightarrow{\sim} Ig_{3,m}$ for all m, compatible with the forgetful maps from level p^{m+1} to level p^m for all m. In particular, the natural action of $\mathbb{L}^0(\mathbb{Z}_p)$ on Ig_∞ extends canonically to an action of $L^0(\mathbb{Q}_p)$.*

The final assertion is completely analogous to the existence of an action of $G(\mathbf{A}^p_f)$ in the inverse limit over K^p.

(2.1.9) *Irreducibility of the Igusa tower*

We reintroduce the prime-to-p level subgroups K^p, and the level subgroup $K = K^p \times K_p$. The fiber over $\mathbb{Q}_p$ of the ordinary locus ${}_K\mathbb{S}^{ord}$ coincides with ${}_K\mathbb{S} \times_{\mathbb{Z}_p} \mathbb{Q}_p = {}_KSh(V)_{\mathbb{Q}_p}$; here, as above, we identify $\mathbb{Q}_p = E(V)_{w_0}$. The generic fibers ${}_{K^p}Ig_{m,\mathbb{Q}_p}$ can be identified with Shimura varieties attached to appropriate level subgroups, as follows. Let $U \subset \mathbb{P}^0$ denote the unipotent radical. For any non-negative integer m, let $K(U,m)_p \subset K_p$ denote the inverse image of $U(\mathbb{Z}_p/p^mZp) \times GL(1,\mathbb{Z}_p)$ under the natural map $K_p \to \mathbb{K}(\mathbb{Z}_p/p^mZp)$. Let $K(U,m) = K(U,m)_p \times K^p$. The variety ${}_{K(U,m)}Sh$, as m tends to infinity, parametrizes quadruples $(A, \lambda, \iota, \alpha)$ where $\alpha = (\alpha_{p,m}, \alpha^p)$ with α^p as above and

$$\alpha^0_{p,m} : M/p^mM \xrightarrow{\sim} A[p^m] \pmod{K(U,m)}$$

is an $\mathcal{O}/p^m\mathcal{O}$-linear injection that identifies the given skew-symmetric pairing on M/p^mM with the Weil pairing on $A[p^m]$. This comes down to an inclusion of $(M/p^mM)^{K(U,m)} = M^0/p^mM^0$ in $A[p^m]_{\Sigma_p}$ and a Cartier dual surjection of $A[p^m]_{\Sigma_p}$ onto M^{-1}/p^mM^{-1}. It follows that there are natural isomorphisms

$$(2.1.9.1) \qquad {}_{K^p}Ig_{m,\mathbb{Q}_p} \xrightarrow{\sim} {}_{K(U,m)}Sh$$

compatible with the forgetful maps from level $m+1$ to level m.
Over $\mathbb{C}$, the connected components of ${}_{K(U,m)}Sh(G,X)$ are in bijection with the class group $C(m) = C(K(U,m))$, as at the end of (1.2). Consider the normalization $\widehat{{}_K\mathbb{S}}$ of ${}_K\mathbb{S}$ in ${}_{K(U,m)}Sh(G,X)$. This is an $\mathcal{O}_v$-model of ${}_{K(U,m)}Sh(G,X)$, though not a very good one. However the non-singular locus $(\widehat{\bar{S}}^o$ is étale over ${}_K\bar{S}^{ord}$, and ${}_{K^p}Ig_m$ is naturally isomorphic to an open subscheme of $(\widehat{\bar{S}})^o$. In particular, there is a map $c_m :_{K^p} Ig_m \to C(m)$, which can be given a modular interpretation as in (1.2). A special case of Corollary 8.17 of [Hi04], (cf. also [Hi05, §10]) is that

(2.1.10) Theorem. ([Hida]) *The fibers of c_m are geometrically irreducible for all m.*

This is proved in [loc. cit.] under a hypothesis labeled (ord), which is equivalent to our hypothesis (1.1.2). Lemma 8.10 of [loc. cit.] makes this explicit, but only for imaginary quadratic $\mathcal{K}$.

(2.1.11) *Inclusion of Igusa towers for $Sh(V,-V)$ in $Sh(2V)$*

Applying the previous discussion to the hermitian space $2V$, we identify $Ig(2V)_m = Ig(2V)_{2,m}$ with the moduli space of quintuples

$$\{\underline{B} = (B,\mu,\iota_2,\beta^p), j^o_{2V} : M(2V)^0 \otimes \mu_{p^m} \hookrightarrow B[p^m]).$$

Now $M(2V)^0$ is a lattice in the $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$-submodule $F^0(2V)_p$ of $(2V)_p$, which we can choose arbitrarily as long as we respect Hypothesis (1.1.6). For example, we can choose

$$(2.1.11.1) \qquad F^0(2V)_p = F^0V_p \oplus F^0(-V)_p$$

where $F^0(-V)_p \subset (-V)_p$ is any $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$-submodule satisfying (1.1.6), which for $-V$ amounts to the condition that $\dim F^0(-V)_w = n - a_\sigma = a_{c\sigma}$ for any $\sigma \in \Sigma_w$. As $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$-module $-V$ is isomorphic to V, and it is particularly convenient to choose $F^0(-V)_p \subset (-V)_p = V_p$ to be a subspace mapping isomorphically to V_p/F^0V_p under the projection, or equivalently such that (2.1.1) restricts to a duality between $F^0(-V)_w$ and F^0V_{cw} for any w dividing p.
We define $Ig(V,-V)_m \subset Ig(V)_m \times Ig(-V)_m$ as $Sh(V,-V)$ in (1.3) as the subvariety with compatible polarizations. Then, ignoring prime-to p level structures, the reduction modulo p of the natural morphism $Sh(V,-V) \subset Sh(2V)$ defines a family of morphisms $Ig(V,-V)_m \to Ig(2V)_m$ whose image, in the version $Ig_{2,m}$, is the moduli space of quintuples as above where

$$(B,\mu,\iota_2,\beta) \xrightarrow{\sim} (A \times A^-, \lambda \times \lambda^-, \iota \times \iota^-, \alpha \times \alpha^-)$$

as in §1.4 and where

$$(2.1.11.2)\quad j^o_{2V} = j^o_V \times j^o_{-V} : M(V)^0 \otimes \mu_{p^m} \times M(-V)^0 \otimes \mu_{p^m} \hookrightarrow A[p^m] \times A^-[p^m].$$

We make this more explicit. Fix w dividing p, let $(a,b) = (a_w, b_w)$, and choose bases $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$ for V_w and $(-V)_w$, respectively, with $e_1, \ldots e_a$ a basis for F^0V_w, $f_1, \ldots f_b$ a basis for $F^0(-V_w)$. We regard the natural identification of V_w with $(-V)_w$ as an isomorphism between the two halves of $2V$, in such a way that e_i is taken to f_{b+i} for $1 \leq i \leq a$ and e_{a+j} is taken to f_j for $1 \leq j \leq b$. The $2n \times 2n$-matrix $\gamma_1 = \gamma_{1;a,b}$:

$$(2.1.11.3)\qquad \gamma_1 = \gamma_{1;a,b} = \begin{pmatrix} I_a & 0 & 0 & 0 \\ 0 & 0 & 0 & I_b \\ 0 & 0 & I_a & 0 \\ 0 & I_b & 0 & 0 \end{pmatrix},$$

in the basis $(e_1, \ldots, e_n, f_1, \ldots f_n)$ of $2V_w$, takes the subspace $V_w \subset 2V_w$ to the subspace $F^0(2V)_w$ defined by (2.1.11.1).

(2.2) The Igusa tower, II: p-adic modular forms.

We now recall Hida's generalization of the Deligne-Katz construction of p-adic modular forms, for the Shimura varieties $Sh(G,X)$. In the present article we will only need p-adic modular forms in order to define a good notion of p-integrality for certain holomorphic Eisenstein series ramified at p, but later we will use them to construct p-adic L-functions and establish their boundedness . So for the moment we let $(G,X) = (GU(V), X(V))$ or $(GU(V,-V), X(V,-V))$. We work with a smooth, projective, toroidal compactification ${}_K\mathbb{S}^{\sim}$ of ${}_K\mathbb{S}$. The construction of such compactifications in this setting is due to Fujiwara. The choice of ${}_K\mathbb{S}^{\sim}$ is not canonical. However, the universal abelian scheme ${}_K\mathbb{A}$ over ${}_K\mathbb{S}$ extends to a semi-abelian scheme over ${}_K\mathbb{S}^{\sim}$. Hence ω, and therefore each ρ_τ, also extends.

Let v be the prime of $\mathcal{K}$ determined by $incl_p$. We begin by choosing a lifting of ${}_K\bar{S}^{ord}$ to an $\mathcal{O}_v$-flat open subscheme of ${}_K\mathbb{S}^{\sim}$. (This is possible since under (1.1.2) $E(V)_{w_0} = \mathbb{Q}_p$ so our schemes are all defined over $\mathcal{O}_v$.) More precisely, ${}_K\bar{S}^{ord}$ is defined by the non-vanishing of the Hasse invariant H, which can be regarded as a section of a certain automorphic line bundle $[\mathcal{L}]$ over $\bar{S}$. The line bundle $\mathcal{L}$ is known to be ample, hence for some power $\kappa >> 0$ the section H^κ lifts to a section $\tilde{H} \in \Gamma({}_K\mathbb{S}, [\mathcal{L}]^\kappa)$. We let ${}_K\mathbb{S}^{ord} \subset {}_K\mathbb{S}$ be the open subscheme defined by non-vanishing of $\tilde{H}$. This is slightly abusive, since it depends on the choice of lifting $\tilde{H}$, but different choices yield isomorphic theories. For all this, see [Hi05, p. 213 ff.] or [SU].

We let W be a finite flat $\mathcal{O}_v$ algebra, $W_r = W/p^rW$, and let $S_m = {}_K\mathbb{S}^{ord} \otimes_{\mathcal{O}_v} W_r$. The S_r form a sequence of flat W_r schemes, with given isomorphisms

$$S_{r+1} \otimes_{W_{r+1}} W_r \xrightarrow{\sim} S_r.$$

For $m \geq 1$, let $P_m = \mathbb{A}[p^m]^{et} = \mathbb{A}[p^m]/\mathbb{A}[p^m]^0$ over ${}_K\bar{S}^{ord}$, the quotient of the ${}_K\bar{S}^{ord}$ group scheme of p^m-division points of $\mathbb{A}$ by its maximal connected subgroup scheme. This is a free étale sheaf in $\mathcal{O}_v/p^m\mathcal{O}_v$-modules over ${}_K\bar{S}^{ord}$, hence lifts canonically, together with its $\mathcal{O}_v$-action, to an étale sheaf over S_r for all r. Following [Hi04], we define $\mathcal{T}_{r,m}$ to be the lifting to S_r of the corresponding principal $GL(n, \mathcal{O}/p^m\mathcal{O})$-bundle (resp.., $GL(n, \mathcal{O}/p^m\mathcal{O}) \times GL(n, \mathcal{O}/p^m\mathcal{O})$-bundle) $Ig_m(V) = Ig_{1,m}$ (resp., $Ig_m(V, -V)$), defined by (2.1.6.1) (resp., as in (2.1.11)); note that our indices are not the same as Hida's. Let

$$\mathcal{V}_{r,m} = \Gamma(\mathcal{T}_{r,m}, \mathcal{O}_{\mathcal{T}_{r,m}});\ \mathcal{V}_{r,\infty} = \varinjlim_{m} \mathcal{V}_{r,m};\ \mathcal{V}_{\infty,\infty} = \varprojlim_{r} \mathcal{V}_{r,\infty}$$

Note that these carry actions of $GL(n, \mathcal{O}_p)$ or of $GL(n, \mathcal{O}_p) \times GL(n, \mathcal{O})$, depending on whether $G = GU(V)$ or $GU(V, -V)$. Let U be the upper-triangular unipotent radical of $GL(n, \mathcal{O}_p)$ or $GL(n, \mathcal{O}_p) \times GL(n, \mathcal{O}_p)$, depending. We then define our space of p-adic modular forms to be

$$\mathcal{V} := \mathcal{V}_{\infty,\infty}^{U}.$$

We will adopt the convention of adding a superscript V or $V, -V$ when it is necessary to distinguish the groups in question. Hence, $\mathcal{V}_V$ is the ring of p-adic modular forms for $GU(V)$.

It is clear that the construction of the spaces of p-adic modular forms for $GU(V, -V)$ and $GU(2V)$ can be done compatibly, at least when the various prime-to-p level structures are compatible (i.e., there are morphisms ${}_KSh(V, -V) \rightarrow {}_{K'}Sh(2V)$). This gives rise to a restriction map

$$r_V : \mathcal{V}_{2V} \rightarrow \mathcal{V}_{(V,-V)}.$$

The primary goal of this section is to explain why this is a good definition and how it naturally contains all p-adic sections of $[W_\tau]$ for all τ, and, in the case $G = GU(2V)$, is contained in the power series ring $R[[q^{\Lambda^* \cap \mathfrak{c}^*}]]$ of (1.5.3) for an appropriate R. For $n > 1$, the sections of $[W_\tau]$ are vector-valued functions. To compare them for different τ, we follow Hida and trivialize the $[W_\tau]$, using the modular definition of $\mathcal{T}_{r,m}$, and then apply the theorem of the highest weight in integral form. The discussion below follows [Hi04,8.1], to which we refer for missing details.

Let $\omega_{r,m}$ denote the pullback of ω to $\mathcal{T}_{r,m}$. By Cartier duality, the universal surjection (2.1.6.1), with $S = \mathcal{T}_{1,m}$, is equivalent to an isomorphism of group schemes

$$\mathfrak{d}^{-1} \otimes (\mu_{p^m})^n \xrightarrow{\sim} \hat{\mathbb{A}}[p^m]^0. \tag{2.2.1}$$

Here $\mathfrak{d}^{-1}$ is the different of $\mathcal{K}$ over $\mathbb{Q}$, μ_{p^m} is the kernel of multiplication by p^m in the multiplicative group scheme, $\hat{\mathbb{A}}$ is the abelian scheme dual to $\mathbb{A}$, and the superscript ^{0} denotes the maximal connected subgroup scheme. Since (2.2.1) is Cartier dual to an isomorphism of étale group schemes induced by (2.1.6.1), it lifts canonically to $\mathcal{T}_{r,m}$. Since there are canonical isomorphisms

$$\omega_{r,m} \xrightarrow{\sim} Lie(\hat{\mathbb{A}}) \otimes W_r \xrightarrow{\sim} Lie(\hat{\mathbb{A}}[p^m]^0) \otimes W_r$$

we can identify

$$\omega_{r,m} \xrightarrow{\sim} \mathfrak{d}^{-1} \otimes Lie(\mu_{p^m})^n \otimes W_r \xrightarrow{\sim} \mathfrak{d}^{-1} \otimes \mathcal{O}^n_{\mathcal{T}_{r,m}}. \tag{2.2.2}$$

as $\mathcal{O}_p \otimes_{\mathbb{Z}_p} W_r$ modules.

Since $\mathcal{K}$ is unramified at p, $\mathfrak{d}^{-1}$ is prime to p, and (2.2.2) reduces to a family of $\mathcal{O}_p \otimes_{\mathbb{Z}_p} W_r$ isomorphisms

$$\omega_{r,m} \xrightarrow{\sim} \mathcal{O} \otimes_{\mathbb{Z}_p} \mathcal{O}^n_{\mathcal{T}_{r,m}}, \tag{2.2.3}$$

compatible as m and r vary. Note that in (2.2.1), (2.2.2), and (2.2.3) the n should be replaced by a $2n$ if $G = GU(V, -V)$.

Suppose that $G = GU(V)$. Now we apply the highest weight formalism as in [Hi05]. Let $G_1 = Res_{\mathcal{O}_p/\mathbb{Z}_p} GL(n)$, let B_1 be the upper-triangular Borel of G_1, U_1 its unipotent radical, and T_1 the torus of diagonal elements. Let $\mathcal{H} = G_1/U_1$. Then (2.2.3) yields a family of isomorphisms

$$G_{1/\mathcal{T}_{r,m}} \xrightarrow{\sim} GL_{\mathcal{O}}(\omega_{r,m}) \tag{2.2.4}$$

and

$$\mathcal{H}_{\mathcal{T}_{r,m}} \xrightarrow{\sim} Y_{r,m} \overset{def}{=} GL_{\mathcal{O}}(\omega_{r,m})/U_{can} \tag{2.2.5}$$

where U_{can} is the $\mathcal{T}_{r,m}$-unipotent group scheme corresponding to U_1 under (2.2.4). The isomorphisms (2.2.5) are compatible with the natural $G_1 \times T_1$ actions on the two sides (G_1 acting on the left and T_1 on the right) and patch together as r and m vary. Not that for any character κ of T_1, taking κ-equivariant sections (indicated by $[\kappa]$) of $\mathcal{O}_{Y_{r,m}}$ makes sense.

Continuing as in [Hi05, §7], and writing $Y = Y_{r,m}$, $p_Y : Y \to T_{r,m}$ the natural map, note that $p_{Y,*}(\mathcal{O}_Y[\kappa])$ inherits an action of $G_1(\mathbb{Z}_p)$, covering the trivial action on $T_{r,m}$, because p_Y is a fibration in $G_1(\mathbb{Z}/p^m\mathbb{Z})$-homogeneous spaces. On the other hand, $T_{r,m}$ is a $G_1(\mathbb{Z}/p^m\mathbb{Z})$-torsor over S_r. We let δ_m denote the diagonal action of $G_1(\mathbb{Z}/p^m\mathbb{Z})$ on $p_{Y,*}(\mathcal{O}_Y[\kappa])$ over S_r. Over S_r

$$\rho_\kappa = p_{Y,*}(\mathcal{O}_Y[\kappa])/\delta_m(G_1(\mathbb{Z}/p^m\mathbb{Z})), \tag{2.2.6}$$

From the isomorphism (2.2.5) one obtains an isomorphism

$$\begin{aligned}\phi_m : {} & H^0(S_m, \rho_\kappa) \\ & \xrightarrow{\sim} \{f \in Mor_{\mathcal{V}_{m,m}}(G_{1/\mathcal{V}_{m,m}}, \mathbf{G}_{a/\mathcal{V}_{m,m}}) \mid f(hgut) = \kappa(t)h \cdot f(g), \\ & \qquad\qquad h \in G_1(\mathbb{Z}_p), u \in U_1, t \in T_1\}.\end{aligned}$$

These isomorphisms are clearly compatible with varying m. Composing with the evaluation at the identity map yields a map

$$\beta_\kappa : H^0(S_m, \rho_\kappa) \to \mathcal{V}_{m,m}^{U_1}.$$

Because of the compatibilities as m varies, this also makes sense for $m = \infty$, in which case we have an injection

$$\beta_\kappa : H^0(S_\infty, \rho_\kappa) \to \mathcal{V} = \mathcal{V}_{\infty,\infty}^{U_1}. \tag{2.2.7}$$

The image of β_κ is naturally contained in $\mathcal{V}[\kappa]$.
From (2.2.7) we obtain an injection
(2.2.8)
$Ig : H^0({}_{K(U,\infty)}Sh(V), [W_\tau]) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = H^0({}_{K(U,\infty)}Sh(V), \rho_\tau) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p \to \mathcal{V} \otimes_{\mathcal{O}_v} \mathbb{C}_p.$

This is defined by restricting a section of $H^0({}_{K(U,\infty)}Sh(V), \rho_\tau)$ to a formal neighborhood of the Igusa tower in the special fibre of the normalization $\widehat{{}_K\mathbb{S}}$ of ${}_K\mathbb{S}$ in ${}_KSh(V)$.
When $G = GU(V, -V)$ the same arguments apply, but in the definition of G_1, $GL(n)$ is replaced by $GL(n) \times GL(n)$, and in (2.2.4) $GL_{\mathcal{O}}(\omega_{r,m})$ is replaced by the subgroup preserving the splitting of $Lie(\hat{\mathbb{A}})$ coming from the splitting of $\mathbb{A}$. In particular, when the prime-to-p levels are compatible, there is a commutative diagram
(2.2.9)

$$\begin{tikzcd}
H^0({}_{K(U,\infty)}Sh(2V), [W_\tau]) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p \arrow[r, "res'"] \arrow[d, "Ig_{2V}"'] & H^0({}_{K(U,\infty)}Sh(V,-V), [W_\tau]) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p \arrow[d, "Ig_{V,-V}"'] \\
\mathcal{V}_{2V} \otimes_{\mathcal{O}_v} \mathbb{C}_p \arrow[r, "r_V"] & \mathcal{V}_{V,-V} \otimes_{\mathcal{O}_v} \mathbb{C}_p
\end{tikzcd}$$

where res' is the map coming from the inclusion of Igusa towers as in (2.1.11).

(2.3) p-adic modular forms and the q-expansion principle.

Now we return to the situation of (1.5), with the Shimura datum $(GU(2V), X(2V))$. We write $Sh(L_P)$ instead of $Sh(L_P, X_P)$. For simplicity, we again restrict attention to one-dimensional $[W_\tau]$. Then the Fourier expansion of (1.5.6.8), applied to

$$H^0({}_{K(U,\infty)}Sh(2V), [W_\tau]) := \varinjlim_m H^0({}_{K(U,m)}Sh(2V), [W_\tau]),$$

takes values in

$$\hat{\bigoplus_{\beta \in U^*}} H^0({}_{K_P(\infty)}Sh(L_P), [W_{\tau_P}]) := \hat{\bigoplus_{\beta \in U^*}} \varinjlim_m H^0({}_{K_{L_P}(m)}Sh(L_P), [W_{\tau_P}]).$$

These can be translated into locally constant functions on $L_P(\mathbf{A}_f)$ as in the discussion following (1.5.6.5), and as indicated there, it suffices to consider values on $L_P(\mathbf{A}_f^p)$. In [Hi04, 8.3.2], Hida explains how to fill in the lower horizontal arrow in the following commutative diagram:

(2.3.1)
$$\begin{tikzcd}
H^0({}_{K(U,\infty)}Sh(2V),[W_\tau])\otimes_{\overline{\mathbb{Q}}}\mathbb{C}_p \arrow[r, "F.J.^P"] \arrow[d, "Ig"'] & \widehat{\bigoplus_{\beta\in U^*}} H^0({}_{K_P(\infty)}Sh(L_P),[W_{\tau_P}])\otimes_{\overline{\mathbb{Q}}}\mathbb{C}_p \arrow[d, "="'] \\
\mathcal{V}\otimes_{\mathcal{O}_v}\mathbb{C}_p \arrow[r, "(F.J.^P)_{\mathbb{C}_p}"] & \widehat{\bigoplus_{\beta\in U^*}} H^0({}_{K_P(\infty)}\mathbb{S}_P,[W_{\tau_P}])\otimes_{\mathcal{O}_v}\mathbb{C}_p
\end{tikzcd}$$

More precisely, and more usefully, Hida explains how to construct an *integral* map

$$\mathcal{V}\xrightarrow{F.J.^P}\widehat{\bigoplus_{\beta\in U^*}} H^0({}_{K_P(\infty)}\mathbb{S}_P,\mathcal{O}_{\mathbb{S}_P}) \tag{2.3.2}$$

which yields the bottom line of (2.3.1) upon tensoring with $\mathbb{C}_p$.[6]
Now we can state

Theorem 2.3.3 (q-expansion principle, [Hi04]).
(a) The map $F.J.^P$ of (2.3.2) is injective and its cokernel has no p-torsion.
(b) Let $f\in H^0({}_{K(U,\infty)}Sh(2V),[W_\tau])$ and suppose f is defined over $\overline{\mathbb{Q}}$, viewed as a subfield of $\mathbb{C}$ or of $\mathbb{C}_p$. Then the expansions $F.J.^P(f)$, defined via (2.3.2) or (1.5.6.8), coincide, and the following are equivalent:

(i) $Ig(f)\in H^0(S_\infty,\rho_\kappa)\otimes\mathcal{O}_{\mathbb{C}_p}$
(ii) $F.J.^P(f)$ *has coefficients in* $\mathcal{O}_{\mathbb{C}_p}$.

Here, as in (1.5), *the coefficients of $F.J.^P(f)$ can be viewed as functions on $L_P(\mathbf{A}_f)$, and to test their integrality it suffices to consider their values on $L_P(\mathbf{A}_f)$.*

When $n=1$ and $E=\mathbb{Q}$, this theorem, or rather the corrected version of this theorem incorporating a growth condition at the cusps, is essentially due to Katz; for general E, still with $n=1$, it is due to Ribet. The principal ingredient in the proof is the irreducibility theorem 2.1.10.

(2.4) The case of definite groups.

We end our discussion of p-adic modular forms with a naive description when V is definite. The comparison of this naive description, which is useful, for

[6] Actually Hida only considered the case of level prime to p; the general case is treated in [SU].

calculations, and the geometric description of the previous section is made in (2.4.7). We will need it to understand how the restriction of a p-adic modular form on $U(2V)$ to $U(V,-V)$ can be described in the naive sense.
Throughout this section we assume that $< \bullet, \bullet >_\sigma$ is positive definite for all $\sigma \in \Sigma$ (so $a_\sigma = n$ for all σ).

(2.4.1) *Spaces of forms and rational structures.*

For applications to definite unitary groups, we can avoid similitude factors, so for the moment we let G denote $U(V)$ or $U(-V)$ (since these are canonically identified, the distinction is made primarily for ease of subsequent notation). In what follows, we consider only compact subgroups $K \subset G(\mathbf{A}^f)$ of the form $K = \prod_v K_v$, the product being over finite places of $\mathbb{Q}$, with K_v a subgroup of G_v. We fix a rational prime p such that all places of E dividing p split in $\mathcal{K}$ and let $K^p = K \cap G(\mathbf{A}^{f,p}) \cong \prod_{v \neq p} K_v$.
Let ρ be a complex algebraic character of G. Via the fixed isomorphism $\mathbb{C}_p \cong \mathbb{C}$ we view ρ as an algebraic character over $\mathbb{C}_p$. Then ρ has a model over some finite extension F of $\mathbb{Q}_p$. We fix such an F. For each finite place v of $\mathbb{Q}$ let $\mathfrak{s}_v : K_v \to \mathrm{GL}(\mathfrak{L}_v)$ be a finite-dimensional F-representation of K_v factoring through a finite quotient of K_v and such that $\mathfrak{s}_v$ and $\mathfrak{L}_v$ are trivial for almost all v and for $v = p$. Let $\mathfrak{s} = \otimes_{v,F}\mathfrak{s}_v$ and $\mathfrak{L} = \otimes_{v,F}\mathfrak{L}_v$. The product $G_\infty \times K$ acts on $\mathbb{C} \otimes_F \mathfrak{L}$ via $\rho \otimes \mathfrak{s}$.
For a finite set S of places of $\mathbb{Q}$ and a finite-dimensional complex vector space H let $C^\infty(G(\mathbf{A}^S), H)$ denote the space of functions from $G(\mathbf{A}^S)$ to $W_\sigma(\mathbb{C})$ that are smooth as functions of the infinite component of $G(\mathbf{A}^S)$ and locally constant as functions of the finite component. If S contains ∞, $G' \subset G(\mathbf{A}^S)$ is an open subgroup, and M is any set, then we write $C^\infty(G', M)$ for the set of locally constant functions from G' to M.
Let

$$\begin{aligned}&\mathcal{A}_0(G,K,\rho,\mathfrak{s}) = \\ &\qquad = \{f \in C^\infty(G(\mathbf{A}), \mathbb{C} \otimes_F \mathfrak{L})) \mid f(\gamma g \cdot g_\infty k) = (\rho \otimes \mathfrak{s})(g_\infty \times k)^{-1} f(g)\},\end{aligned}$$

where $\gamma \in G(\mathbb{Q})$, $g \in G(\mathbf{A})$, $g_\infty \in G_\infty$, and $k \in K$. For any F-algebra R let

$$\begin{aligned}&\mathcal{A}_f(G,K,\rho,\mathfrak{s})(R) = \\ &\qquad\quad = \{f \in C^\infty(G(\mathbf{A}^f), R \otimes_F \mathfrak{L}) \mid f(\gamma \cdot gk) = (\rho \otimes \mathfrak{s})(\gamma \times k^{-1}) f(g)\},\end{aligned}$$

where $\gamma \in G(\mathbb{Q})$, $g \in G(\mathbf{A}^f)$, and $k \in K$. Note that there is a canonical isomorphism

$$(2.4.1.1) \qquad \mathcal{A}_f(G,K,\rho,\mathfrak{s})(R) = \mathcal{A}_f(G,K,\rho,\mathfrak{s})(F) \otimes_F R.$$

Restriction to $G(\mathbf{A}^f)$ defines a natural isomorphism

$$(2.4.1.2) \qquad \mathrm{res} : \mathcal{A}_0(G,K,\rho,\mathfrak{s}) \xrightarrow{\sim} \mathcal{A}_f(G,K,\rho,\mathfrak{s})(\mathbb{C}),$$

and hence, by (2.4.1.1), $\mathcal{A}_f(G,K,\rho,\mathfrak{s})(F)$ defines an F-structure on $\mathcal{A}_0(G,K,\rho,\mathfrak{s})$.

When ρ or $\mathfrak{s}$ is the trivial one-dimensional representation, we drop it from our notation.

(2.4.2) *Integral structures.*

Let R be a commutative ring. For any $R[K]$-module M let

$$\mathcal{A}(G,K,M) = \\ = \{f \in C^\infty(G(\mathbf{A}^f),M) \mid f(\gamma g k) = k^{-1}\cdot f(g), \gamma \in G(\mathbb{Q}), k \in K\}.$$

If $K' \subseteq K$ is an open subgroup then $\mathcal{A}(G,K,M) \subseteq \mathcal{A}(G,K',M)$ and there is a trace map $\mathrm{tr}_{K',K} : \mathcal{A}(G,K',M) \to \mathcal{A}(G,K,M)$ defined by $\mathrm{tr}_{K',K}f(x) = \sum_{y\in K/K'} yf(xy)$. These maps are clearly functorial in M and R and they satisfy

$$\text{(2.4.2.1)} \qquad \mathrm{tr}_{K'',K} = \mathrm{tr}_{K',K} \circ \mathrm{tr}_{K'',K'}, \quad K'' \subseteq K' \subseteq K.$$

Let A be the ring of integers of F. We choose a K_v-stable A-lattice $\Lambda_{\mathfrak{s}_v}$ in each $\mathfrak{L}_v$ and let $\Lambda_{\mathfrak{s}} = \otimes_{v,A}\Lambda_{\mathfrak{s}_v}$. Clearly $\mathcal{A}(G,K,\Lambda_{\mathfrak{s}})$ is an A-lattice in $A_f(G,K,\mathfrak{s})(F)$.

Let $\Gamma_K = G(\mathbb{Q}) \cap K_p$. For χ an $R^\times$-valued character of Γ_K and M an $R[K]$-module let

$$\mathcal{A}_f(G,K,\chi,M) = \{f \in C^\infty(G(\mathbf{A}^{f,p}) \times K_p, M \mid \\ f(\gamma g k) = \chi(\gamma^{-1})\cdot k^{-1}f(g), \gamma \in \Gamma_K, k \in K\}.$$

Weak approximation shows that restriction to $G(\mathbf{A}^{f,p}) \times K_p$ yields an isomorphism

$$\text{(2.4.2.2)} \qquad \mathcal{A}(G,K,M) \xrightarrow{\sim} \mathcal{A}_f(G,K,\mathbf{1},M).$$

Similarly, when R is an F-algebra, restriction to $G(\mathbf{A}^{f,p}) \times K_p$ yields an isomorphism

$$\text{(2.4.2.3)} \qquad \mathcal{A}_f(G,K,\rho,\mathfrak{s})(R) \xrightarrow{\sim} \mathcal{A}_f(G,K,\rho,\mathfrak{L}\otimes_F R).$$

It follows from (2.4.2.3) that to define an A-lattice in $\mathcal{A}_f(G,K,\rho,\mathfrak{s})(F)$ it suffices to define an A-lattice in $\mathfrak{L}$. In particular, $\mathcal{A}_f(G,K,\rho,\Lambda_{\mathfrak{s}})$ defines an A-lattice in $\mathcal{A}_f(G,K,\rho,\mathfrak{s})$.

For $K' \subseteq K$ we define a trace map $\mathrm{tr}_{K',K} : \mathcal{A}_f(G,K',\chi,M) \to \mathcal{A}_f(G,K,\chi,M)$ just as we did above. These maps also satisfy (2.4.2.1) and are functorial in M, and R and agree with our previous definitions via (2.4.2.2) when $\chi = \mathbf{1}$.

(2.4.3) *p-adic forms*

For a topological space X and a group $G' = H \times H'$ with $H \subseteq G(\mathbb{Q}_p)$ and $H' \subseteq G(\mathbf{A}^{f,p})$ open sets, we write $C^p(G', X)$ for the space of maps from G' to X that are continuous on H (for the p-adic topology) and locally constant on H'.

Let G_1 denote the group scheme $R_{\mathcal{O}_{E,p}/\mathbb{Z}_p}\mathrm{GL}(n)$ over $\mathbb{Z}_p$ and fix an identification of G with G_1 over $\mathbb{Q}_p$. Let $B \subseteq G_1$ be its upper-triangular Borel. Let $P \supseteq B$ be a standard parabolic of G_1. Let L be its standard Levi subgroup and U_P its unipotent radical. Upon fixing an identification $\mathcal{O}_{E,p} = \prod_{w|p} \mathcal{O}_{E,w}$ we have $G_1(\mathbb{Z}_p) = \prod_{w|p} \mathrm{GL}(n, \mathcal{O}_{E,w})$, $P(\mathbb{Z}_p) = \prod_{w|p} P_w(\mathcal{O}_{E,w})$ where $P_w \subseteq \mathrm{GL}(n)$ is a standard parabolic corresponding to a partition $p_w : n = n_{1,w} + \cdots + n_{l_w,w}$ of n, and $L(\mathbb{Z}_p) = \prod_{w|p} L_w$ where L_w is the set of block diagonal matrices $\mathrm{diag}(A_1, ..., A_{l_w})$ with $A_i \in \mathrm{GL}(n_{i,w}, \mathcal{O}_{E,w})$. Let $L_1 \subseteq L(\mathbb{Z}_p)$ be the subgroup $\prod_{w|p} L_{w,1}$ where $L_{w,1}$ is the subgroup defined by $\det(A_i) = 1$. Let $P_1 = L_1 U_P(\mathbb{Z}_p)$. For $m \geq 0$ let $U_{P,m} = \{x \in G_1(\mathbb{Z}_p) \mid x \bmod p^m \in (P_1 \mod p^m)\}$. So $\cap U_{P,m} = P_1$. Let $I_{P,m} = \{x \in G_1(\mathbb{Z}_p) \mid x \bmod p^m \in P(\mathbb{Z}_p/p^m)\}$.

Assume that $K = G_1(\mathbb{Z}_p) \times K^p$. Let $K_{P,m} = U_{P,m} \times K^p$ and let $K_P = P_1 \times K^p$. Then $\cap K_{P,m} = K_P$. Let R be a p-adic ring and M any finite R-module that is also an $R[K]$-module on which K_p acts trivially. Let

$$\mathcal{A}_p(G, K_P, M) = \{f \in C^p(G(\mathbf{A}^f), M) \mid f(\gamma g k) = k^{-1} \cdot f(g), \gamma \in G(\mathbb{Q}), k \in K_P\}.$$

Since $M/p^r M$ is discrete, the canonical projections $M \twoheadrightarrow M/p^r M$ together with (2.4.2.2) induce a canonical isomorphism

$$\mathcal{A}_p(G, K_P, M) \xrightarrow{\sim} \varprojlim_r \varinjlim_m \mathcal{A}_f(G, K_{P,m}, M/p^r M). \tag{2.4.3.1}$$

Let A and $\Lambda_{\mathfrak{s}}$ be as in (2.4.2) and take $R = A$. Then $\Lambda_{\mathfrak{s}}$ provides an important example of an M as above. We call $\mathcal{A}_p(G, K_P, \Lambda_{\mathfrak{s}})$ the space of ($\Lambda_{\mathfrak{s}}$-valued) p-adic modular forms on G relative to P (and K). When P is understood then we just call this the space of p-adic modular forms.

(2.4.4) *Characters*

The group $L(\mathbb{Z}_p)$ normalizes each $K_{P,m}$, $m > 0$, and so acts on $\mathcal{A}_p(G, K_P, M)$ via right translation, determining an action of

$$Z_P = L(\mathbb{Z}_p)/L_1 = P(\mathbb{Z}_p)/P_1 \xrightarrow{\sim} \varprojlim_m I_{P,m}/U_{P,m}.$$

For any $R^\times$-valued character χ of Z_P we define $\mathcal{A}_p(G, K_P, M)[\chi]$ to be the submodule on which Z_P acts via χ. Note that

$$Z_P \xrightarrow{\sim} \prod_{w|p} (\mathcal{O}_{E,w}^\times)^{l_w}, \quad \mathrm{diag}(A_1, ..., A_{l_w})) \mapsto (\det(A_1), ..., \det(A_{l_w}). \tag{2.4.4.1}$$

By an *arithmetic* character of $Z(\mathbb{Z}_p)$ we will mean a character χ such that $\chi = \chi_0\rho$ with χ_0 a finite-order character and ρ arising from the restriction of an algebraic character of G as in (2.4.1). For an arithmetic character χ let m_χ be the smallest integer such that χ_0 is trivial on $I_{P,m_\chi}/U_{P,m_\chi}$. For $m \geq m_\chi$ we can extend χ to a character of $I_{P,m}$ by setting $\chi(x) = \chi(z)$ where $z \in Z_p$ is such that z has the same image as x in $I_{P,m}/U_{P,m}$. We also extend χ to a character of the center of $L(\mathbb{Q}_p)$ as follows. We fix a uniformizer ξ_w of $\mathcal{O}_{E,w}$ for each $w|p$. Then we put

$$\chi(\mathrm{diag}(\xi_w^{r_1}1_{n_{1,w}}, ..., \xi_w^{r_{l_w}}1_{n_{l_w,w}})) = \rho(\mathrm{diag}(\xi_w^{r_1}1_{n_{1,w}}, ..., \xi_w^{r_{l_w}}1_{n_{l_w,w}})).$$

Since any element of the center of $L(\mathbb{Q}_p)$ can be uniquely written as a product of a diagonal element as above and an element in $L(\mathbb{Z}_p)$ this is enough to define the desired extension.

For any $R^\times$-valued arithmetic character $\chi = \chi_0\rho$ of Z_P we have injective maps

$$\begin{gathered} r_\chi : \mathcal{A}_f(G, K^0_{P,m}, \chi, M) \hookrightarrow \mathcal{A}_p(G, K_P, M)[\chi], \quad m \geq m_\chi, \\ r_\chi(f)(g) = \chi(x_p)f(x), \\ g = \gamma x, \gamma \in G(\mathbb{Q}), x \in G(\mathbf{A}^{f,p}) \times I_{P,m}, \end{gathered} \tag{2.4.4.2}$$

where $K^0_{P,m} = K^p \times I_{P,m}$. A product decomposition of g as in (2.4.4.2) always exists by weak approximation.

An important observation is that the r_χ's induce an isomorphism

$$\varinjlim_{m\geq n} \mathcal{A}_f(G, K^0_{P,m}, \chi, M/p^rM) \xrightarrow{\sim} \mathcal{A}_p(G, K_P, M/p^rM)[\chi]. \tag{2.4.4.3}$$

For the surjectivity we note that for any $f \in \mathcal{A}_p(G, K_P, M/p^rM)[\chi]$ if m is sufficiently large then f belongs to $\mathcal{A}(G, K_{P,m}, M/p^r)$. For $g \in G(\mathbf{A}^{f,p}) \times I_{P,m}$ let $s_\chi(f)(g) = \chi(g_p^{-1})f(g)$. Then $s_\chi(f) \in \mathcal{A}_f(G, K^0_{P,m}, \chi, M/p^r)$ and $r_\chi(s_\chi(f)) = f$.

(2.4.5) *Hecke actions.*

Let K be an open compact subgroup of $G(\mathbf{A}^f)$. Suppose $H \subseteq G(\mathbf{A})$ is a subgroup containing K and M is a $\mathbb{Z}[K]$-module on which K_v acts trivially for all v not in some finite set Σ_M. For an open subgroup $K' \subseteq K$ let $C(H, K', M)$ be the space of functions $f : H \to M$ such that $f(gk) = k^{-1}f(g)$ for all $k \in K'$. Then for any $g \in H \cap G(\mathbf{A}^f)$ such that $g_v = 1$ if $v \in \Sigma_M$ and any two open subgroups $K', K'' \subseteq K$, the double coset $K'gK''$ determines a map from $C(H, K', M)$ to $C(H, K'', M)$ by

$$[K'gK'']f(x) = \sum_i f(xg_i^{-1}), \quad K'gK'' = \sqcup K'g_i. \tag{2.4.5.1}$$

This map is obviously functorial in M. It is easy to see that from (2.4.5.1) we get actions of double cosets on the various modules of functions defined

in the preceding sections; one need only observe that these actions preserve the requisite topological properties. These actions are compatible with all the various comparisons and isomorphisms described so far.
One important observation is that if g is such that the $K_{P,m}gK_{P,m}$ have the same left-coset representatives for all m, then from (2.4.3.1) we get an action of $T(g) = \varinjlim_m [K_{P,m}gK_{P,m}]$ on $\mathcal{A}_p(G, K_P, M)$. If we further assume that g_p is in the center of $L(\mathbb{Q}_p)$, then $T(g)$ commutes with the action of $P(\mathbb{Z}_p)$ and hence stabilizes each $\mathcal{A}_p(G, K_P, M)[\chi]$, χ a character of Z_P.
Let $C_P \subset G_1(\mathbb{Q}_p)$ be those elements g in the center of $L(\mathbb{Q}_p)$ such that

$$g^{-1}U_P(\mathbb{Z}_p)g \subseteq U_P(\mathbb{Z}_p). \tag{2.4.5.2}$$

For such g we also have
(2.4.5.3)
$$I_{P,m}gI_{P,m} = \sqcup I_{P,m}gu_i \quad \text{and} \quad U_{P,m}gU_{P,m} = \sqcup U_{P,m}gu_i, \quad u_i \in U_P(\mathbb{Z}_p).$$

Also, for $g, g' \in C_P$,

$$\begin{array}{c} I_{P,m}gI_{P,m} \cdot I_{P,m}g'I_{P,m} = I_{P,m}gg'I_{P,m} \\ U_{P,m}gU_{P,m} \cdot U_{P,m}g'U_{P,m} = U_{P,m}gg'U_{P,m} \end{array}, \tag{2.4.5.4}$$

where the multiplications are the usual double-coset multiplications.
Let $M_1 = R_{\mathcal{O}_{E,p}/\mathbb{Z}_p}M_{n\times n}$. Suppose $K_p \subseteq G_1(\mathbb{Z}_p)$ and let Δ_K be the semigroup in $M_1(\mathbb{Q}_p)$ generated by K_p and those g such that $g^{-1} \in C_P$. Let M be an $A[K]$-module for which there exists a finite set of places Σ_M, $p \notin \Sigma_M$, such that K_v acts trivially on M if $v \notin \Sigma_M$. Let $g \in G(\mathbf{A}^f)$ be such that $g_v = 1$ for all $v \in \Sigma_M$, $g_p \in C_P$, and suppose that

$$KgK = \sqcup Kg_i, \quad g_{i,p}^{-1} \in \Delta_K. \tag{2.4.5.5}$$

Under this assumption we define an action of KgK on $\mathcal{A}_f(G, K, \chi, M)$ by

$$\begin{array}{c} (KgK)f(x) = \sum_i \chi(\gamma_i)f(x_i), \\ \gamma_i \in G(\mathbb{Q}), \gamma_i x g_i^{-1} = x_i \in G(\mathbf{A}^{f,p}) \times K_p; \end{array} \tag{2.4.5.6}$$

the assumption (2.4.5.5) ensures that $\gamma_i^{-1} \in \Delta_K$.
Let χ be an $A^\times$-valued arithmetic character of Z_P. If $g_p \in C_P$ and $g_v = 1$ for $v \in \Sigma_M$ then (2.4.5.3) implies that (2.4.5.5) holds with K replaced by $K^0_{P,m}$ for any $m \geq m_\chi$. In particular, (2.4.5.6) defines an action of $\tilde{T}(g) = (K^0_{P,m}gK^0_{P,m})$ on $A_f(G, K^0_{P,m}, \chi, M)$, $m \geq m_\chi$, which is multiplicative in such g by (2.4.5.4). Moreover, viewing $\mathcal{A}_f(G, K^0_{P,m}, \chi, \Lambda_{\mathfrak{s}})$ as an A-submodule of $\mathcal{A}_f(G, K_{P,m}, \rho, \sigma)(F)$ we find that

$$\tilde{T}(g) = \chi^{-1}(g_p)[K_{P,m}gK_{P,m}]. \tag{2.4.5.6}$$

Additionally, it is clear from the definitions that

$$r_\chi \circ \tilde{T}(g) = T(g) \circ r_\chi, \tag{2.4.5.7}$$

where r_χ is as in (2.4.4.2).

(2.4.6) *Pairings.*

For $K \subseteq G(\mathbf{A}^f)$ an open compact subgroup, let

$$_K S(G) = G(\mathbb{Q})\backslash G(\mathbf{A}^f)/K.$$

This is a finite set. Let R be a commutative ring and let M, M' be $R[K]$-modules on which K_p acts trivially. Suppose $(\bullet,\bullet) : M \times M' \to R$ is a K-equivariant R-pairing. Given an $R^\times$-valued character χ of Γ_K we define an R-pairing

$$< \bullet, \bullet >_K : \mathcal{A}_f(G,K,\chi,M) \times \mathcal{A}_f(G,K,\chi^{-1},M') \to R,$$

$$< f, g >_K = \sum_{[x]\in {}_K S(G)} (f(x), g(x)), \quad x \in G(\mathbf{A}^{f,p}) \times K_p. \tag{2.4.6.1}$$

These pairings (integration with respect to the measure $d\mu_K(g)$ of (0.2.4)) are clearly functorial in R, M, M'. The following lemma records some basic but important properties of these pairings. For simplicity we will assume that

$$\gamma x k = x, \gamma \in G(\mathbb{Q}), x \in G(\mathbf{A}^f), k \in K \implies k = 1. \tag{2.4.6.2}$$

This holds for sufficiently small K.

(2.4.6.3) LEMMA. *Assume* (2.4.6.2).

(i) *If* $(\bullet,\bullet)$ *is a perfect pairing, then so is* $< \bullet, \bullet >_K$.

(ii) *Let* $K' \subseteq K$ *be an open subgroup. Then*

$$\begin{gathered} < f, \mathrm{tr}_{K',K}(h) >_K = < f, h >_{K'}, \\ f \in \mathcal{A}_f(G,K,\chi,M), \ h \in \mathcal{A}_f(G,K',\chi^{-1},M'). \end{gathered} \tag{2.4.6.4}$$

(iii) *Suppose there exists a finite set of places* Σ_M *such that* K_v *acts trivially on* M *if* $v \notin \Sigma_M$. *Let* $K', K'' \subseteq K$ *be open subgroups and let* $g \in G(\mathbf{A}^f)$ *be such that* $g_p = 1$ *and* $g_v = 1$ *for all* $v \in \Sigma_M$. *Then*

$$\begin{gathered} < [K''gK']f, h >_{K'} = < f, [K'g^{-1}K'']h >_{K''}, \\ f \in \mathcal{A}_f(G,K'',\chi,M), \ h \in \mathcal{A}_f(G,K',\chi^{-1},M'). \end{gathered} \tag{2.4.6.5}$$

Part (i) holds because $\mathcal{A}_f(G,K,\chi,M)$ is spanned by the functions $\delta_{x,m}$, $x \in G(\mathbf{A}^{f,p}) \times K_p$, $m \in M$, defined by

$$\delta_{x,m}(y) = \begin{cases} \chi(\gamma^{-1}) \cdot k^{-1}m & y = \gamma x k, \gamma \in \Gamma_K, k \in K, \\ 0 & \text{otherwise.} \end{cases}$$

The assumption (2.4.6.2) ensures that these functions are well-defined. Part (ii) is also clear from (2.4.6.2). Part (iii) follows from part (ii) and the observation that

$$[K''gK'](f(x)) = \mathrm{tr}_{K' \cap g^{-1}K''g, K'}(f(xg^{-1})).$$

For our purposes, the most important situation to which we will apply Lemma (2.4.6.3) is when R is the integer ring of some finite extension of F, χ comes from an arithmetic character of Z_P, and $M = \Lambda_{\mathfrak{s}} \otimes_A R$. In this case we let $M' = \mathrm{Hom}_A(\Lambda_{\mathfrak{s}}, R)$, the latter being an $R[K]$-module with the usual action, and let $(\bullet, \bullet)$ be the canonical pairing between M and M'. Let

$$(2.4.6.6) \qquad < \bullet, \bullet >_{m,\chi,\sigma} = < \bullet, \bullet >_{K^0_{P,m}}, \quad m \geq m_\chi,$$

where the right-hand side is defined by (2.4.6.1) with our current choices of M, M', etc. Assuming that (2.4.6.2) holds for $K^0_{P,m}$, then all the conclusions of Lemma (2.4.6.3) hold for $< \bullet, \bullet >_{m,\chi,\sigma}$.

(2.4.7) *Comparison with the geometric picture.*

Previously, we defined spaces of p-adic modular form for $GU(V)$ from a geometric perspective. We now compare these to the spaces in (2.4.3). For simplicity we will assume that the similitude character maps K onto $\widehat{\mathbb{Z}}^\times$.

In the definite situation the geometric constructions of (2.2) are simple. The varieties ${}_{K(U,m)}Sh(V)$ clearly all have models over $\mathcal{O}_v$; the base change to $\mathcal{O}_v/p^r$ is just $\mathcal{T}_{r,m}$. From this it is easily deduced that $\mathcal{V}^U_{r,m}\Gamma(\mathcal{T}_{r,m}, \mathcal{O}_{\mathcal{T}_{r,m}})$ is naturally identified with the set of $\mathcal{O}_v/p^r$-valued functions on ${}_{K(U,m)}Sh(V)$ and so, under our hypotheses on K, with $\mathcal{A}_f(G, K(U,m), \mathcal{O}_v/p^m)$ (in particular, these identifications are compatible with varying r and m. Thus we have that

$$(2.4.7.1) \qquad \mathcal{V} = \varprojlim_r \varinjlim_m \mathcal{V}^U_{r,m} = \varprojlim_r \varinjlim_m \mathcal{A}_f(G, K(U,m), \mathcal{O}_v/p^m).$$

Then (2.4.3.1) identifies $\mathcal{V}$ with $\mathcal{A}_p(G, K_B, \mathcal{O}_v)$. The spaces of p-adic modular forms for other parabolics are obtained by taking U_P-invariants.

The restriction on K can be dropped; then $\mathcal{V}$ is identified with a direct sum of copies of $\mathcal{A}_p(G, K_B, \mathcal{O}_v)$.

3. Fourier coefficients of Siegel Eisenstein series on unitary groups

(3.0) Conventions for automorphic forms on unitary groups. We let Σ_E denote the set of archimedean places of E. Let W be any hermitian space over $\mathcal{K}$ of dimension n, and define $-W$ and $2W = W \oplus (-W)$ as in §1. Set

$$W^d = \{(v,v) \mid v \in W\}, \qquad W_d = \{(v,-v) \mid v \in W\}$$

These are totally isotropic subspaces of $2W$. Let P be the stablizer of W^d in $U(2W)$. As a Levi component of P we take the subgroup $M \subset U(2W)$ which is stablizer of both W^d and W_d. Then $M \simeq GL(W^d)$. We let U denote the unipotent radical of P.

The decomposition $2W = W^d \oplus W_d$ is a complete polarization. Choose a basis $(u_1,\ldots,u_m)$ for W, so that (u_i,u_i) is a basis for W^d. Let $(-v_j,v_j)$, $j = 1,\ldots,m$, be the dual basis of W_d. For any $A \in GL(n)_{\mathcal{K}}$, we define $m(A)$ to be the element of $U(2W)$ with matrix $\begin{pmatrix} A & 0 \\ 0 & {}^t\bar{A}^{-1}\end{pmatrix}$ in the basis $\{(u_i,u_i)\} \cup \{(-v_j,v_j)\}$, where $\bar{A}$ is the image of A under the non-trivial Galois automorphism of $\mathcal{K}/E$. We will let

$$w = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$$

in the same basis; then $P\backslash PwP$ is the big cell in the Bruhat decomposition of $P\backslash U(2W)$.

All automorphic forms will be assumed K_∞-finite, where K_∞ will be a maximal compact modulo center subgroup of either $U(2W)(\mathbb{R})$ or $U(W)(\mathbb{R})$, as appropriate. Conventions are as in §1.5; in particular K_∞ will be associated to a CM point, except where otherwise indicated.

We let $GU(2W)$ be the group of rational similitudes, as in §1. Let $GP \subset GU(2W)$ denote the stabilizer of W^d, and let GM be the normalizer of M in GP. We can identify $GM \xrightarrow{\sim} M \times \mathbb{G}_m$ where M acts as $GL(W^d)$ and $\mathbb{G}_m$ acts via the center of $GL(W_d)$. Here and below $\mathbb{G}_m$ designates $\mathbb{G}_{m,\mathbb{Q}}$. In other words, writing GP in standard form:

$$GP = \{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}\} \tag{3.0.1}$$

with $D = d \cdot {}^tc(A)^{-1}$ for some scalar d, we can identify the factor $\mathbb{G}_m \subset GM$ with the group of matrices

$$\{d(t) = \begin{pmatrix} 1_n & 0 \\ 0 & t1_n \end{pmatrix}\} \subset GU(2W). \tag{3.0.2}$$

Let v be any place of E, $|\cdot|_v$ the corresponding absolute value on $\mathbb{Q}_v$, and let

$$\delta_v(p) = |N_{\mathcal{K}/E} \circ \det(A(p))|_v^{\frac{n}{2}} |\nu(p)|^{-\frac{1}{2}n^2}, \; p \in GP(E_v). \tag{3.0.3}$$

This is the local modulus character of $GP(E_v)$. The adelic modulus character of $GP(\mathbf{A})$, defined analogously, is denoted $\delta_{\mathbf{A}}$. Let χ be a Hecke character of $\mathcal{K}$. We view χ as a character of $M(\mathbb{A}_E) \xrightarrow{\sim} GL(W^d)$ via composition with det. For any complex number s, define

$$\delta^0_{P,\mathbf{A}}(p,\chi,s) = \chi(\det(A(p))) \cdot |N_{\mathcal{K}/E} \circ \det(A(p))|^s_v |\nu(p)|^{-ns}$$

$$\begin{aligned}\delta_{\mathbf{A}}(p,\chi,s) = \delta_{\mathbf{A}}(p)\delta^0_{P,\mathbf{A}}(p,\chi,s) = \\ = \chi(\det(A(p))) \cdot |N_{\mathcal{K}/E} \circ \det(A(p))|_v^{\frac{n}{2}+s} |\nu(p)|^{-\frac{1}{2}n^2-ns}.\end{aligned}$$

The local characters $\delta_{P,v}(\cdot,\chi,s)$ and $\delta^0_{P,v}(\cdot,\chi,s)$ are defined analogously. The restrictions to M of the characters $\delta_{P,v}$, $\delta^0_{P,v}$, and so on are denoted by the same notation.

As in (2.2), the symmetric domain $X(2W)$ is isomorphic to the $X^d_{n,n}$ of tube domains. Let $\tau_0 \in X(2W)$ be a fixed point of K_∞, X^+ the connected component of $X(2W)$ containing τ_0, $GU(n,n)^+ \subset GU(2W)(\mathbb{R})$ the stabilizer of X^+. Thus $X^+ \xrightarrow{\sim} \prod_{\sigma\in\Sigma_E} X^+_{n,n;\sigma}$ with $X^+_{n,n;\sigma}$ the symmetric space associated to $U(n,n) = U(E_\sigma)$. Let $GK_\infty \subset GU(n,n)^+$ be the stabilizer of τ_0; thus GK_∞ contains K_∞ as well as the center of $GU(n,n)$.

In the tube domain realization, the canonical holomorphic automorphy factor associated to GP and GK_∞ is given as follows. Let $\tau = (\tau_\sigma)_{\sigma\in\Sigma_E} \in X^+$ and $h = \left(\begin{pmatrix} A_\sigma & B_\sigma \\ C_\sigma & D_\sigma \end{pmatrix}\right)_{\sigma\in\Sigma_E} \in GU(n,n)^+$. Then the triple

$$J(h,\tau) = (C_\sigma\tau_\sigma + D_\sigma)_{\sigma\in\Sigma_E},\ J'(h,\tau) = (\bar{C}^t_\sigma\tau_\sigma + \bar{D}_\sigma)_{\sigma\in\Sigma_E}, \nu(h) \tag{3.0.4}$$

defines a canonical automorphy factor with values in $(GL(n,\mathbb{C})\times GL(n,\mathbb{C}))^d \times GL(1,\mathbb{R})$ (note the misprint in [H3, 3.3]). Write $J(h) = J(h,\tau_0) = (J_\sigma(h))_{\sigma\in\Sigma_E}$ and define $J'(h)$ and $J'_\sigma(h)$ analogously. Given a pair of integers (μ,κ), we define a complex valued function on $GU(n,n)^+$:

$$\mathbf{J}_{\mu,\kappa}((h_\sigma)_{\sigma\in\Sigma_E}) = \prod_{\sigma\in\Sigma_E} \det J_\sigma(h)^{-\mu} \cdot \det(J'_\sigma(h))^{-\mu-\kappa} \cdot \nu(h)^{n(\mu+\kappa)} \tag{3.0.5}$$

For purposes of calculation, we let $\tau_0 = (\sigma(\daleth))_{\sigma\in\Sigma}$, where $\daleth$ is the trace zero element of $\mathcal{K}$ chosen in (1.4). We also write $\daleth_\sigma = \sigma(\daleth)$. Then the stabilizer GK_∞ is rational over the reflex field $E(GU(2W),X(2W)) = E(\mathcal{K},\Sigma)$, and the map $h \mapsto J(h)$ is a rational function on the algebraic group $GU(2W)$ with values in GK_∞, rational over $E(\mathcal{K},\Sigma)$.

(3.1) The Siegel Eisenstein series and doubling.

In this section we let G denote $U(W)$, $H = U(2W)$, viewed alternatively as groups over E or, by restriction of scalars, as groups over $\mathbb{Q}$. Identifying G

with $U(-W)$, we obtain a natural embedding $G\times G \subset H$. We choose maximal compact subgroups $K_{\infty,G} = \prod_{v\in\Sigma_E} K_{v,G} \subset G(\mathbb{R})$ and $K_\infty = \prod_{v\in\Sigma_E} K_v \subset H(\mathbb{R})$ – as at the end of the previous subsection – such that

$$K_\infty \cap (G\times G)(\mathbb{R}) = K_{\infty,G}\times K_{\infty,G}.$$

We will be more precise about these choices in (4.3).

(3.1.1) *Formulas for the Eisenstein series*

Let χ be a unitary Hecke character of $\mathcal{K}$. We view χ as a character of $M(\mathbb{A}_E) \xrightarrow{\sim} GL(W^d)$ via composition with det. Consider the induced representation

$$I(\chi,s) = \mathrm{Ind}(\chi|\cdot|_{\mathcal{K}}^{s}) \xrightarrow{\sim} \otimes_v I_v(\chi_v|\cdot|_v^s), \tag{3.1.1.1}$$

the induction being normalized; the local factors I_v, as v runs over places of E, are likewise defined by normalized induction. At archimedean places we assume our sections to be K_∞-finite. For a section $f(h;\chi,s)\in I(\chi,s)$ (cf. [H4, I.1]) we form the Eisenstein series

$$E_f(h;\chi,s) = \sum_{\gamma\in P(k)\backslash U(2V)(k)} f(\gamma h;\chi,s) \tag{3.1.1.2}$$

This series is convergent for $\mathrm{Re}(s) > n/2$, and it can be continued to a meromorphic function on the entire plane. We now fix an integer $m \geq n$ and assume

$$\chi|_{\mathbf{A}} = \varepsilon_{\mathcal{K}}^{m} \tag{3.1.1.3}$$

Then the main result of [T] states that the possible poles of $E_f(g;\chi,s)$ are all simple, and can only occur at the points in the set

$$\frac{n-\delta-2r}{2},\ r = 0,\ldots,[\frac{n-\delta-1}{2}], \tag{3.1.1.4}$$

where $\delta = 0$ if m is even and $\delta = 1$ if m is odd.

(3.1.2) The standard L-function via doubling. Let (π, H_π) be a cuspidal automorphic representation of G, $(\pi^\vee, H_{\pi^\vee})$ its contragredient, which we assume given with compatible isomorphisms of $G(\mathbf{A})$-modules

$$\pi \xrightarrow{\sim} \otimes_v \pi_v,\ \pi^\vee \xrightarrow{\sim} \otimes_v \pi_v^\vee. \tag{3.1.2.1}$$

The tensor products in (3.1.2.1) are taken over places v of the totally real field E, and at archimedean places π_v is a admissible $(\mathfrak{g}_v, K_{v,G})$-module, which we assume to be of cohomological type, with lowest $K_{v,G}$-type (cf., e.g., [L1]) τ_v. For each v we let $(\bullet,\bullet)_{\pi_v}$ denote the canonical bilinear pairing $\pi_v\otimes\pi_v^\vee \to \mathbb{C}$.

Let $f(h;\chi,s)$ be a section, as above, $\varphi \in H_\pi$, $\varphi' \in H_{\tilde{\pi}}$, and let $\varphi'_\chi(g) = \varphi'(g)\chi^{-1}(\det g')$. We define the zeta integral:
(3.1.2.2)

$$Z(s,\varphi,\varphi',f,\chi) = \int_{G\times G)(\mathbb{Q})\backslash(G\times G)(\mathbf{A})} E_f((g,g');\chi,s)\varphi(g)\varphi'_\chi(g')dgdg'.$$

The Haar measures $dg = dg'$ on $G(\mathbf{A})$ are normalized as in (0.2.2). The relation to the integral in terms of Tamagawa measure is determined by (0.2.3).

The theory of this function, due to Piatetski-Shapiro and Rallis [PSR], was worked out (for trivial χ) by Li [L2] and more generally in [HKS,§6]. We make the following hypotheses:

(3.1.2.4) Hypotheses

(a) There is a finite set of finite places S_f of E such that, for any non-archimedean $v \notin S_f$, the representations π_v, the characters χ_v, and the fields $\mathcal{K}_w$, for w dividing v, are all unramified;

(b) The section f admits a factorization $f = \otimes_v f_v$ with respect to (3.1.1.1).

(c) The functions φ, φ' admit factorizations $\varphi = \varphi_{S_f} \otimes \otimes_{v\notin S_f}\varphi_v$, $\varphi' = \varphi_{S_f} \otimes \otimes_{v\notin S_f}\varphi'_v$, with respect to (3.1.2.1)

(d) For $v \notin S_f$ non-archimedean, the local vectors f_v, φ_v, and φ'_v, are the normalized spherical vectors in their respective representations, with $(\varphi_v,\varphi'_v)_{\pi_v} = 1$.

(e) For v archimedean, the vector φ_v (resp. φ'_v) is a non-zero highest (resp. lowest) weight vector in τ_v (resp. in $\tau_v^\vee$), such that $(\varphi_v,\varphi'_v)_{\pi_v} = 1$.

We let $S = \Sigma_E \cup S_f$. Define

$$d_n(s,\chi) = \prod_{r=0}^{n-1} L(2s+n-r,\varepsilon_{\mathcal{K}}^{n-1+r}) = \prod_v d_{n,v}(s,\chi), \tag{3.1.2.5}$$

the Euler product on the right being taken only over finite places;

$$Q^0_W(\varphi,\varphi') = \int_{G(\mathbb{Q})\backslash G(\mathbf{A})} \varphi(g)\varphi'(g)dg; \tag{3.1.2.6}$$

$$Z_S(s,\varphi,\varphi',f,\chi) = \int_{\prod_{v\in S} G(E_v)} f_v((g_v,1);\chi,s)(\pi_v(g_v)\varphi,\varphi')dg_v; \tag{3.1.2.7}$$

$$\tilde{Z}_S(s,\varphi,\varphi',f,\chi) = \prod_{v\in S}[d_{n,v}(s,\chi)]Z_S(s,\varphi,\varphi',f,\chi).$$

The integral in (3.1.2.7) converges absolutely in a right halfplane and admits a meromorphic continuation to all s.[7] We have the following identity of meromorphic functions on $\mathbb{C}$:

[7] For non-archimedean places this is worked out in detail in [HKS]. There is no published reference for unitary groups at archimedean places in general. Shimura [S97] calculates the archimedean integrals explicitly for holomorphic automorphic forms of scalar weight. For general π_∞ meromorphic continuation is established by Kudla and Rallis [KR] for symplectic groups by reduction to principal series. The same technique applies to unitary groups, bearing in mind that not all unitary groups are quasi-split. For the special values we have in mind we appeal to the explicit calculations of Garrett [G].

(3.1.2.8) BASIC IDENTITY OF PIATETSKI-SHAPIRO AND RALLIS.

$$d_n(s,\chi)Z(s,\varphi,\varphi',f,\chi) = \tilde{Z}_S(s,\varphi,\varphi',f,\chi)L^S(s+\frac{1}{2},\pi,\chi,St).$$

Here $L^S(s+\frac{1}{2},\pi,\chi,St) = \prod_{v\notin S} L_v(s+\frac{1}{2},\pi_v,\chi_v,St)$*, where* $L_v(s+\frac{1}{2},\pi_v,\chi_v,St)$ *is the local Langlands Euler factor attached to the unramified representations* π_v *and* χ_v *and the standard representation of the L-group of* $G\times R_{\mathcal{K}/\mathbb{Q}}\mathbb{G}_{m,\mathcal{K}}$.[8]

For any place $v\notin S$, there is a formal (unramified) base change from π_v to a representation $BC(\pi_v)$ of $G(\mathcal{K}\otimes_E E_v) \xrightarrow{\sim} GL(m,\mathcal{K}\otimes_E E_v)$, and

$$L_v(s,\pi_v,\chi_v,St) = L(s,BC(\pi_v)\otimes\chi_v\circ\det),$$

where the right-hand term is the standard Godement-Jacquet Euler factor (cf. [H4,I.1] for a further discussion).

If we assume φ_{S_f} and φ'_{S_f} to be factorizable over the $v\in S_f$, with respect to the isomorphisms (3.1.2.1), then the integral Z_S also breaks up as a product of local integrals multiplied by the factor Q_W^0, as in [H3,H4], as well as [PSR,Li92]. To treat congruences it seems preferable not to impose factorizability at this stage. However, under special hypotheses on the local data we can obtain a factorization, as follows. Write $G_v = G(E_v)$, and let $K_v\subset G(E_v)$ be a compact open subgroup fixing φ. The natural map $G\times G\to P\backslash H$ defines an isomorphism between $G\times 1$ and the open $G\times G$ orbit in the flag variety $P\backslash H$ [PSR, p. 4]. In particular, $P\cdot(G\times 1)$ is open in H and $P\cap(G\times 1) = \{1\}$. It follows that, if Y is any locally constant compactly supported function on G_v, there is a unique section $f_Y(h,\chi,s)\in I_v(\chi_v,s)$ such that $f_Y((g,1),\chi,s) = Y(g)$ for all $g\in G_v$, $s\in\mathbb{C}$. Let $f_{K_v}(h,\chi,s) = f_{Y(K_v)}(h,\chi,s)$, where $Y(K_v)$ is the characteristic function of the open compact subgroup K_v chosen above. With this choice, we have

$$\int_{G_v} f_{K_v}((g_v,1);\chi,s)(\pi_v(g_v)\varphi,\varphi')dg_v = vol(K_v) \tag{3.1.2.9}$$

for any s. If we choose $f_v = f_{K_v}$ for all $v\in S_f$, the basic identity becomes

$$d_n(s,\chi)Z(s,\varphi,\varphi',f,\chi) =$$
$$= d_{n,S}(s,\chi)\cdot vol(K_{S_f})Z_\infty(s,\varphi,\varphi',f,\chi)L^S(s+\frac{1}{2},\pi,\chi,St),$$

where $d_{n,S}(s,\chi) = \prod_{v\in S_f}[d_{n,v}(s,\chi)]$, $K_{S_f} = \prod K_v$, and

$$Z_\infty(s,\varphi,\varphi',f,\chi) = \int_{\prod_{v\in\Sigma_E} G(E_v)} f_v((g_v,1);\chi,s)(\pi_v(g_v)\varphi,\varphi')dg_v. \tag{3.1.2.10}$$

[8] As in the previous footnote, there is no published reference for the meromorphic continuation and functional equation of standard L-functions of unitary groups, although the results of Kudla and Rallis for symplectic groups adapt to the case of unitary groups. In the applications we will restrict attention to π admitting base change to automorphic representations of $GL(n,\mathcal{K})$, which immediately implies the analytic continuation of the standard L-functions.

The integrals in (3.1.2.10) are purely local in the following sense. For any archimedean place v we can define a local analogue of (3.1.2.7) by

$$Z_v(s,\varphi_v,f_v,\chi_v) = \int_{G(E_v)} f_v((g_v,1);\chi_v,s)\pi_v(g_v)\varphi_v dg_v. \tag{3.1.2.11}$$

This is a function of s with values in the $K_{\infty,v}$-finite vectors of π_v, absolutely convergent and holomorphic in a right half-plane, and admitting a meromorphic continuation to $\mathbb{C}$ (see note 5). Let $\tau_v^+ \subset \tau_v$ denote the line spanned by the highest weight vector φ_v, let $p_v^+ : \pi_v \rightarrow \tau_v^+$ denote orthogonal projection. Define the meromorphic function $Z_v(s,f_v,\chi_v)$ by

$$p_v^+(Z_v(s,\varphi_v,f_v,\chi_v)) = Z_v(s,f_v,\chi_v)\cdot\varphi_v.$$

This is well-defined, because τ_v^+ is a line, and does not depend on the choice of φ_v because both sides are linear functions of φ_v. Let $Z_\infty(s,f,\chi) = \prod_{v\in\Sigma_E} Z_v(s,f_v,\chi_v)$ It then follows that

$$Z_\infty(s,\varphi,\varphi',f,\chi) = Z_\infty(s,f,\chi)Q_W^0(\varphi,\varphi'), \tag{3.1.2.12}$$

hence that

$$\begin{aligned} &d_n(s,\chi)Z(s,\varphi,\varphi',f,\chi) \\ &\quad = d_{m,S}(s,\chi)\cdot vol(K_{S_f})Z_\infty(s,f,\chi)L^S(s+\frac{1}{2},\pi,\chi,St)Q_W^0(\varphi,\varphi') \end{aligned} \tag{3.1.2.13}$$

We note the following consequence of the basic identity in the form (3.1.2.13). Let $K_f = K_{S_f}\times K^S$, where $K^S = \prod_{w\notin S} K_w$ is a product of hyperspecial maximal compact subgroups fixing φ and φ'.

(3.1.2.14) Hypothesis. *We assume f, $s = s_0$, and χ can be chosen so that*

$$d_{n,S}(s_0,\chi)Z_\infty(s_0,f,\chi)\neq 0.$$

Thus we are staying away from poles of the local Euler factors in $d_{n,S}(s,\chi)$) and the global Euler products $d_n(s,\chi)$ and $L^S(s+\frac{1}{2},\pi,\chi,St)$ have neither zeros nor poles at $s = s_0$. This hypothesis is easy to verify in practice, e.g. in the situation of [H3]; the only subtle point is the non-vanishing of $Z_\infty(s_0,f,\chi)$ when ϕ_v is holomorphic and the Eisenstein series defined by f_v is nearly holomorphic, and in this case the non-vanishing follows from the arguments of Garrett [G]. Let $\mathcal{A}_0(\pi,S)$, resp. $\mathcal{A}_0(\pi^\vee,S)$ denote the space spanned by K_f-invariant cusp forms on G, that generate irreducible automorphic representations whose v-component is isomorphic to π_v (resp. to $\pi_v^\vee$) for all $v\notin S_f$, and belonging to the highest weight subspace τ_v^+ of τ_v (resp. to the lowest weight subspace of $\tau_v^\vee$ for all $v\in\Sigma_E$. Then (3.1.2.12) asserts that the bilinear forms $Z(s_0,\varphi,\varphi',f,\chi)$ and Q_W^0 on $\mathcal{A}_0(\pi,S)$ are proportional. (If π occurs with multiplicity one in

$\mathcal{A}_0(G)$, then this is automatic.) This simplifies the arguments of §3 of [H3], proving, when $E = \mathbb{Q}$, that critical values of $L(s, \pi, \chi, St)$ are $\mathcal{K}$-multiples of a basic period equal to an elementary expression multiplied by a square norm of the form $Q^0_W(\varphi, \varphi')$, where φ and φ' are arithmetic holomorphic modular forms of the given type.[9] In particular, this gives a somewhat more natural proof of Corollary 3.5.12 of [H3], to the effect that, under the hypotheses of loc. cit. (existence of sufficiently many critical values) $Q^0_W(\varphi, \varphi')$ depends up to arithmetic factors only on the abstract representation π^S.

(3.1.2.15) REMARK. Local Euler factors $L_v(s, \pi_v, \chi_v, St)$ are defined in [HKS] for all finite places, by the method of Piatetski-Shapiro and Rallis. It should not be difficult to prove by global methods that these factors coincide with $L(s, BC(\pi_v) \otimes \chi_v \circ \det)$, at least when π_v is a local component of an automorphic cuspidal representation for a definite unitary group. A complete proof would require local functional equations at archimedean primes. When $n = 2$ the unitary group can be compared simply to the multiplicative group of a quaternion algebra, and the result can be proved easily in that case directly.

(3.1.3) *Eisenstein series and zeta integrals on similitude groups.*

We now return to the situation of (3.1). Let $GH = GU(2W)$, and consider the subgroup $GU(W, -W) = G(U(W) \times U(-W) \subset GH$. The induced representation $I(\chi, s)$ and the Eisenstein series $E_f((g, g'); \chi, s)$ can be extended in various ways to automorphic forms on GH. Let $GP \subset GH$ denote the Siegel parabolic defined in (3.2.5). Global characters of $GM = M \times \mathbb{G}_m$ are given by pairs (χ, υ) where χ is a Hecke character of $M^{ab} = R_{\mathcal{K}/\mathbb{Q}}\mathbb{G}_{m,\mathbb{Q}}$, lifted to a character of M by composition with the determinant, and υ is a Hecke character of $\mathbf{A}^\times/\mathbb{Q}^\times$. Let

$$I(\chi, \upsilon, s) = \mathrm{Ind}_{GP}^{GH}((\chi| \cdot |^s_{\mathcal{K}}) \circ \det \cdot \upsilon \circ \nu). \tag{3.1.3.1}$$

For any section $f(h; \chi, \upsilon, s) \in I(\chi, \upsilon, s)$ we form the Eisenstein series $E_f(h, \chi, \upsilon, s)$ by the analogue of the formula (3.1.1.2). The character υ factors through a character of GH and does not affect convergence.

Let π, π' be automorphic representations of $GU(W)$, with central characters ξ, ξ', respectively. Let $\varphi \in \pi$, $\varphi' \in \pi'$, and consider $\varphi \otimes \varphi'$ by restriction as an automorphic form on $GU(W, -W)$. Let Z be the identity component of the center of $GU(W, -W)$, which we may also view as a central subgroup of GH, or (via projection) as a central subgroup of $GU(W)$. We assume

$$\xi \cdot \xi' \cdot \xi_{\chi,\upsilon} = 1; \tag{3.1.3.2}$$

[9] In [H3] only values of s in the absolutely convergent range are considered, but the argument remains valid in general under hypothesis (3.1.2.14). See [H5] for a more extended discussion of this point.

here $\xi_{\chi,\upsilon}$ is the central character of $I(\chi,\upsilon,s)$. We can then define the zeta integral

$$(3.1.3.3)\quad Z(s,\varphi,\varphi',f,\chi,\upsilon) = \int_{Z(\mathbf{A})GU(W,-W))(\mathbb{Q})\backslash(GU(W,-W)(\mathbf{A})} E_f((g,g');\chi,s)\varphi(g)\varphi'_{\chi}(g')dgdg'.$$

The basic identity (3.1.2.8) then takes the following form (cf. [H3,(3.2.4)]):
(3.1.3.4)

$$d_n(s,\chi)Z(s,\varphi,\varphi',f,\chi,\upsilon) = Q_W(\varphi,\varphi')\tilde{Z}_S(s,\varphi,\varphi',f,\chi)L^S(s+\frac{1}{2},\pi,\chi,St).$$

where

$$(3.1.3.5)\qquad Q_W(\varphi,\varphi') = \int_{Z(\mathbf{A})GU(W)(\mathbb{Q})\backslash GU(W)(\mathbf{A})} \varphi(g)\varphi'(g)\xi_{\chi,\upsilon}^{-1}dg$$

and the remaining terms are as in (3.1.2). The period $Q_W(\varphi,\varphi')$ is slightly more natural from the standpoint of Shimura varieties.

(3.1.4) *Holomorphic Eisenstein series.*

Fix (μ,κ) as in (3.0.1). Define

$$\chi^* = \chi\cdot|N_{\mathcal{K}/E}|^{\frac{\kappa}{2}}.$$

Suppose the character χ has the property that

$$(3.1.4.1)\qquad \chi^*_{\sigma}(z) = z^{\kappa},\ \chi^*_{c\sigma}(z) = 1\ \forall\sigma\in\Sigma_E$$

Then the function $\mathbf{J}_{\mu,\kappa}$, defined in (3.0.5), belongs to

$$(3.1.4.2)\qquad I_n(\mu-\frac{n}{2},\chi^*)_{\infty} = I_n(\mu+\frac{\kappa-n}{2},\chi)_{\infty}\otimes|\nu|_{\infty}^{\frac{n\kappa}{2}}$$

(cf. [H3,(3.3.1)]). More generally, define

$$(3.1.4.3)\qquad \mathbf{J}_{\mu,\kappa}(h,s+\mu-\frac{n}{2}) = \mathbf{J}_{\mu,\kappa}(h)|\det(J(h)\cdot J'(h))|^{-s}\in I_n(s,\chi^*)_{\infty}$$

When $E=\mathbb{Q}$, these formulas just reduce to the formulas in [H3].
Let $f_{\infty}(h,\chi,s) = \mathbf{J}_{\mu,\kappa}(h,s+\mu-\frac{n}{2})$, and suppose the Eisenstein series $E_f(h;\chi,s)$ is holomorphic at $s=0$. The local section $\mathbf{J}(\mu,\kappa)$ is a holomorphic vector in the corresponding induced representation, and in what follows we will extend it to a global section f so that $E_f(h;\chi,0)$ is a holomorphic automorphic form. This is always the case if $\chi/|\chi|$ is a character of $U(1)$ and if f is a Siegel-Weil section, as we will be assuming in later articles. It is also the case for the specific sections f considered in (3.2) and (3.3), where holomorphy is verified

by explicit calculation of Fourier coefficients (see especially (3.3.3.2), (3.2.2.3), and (3.3.4.8)). As in [H3, (3.3.4)] we can identify $E_f(h;\chi,0)$ with an element of $H^0(Sh(2W),\mathcal{E}_{\mu,\kappa})$ where $\mathcal{E}_{\mu,\kappa}$ is the automorphic vector bundle defined in [H3,(3.3)]. The identification is as in (1.3.6) and depends on a choice of canonical trivialization of the fiber of $\mathcal{E}_{\mu,\kappa}$ at τ_0.
The center of symmetry $s=\frac{1}{2}$ for $L(s,\pi,\chi,St)$ in the unitary normalization corresponds via (3.1.2.8) to a zeta integral with the Eisenstein series at $s=s_0=0$. Since χ is by (3.1.1.3) a unitary character, this corresponds in turn to the relation to $s_0=\mu+\frac{\kappa-n}{2}=0$. More generally, the value of the motivically normalized L-function

$$L^{mot}(s,\pi,\chi*,St)\overset{def}{=}L(s-\frac{n-\kappa-1}{2},\pi,\chi,St)$$

at $s=s_0+\frac{n-\kappa}{2}$ corresponds as above to the Eisenstein series at $s_0=\mu+\frac{\kappa-n}{2}$), i.e. at $s=\mu$, as in [H3] (where μ was called m). It follows from (3.1.4.1) that we can choose m in (3.1.1.3) so that

(3.1.4.4) $$m=n+2s_0=2\mu+\kappa;$$

the assumption $m\geq n$ translates to $s_0\geq 0$, so the Eisenstein series is always to the right of the center of symmetry.

(3.2) Fourier coefficients of Eisenstein series: General considerations.

(3.2.1) *Notation and preliminaries.*

We let V, $2V=V\oplus -V$, and $H=U(2V)$ be as in (3.1) with $n=\dim V$. Let $\beth$ be as in (1.4). We fix an orthogonal basis $u_1,\cdots,u_n$ of V, and set

(3.2.1.1) $$e_j=(u_j,u_j),\qquad f_j=\delta_j\cdot(-u_j,u_j)$$

where

(3.2.1.2) $$\delta_j=\frac{1}{2\beth<u_j,u_j>_V}$$

With respect to this basis, the matrix of the skew-hermitian form $<,>_{2V,\beth}$ is given by

$$\begin{pmatrix}0 & 1_n\\ -1_n & 0\end{pmatrix}$$

Let $g\in GL(V)$. When no confusion is possible, we use the same letter g to denote the $n\times n$ matrix (g_{ij}) given by

$$g(u_i)=\sum_{j=1}^{n}g_{ji}u_j$$

Write $\delta = \mathrm{diag}(\delta_1, \cdots, \delta_n)$. Then $g \in U(V)$ if and only if ${}^t\bar{g}\delta^{-1}g = \delta^{-1}$, or equivalently $g\delta{}^t\bar{g} = \delta$. With respect to the basis $\{e_i, f_j\}$, the matrix corresponding to $(g,1) \in U(V) \times U(V) \subseteq U(2V)$ is

$$(g,1) = \begin{pmatrix} \frac{1}{2}(1_n + g) & \frac{1}{2}(1_n - g)\delta \\ \frac{1}{2}\delta^{-1}(1_n - g) & \frac{1}{2}\delta^{-1}(1_n + g)\delta \end{pmatrix} \tag{3.2.1.3}$$

We let

$$w' = \mathrm{diag}(-1_V, 1_V) = \begin{pmatrix} -1_n & 0 \\ 0 & 1_n \end{pmatrix} \quad \text{with respect to} \;\; 2V = V \oplus -V$$

Then with respect to the basis e_i, f_j we have

$$w' = \begin{pmatrix} \delta & 0 \\ 0 & {}^t\bar{\delta}^{-1} \end{pmatrix} \cdot w = m(\delta) \cdot w, \qquad w = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}, \tag{3.2.1.4}$$

This amounts to taking $g = -1_n$ in (3.2.1.3). In other words, the coset $P \cdot (-1_n, 1_n) \subset P \cdot G \times \{1\}$ belongs to the big cell PwP, and indeed

$$P \cdot (-1_n, 1_n) = Pw \cdot 1 \tag{3.2.1.5}$$

More generally, for any positive integer $r \leq n$ let V_r be the subspace of V spanned by $u_1, \cdots, u_r$. Let $V_r^\perp$ be the othogonal complement of V_r in V. We define

$$w'_r = \mathrm{diag}(-1_{V_r}, 1_{V_r^\perp}, 1_{V_r}, 1_{V_r^\perp}) \in U(2V) \tag{3.2.1.6}$$

Then $w' = w'_n$. With respect to the basis e_i, f_j we have

$$w'_r = \begin{pmatrix} {}_r\delta & 0 & 0 & 0 \\ 0 & 1_{n-r} & 0 & 0 \\ 0 & 0 & {}^t_r\bar{\delta}^{-1} & 0 \\ 0 & 0 & 0 & 1_{n-r} \end{pmatrix} \cdot w_r, \tag{3.2.1.7}$$

with ${}_r\delta = \mathrm{diag}(\delta_1, \cdots, \delta_r)$, where

$$w_r = \begin{pmatrix} 0 & 0 & 1_r & 0 \\ 0 & 1_{n-r} & 0 & 0 \\ -1_r & 0 & 0 & 0 \\ 0 & 0 & 0 & 1_{n-r} \end{pmatrix}. \tag{3.2.1.8}$$

By means of the basis $\{e_i, f_j\}$ we identify elements of H as $2n \times 2n$ matrices. Then if v is any finite place of E we define $H(\mathcal{O}_v)$ to be the subgroup of $H(E_v)$ consisting of matrices whose entries are in $\mathcal{O}_\mathcal{K} \otimes \mathcal{O}_v$. Let B be the stablizer of the flag

$$[e_1] \subset [e_1, e_2] \subset \cdots \subset [e_1, \cdots, e_n]$$

where $[e_1, \cdots, e_r]$ denotes the linear span of $e_1, \cdots, e_r$. Then B is a Borel subgroup, and we have the Iwasawa decomposition $H(E_v) = B(E_v)H(\mathcal{O}_v)$.
In what follows we fix a non-trivial character $\psi = \prod \psi_v$ of $\mathbf{A}/E$, as follows. Let $\mathbf{e}^0 = \prod \mathbf{e}^0_p$ be the unique character of $\mathbf{A}_{\mathbb{Q}}/\mathbb{Q}$ such that

$$\mathbf{e}^0_\infty(x) = e^{2\pi i x} \qquad (x \in \mathbb{R}),$$

and that $\mathbf{e}^0_p$ has conductor $\mathbb{Z}_p$ for every finite p. Let $\mathbf{e} = \prod \mathbf{e}_v$ be the character of $\mathbf{A}/E$ defined by

$$\text{(3.2.1.9)} \qquad \mathbf{e}(x) = \mathbf{e}^0(\mathrm{Tr}_{E/Q}(x)) \qquad (x \in \mathbf{A})$$

Alternatively, we may characterize $\mathbf{e}$ as the unique character of $\mathbf{A}/E$ such that for every archimedean place v we have

$$\mathbf{e}_v(x) = e^{2\pi\sqrt{-1}x} \qquad (x \in E_v = \mathbb{R}).$$

An arbitrary character of $\mathbf{A}/E$ is given by $x \mapsto \mathbf{e}(ax)$, with a some element of E. We let ψ be one such character with $a \in E$ totally positive, fixed henceforward. We can and will always assume a to be a unit at all primes dividing p. Thus

$$\text{(3.2.1.10)} \qquad \psi(x) = \mathbf{e}(ax) = \mathbf{e}^0(\mathrm{Tr}_{E/Q}(ax)) \qquad (x \in \mathbf{A})$$

In paricular, for every archimedean place v we have

$$\psi_v(x) = e^{2\pi a\sqrt{-1}x} \qquad (x \in E_v = \mathbb{R}).$$

(3.2.2) *Formulas for Fourier coefficients.*

We start with a general Siegel Eisenstein series $F = E^f(h, \chi, s)$ with $f \in I(\chi, s)$. Here we have written E^f instead of E_f, in order to leave space for a subscript to denote Fourier coefficients. Let Her_n be the space of all $n \times n$ hermitian matrices. For $\beta \in \mathrm{Her}_n(E)$ we define the character ψ_β of $U(\mathbb{Q})\backslash U(\mathbf{A})$ by

$$\psi_\beta(n(b)) = \psi(\mathrm{tr}(\beta b))$$

Note that we have $\mathrm{tr}(\beta\beta') \in E$ for any $\beta, \beta' \in \mathrm{Her}_n(E)$.
We now fix a Haar measure dx on $U(\mathbf{A}) \simeq \mathrm{Her}_n(\mathbf{A})$ as follows. First we take counting measure on the discrete subgroup $\mathrm{Her}_n(E) \subseteq \mathrm{Her}_n(\mathbf{A})$. We choose dx, so that the quotient mesaure on $U(E)\backslash U(\mathbf{A}) = \mathrm{Her}_n(E)\backslash\mathrm{Her}_n(\mathbf{A})$ is normalized, with total volume 1. Consider the lattice $\Lambda \subseteq \mathrm{Her}_n(E)$ consisting of all hermitian matrices with entries in $\mathcal{O}_{\mathcal{K}}$. We shall also need the dual lattice Λ^*, defined by

$$\Lambda^* = \{\beta \in \mathrm{Her}_n(E) \,|\, \mathrm{tr}(\beta\xi) \in \mathcal{O}_E \ \forall \ \xi \in \Lambda\}$$

For each finite place v of E we set

$$\Lambda_v = \mathrm{Her}_n(\mathcal{O}_v) = \Lambda \otimes \mathcal{O}_v,$$

Define Λ_v^* similarly. Then $\Lambda_v = \Lambda_v^*$ unless v ramifies in $\mathcal{K}$. Let dx_v be the Haar measure of $\mathrm{Her}_n(E_v)$ normalized by $\int_{\Lambda_v} dx_v = 1$. For any archimedean place v we set

$$dx_v = |\bigwedge_{j=1}^{n} dx_{jj} \bigwedge_{j<k} (2^{-1} dx_{jk} \wedge d\bar{x}_{jk})|$$

where x_{jk} is the (j,k)-entry of x_v. There is a constant $c(n, E, \mathcal{K})$ so that

$$dx = c(n, E, \mathcal{K}) \cdot \prod_v dx_v.$$

Since $\mathrm{Her}_n(\mathbf{A})$ is the product of n copies of $\mathbf{A}$ and $n(n-1)/2$ copies of $\mathbf{A}_{\mathcal{K}}$, we obtain (say from [Tate])

$$c(n, E, \mathcal{K}) = 2^{n(n-1)[E:\mathbb{Q}]/2} |\delta(E)|^{-n/2} |\delta(K)|^{-n(n-1)/4}, \tag{3.2.2.1}$$

where $\delta(E)$ and $\delta(\mathcal{K})$ are the discriminants of E and $\mathcal{K}$. This is the same as [S97], p. 153.

For $\beta \in \mathrm{Her}_n(E)$ we define the β-th Fourier coefficient

$$F_\beta(h) = \int_{U(\mathbb{Q})\backslash U(\mathbf{A})} F(uh)\psi_{-\beta}(u)du$$

as in (1.5.6).

We now assume that f is factorizable, and write $f = \otimes f_v$. If β has full rank n then a familiar calculation gives

(3.2.2.2)

$$E^f_\beta(h, \chi, s) = c(n, E, \mathcal{K}) \cdot \prod_v \int_{U(E_v)} f_v(wn_vh_v, \chi_v, s)\psi_{-\beta}(n_v)dn_v, \qquad (\det \beta \neq 0)$$

the product being over all places of E. Here w is the Weyl group element given by (3.2.1.4).

Remark 3.2.2.3. Suppose that for at least one place v the function $f_v(\bullet, \chi_v, s)$ is supported on the big cell $P(E_v)wP(E_v)$. Then (3.2.2.2) is valid for $h \in P(\mathbb{A})$ and *any* β. Indeed for $h \in P(\mathbb{A})$ we have

$$f(\gamma h, \chi, s) \neq 0 \Longrightarrow \gamma \in P(E)wP(E) = P(E)wU(E)$$

So that

$$E^f(h, \chi, s) = \sum_{\delta \in U(E)} f(w\delta h, \chi, s)$$

and (3.2.2.1) follows immediately for any β, not necessarily of full rank.

Write

$$W_{\beta,v}(h_v, f_v, s) = \int_{U(E_v)} f_v(wn_vh_v, \chi_v, s)\psi_{-\beta}(n_v)dn_v. \tag{3.2.2.4}$$

This function satisfy a transformation law as follows. Suppose

$$m = m(A) = \begin{pmatrix} A & 0 \\ 0 & {}^t\bar{A}^{-1} \end{pmatrix} \in M(E_v)$$

Then

$$\begin{aligned} W_{\beta,v}(mh_v, f_v, s) &= |N \circ \det A|_v^{n/2-s}\chi_v(\det A) \cdot W_{{}^t\bar{A}\beta A,v}(h_v, f_v, s) \\ &= |N \circ \det A|_v^{\frac{n-\kappa}{2}-s}\chi_v^*(\det A) \cdot W_{{}^t\bar{A}\beta A,v}(h_v, f_v, s) \end{aligned} \tag{3.2.2.5}$$

where $N = N_{\mathcal{K}/E}$.
We now recall a calculation of Shimura. In what follows, a is the totally positive element of E, prime to p, fixed in (3.2.1.10).

(3.2.2.6) Lemma. ([S97], 19.2) *Suppose β is of full rank n. Let v be a finite place of E. Let $f_v(\bullet, \chi_v, s)$ be the unique section which is invariant under $H(\mathcal{O}_v)$, and such that $f_v(1, \chi_v, s) = 1$. Let $m = m(A) \in M(E_v)$. Then $W_{\beta,v}(m, f_v, s) = 0$ unless ${}^t\bar{A}\beta A \in a^{-1}\mathfrak{D}(E/\mathbb{Q})_v^{-1}\Lambda_v^*$, where $\mathfrak{D}(E/\mathbb{Q})_v$ is the different of E_v relative to $\mathbb{Q}_p$ (p being the rational prime lying below v). In this case, one has*

$$W_{\beta,v}(m, f_v, s) =$$
$$= |N \circ \det A|_v^{n/2-s}\chi_v(\det A)g_{\beta,m,v}(\chi(\varpi_v)q_v^{-2s-n}) \cdot \prod_{j=1}^{n} L_v(2s + j, \chi\varepsilon_{\mathcal{K}/E}^{n-j})^{-1}.$$

Here $L_v(\bullet, \bullet)$ is the local abelian L-factor at v, with χ viewed as a character for $\mathbf{A}_E^\times$ by restriction, and $g_{\beta,m,v}$ is a polynomial with constant term 1 and coefficients in $\mathbb{Z}$. Let $\mathfrak{D}(E/\mathbb{Q})_v = \delta_v\mathcal{O}_v$ for some $\delta_v \in E_v$. If v is unramified in $\mathcal{K}$, and

$$\det(a\delta_v{}^t\bar{A}\beta A) \in \mathcal{O}_v^\times,$$

then $g_{\beta,m,v}(t) \equiv 1$.

Example. Let $n = 1$. Then $\beta \in E_v^\times$ and A is a scalar. Let $r \geq 0$ be the integer determined by

$$|a\delta_v\bar{A}A\beta|_v = q_v^{-r}$$

Then

$$g_{\beta,m,v}(t) = \frac{(1-t)[1-(qt)^{r+1}]}{1-qt}$$

(3.2.2.7) Corollary. *For any finite place v we let T_v be the characteristic function of $\mathfrak{D}(E/\mathbb{Q})_v^{-1}\Lambda_v^*$. Suppose that $\beta \in Her_n(E)$ is of full rank n. Let S be a finite set of places including all the archimedean ones and all places ramified in $\mathcal{K}$, and large enough so that the conditions of Lemma 3.2.2.6 are satisfied at any place $v \notin S$. Let $m = m(A) \in M(\mathbf{A})$. Then*

$$(3.2.2.8)\quad E^f_\beta(m,\chi,s) = c(n,E,\mathcal{K})\cdot|\det A|_{\mathcal{K}}^{n-s}\chi(\det A)\cdot(\prod_{v\in S} W_{{}^t\bar{A}\beta A,v}(1,f_v,s))$$

$$\cdot\prod_{v\notin S}[T_v(a^t\bar{A}\beta A)g_{\beta,m,v}(\chi(\varpi_v)q_v^{-2s-n})]\cdot\prod_{j=1}^n L^S(2s+j,\chi\varepsilon_{\mathcal{K}/E}^{n-j})^{-1}$$

Here $L^S(\bullet,\bullet)$ is the partial L-function, with χ viewed as a character for $\mathbf{A}_E^\times$ by restriction.

(3.2.2.9) Remarks.

(i) In the subsequent sections we will always assume S contains all primes of residue characteristic p. Suppose this is the case and $v \notin S$. Then the local factor $T_v(a^t\bar{A}\beta A)g_{\beta,m,v}(\chi(\varpi_v)q_v^{-2s_0-n})$ is p-adically integral for any half-integer s_0. In particular, the p-adic denominators of the Fourier coefficients $E^f_\beta(m,\chi,s_0)$, normalized by the product of the partial L-functions, are determined by the local factors at $v \in S$ and by the global factors.

(ii) Let $\beta \in \mathrm{Her}_n(E)$ be of full rank n. We say β is *S-primitive* if $\det(a\beta) \in \mathcal{O}_v^\times$ for all $v \notin S$. The condition depends implicitly on a. Since S contains the ramified primes, the local different factors can be ignored. It follows from (3.2.2.7) that for S-primitive β, the product of local coefficients satisfies

$$\prod_{j=1}^n L^S(2s_0+j,\chi\varepsilon_{\mathcal{K}/E}^{n-j})\cdot\prod_{v\notin S}W_{\beta,v}(1,f_v,s_0) = 1$$

and in particular is a p-adic unit.

(iii) On the other hand, the factors $g_{\beta,m,v}(\chi(\varpi_v)q_v^{-2s-n})$ are p-units at half-integer values of s, provided v is prime to p. Our local data at primes v dividing p will guarantee the vanishing of coefficients $W_{\beta,v}$ unless $\det(a\delta_v{}^t\bar{A}\beta A) \in \mathcal{O}_v^\times$, and we will only evaluate the coefficients at points $m = m(A)$ with $A_v \in GL(n,\mathcal{O}_v)$). Thus we will always have the local factors $g_{\beta,m,v}(t) \equiv 1$ for v dividing p, and the product

$$(3.2.2.10)\qquad T^0(\beta,m(A),s) = \prod_{v\notin S}[T_v(a^t\bar{A}\beta A)g_{\beta,m,v}(\chi(\varpi_v)q_v^{-2s-n})]$$

will always be a p-adic unit when $s \in \frac{1}{2}\mathbb{Z}$.

(iv) In other words, the p-adic behavior of the Eisenstein series is completely determined by the global normalizing factor $\prod_{j=1}^n L^S(2s+j,\chi\varepsilon_{\mathcal{K}/E}^{n-j})^{-1}$ and by the local factors at $v \in S$. Calculation of the local factors will occupy most of the rest of this section.

(3.3) LOCAL COEFFICIENTS OF HOLOMORPHIC EISENSTEIN SERIES.

In this section we consider a finite set S of places as in (3.2.2.7), containing all archimedean places, all places ramified in $\mathcal{K}/E$, all places dividing p, and all places at which the character χ_v is ramified. We also include in S a collection of finite places where, to guarantee non-vanishing of local zeta integrals for ramified π_v, f_v cannot be the unramified vector $f_v^{unr} \in I(\chi, s)$, i.e., the vector invariant under $H(\mathcal{O}_v)$. At the archimedean places we will take specific local data. Otherwise the data will vary according to circumstances to be defined later. The resulting calculation (3.3.1.5, 3.3.2.1) of the local Fourier coefficients at ramified finite primes is less precise than at unramified places.
We treat non-split places, split places, and archimedean places separately.

(3.3.1) *Finite non-split places.*

Let v be a finite place in S. Suppose first that v does not split in $\mathcal{K}$. We let w be the unique place of $\mathcal{K}$ dividing v. We define a special section in $I(\chi_v, s)$ as follows. Let u_v be a Schwartz function on $\mathrm{Her}_n(E_v)$. Define a section $f_v(h; \chi_v, s) \overset{def}{=} f_{u_v}(h; \chi_v, s) \in I(\chi_v, s)$ by the condition that it is supported in the big cell $P(E_v)wP(E_v)$, and

$$(3.3.1.2) \qquad f_v(wn(b); \chi_v, s) = u_v(b) \qquad (b \in \mathrm{Her}_n(E_v))$$

It is easy to see that $W_{\beta,v}(1, f_v, s) = \hat{u}_v(\beta)$. Together with the transformation law (3.2.2.5), we find that

$$(3.3.1.3) \qquad W_{\beta,v}(m(A)\tilde{f}_v, s) = |\det A|_v^{n/2-s}\chi_v(\det A) \cdot \hat{u}_v({}^t\bar{A}\beta A)$$

We now choose a lattice $L_v \subset \mathrm{Her}_n(E_v)$, and make the following assumption:

(3.3.1.4) HYPOTHESIS. *u_v is the characteristic function of L_v.*

Let $L_v^\vee$ be the dual lattice defined by

$$L_v^\vee = \{\beta \,|\, \psi(\mathrm{tr}\beta x) = 1 \text{ for all } x \in L_v\}$$

Then we have

$$(3.3.1.5) \qquad W_{\beta,v}(m(A), f_{u_v}, s) = T_v({}^t\bar{A}\beta A)|\det A|_v^{n/2-s}\chi_v(\det A) \cdot vol(L_v),$$

(3.3.2)*Finite split places.*

Next we consider the case where v is finite and splits in $\mathcal{K}$, of residue characteristic different from p. Let u_v be a Schwartz function on $\mathrm{Her}_n(E_v) \simeq M_{n,n}(E_v)$ ($n \times n$ matrices with entries in E_v). Then there is a section $f_{u_v}(h; \chi_v, s)$ such that $f_v(\bullet; \chi_v, 0)$ has support in $P(E_v)wP(E_v)$, and $f_v(wn(b); \chi_v, 0) = u_v(b)$. Formula (3.3.1.3) remains valid for all β. If u_v is chosen as in (3.3.1.4), then we write f_{L_v} instead of f_{u_v}. In what follows, $A \in GL(n, \mathcal{K}_v)$ can be written as a pair $(\mathbf{A}_v, \mathbf{B}_v)$ with $\mathbf{A}_v, \mathbf{B}_v \in GL(n, E_v)$, and $|\det(A)|_v = |\det(\mathbf{A}_v \cdot \mathbf{B}_v^{-1})|_v$, with conventions as in (3.3.4) below.

(3.3.2.1) Lemma. *With $f_v = f_{L_v}$, formula (3.3.1.5) is valid for all β.*

At split places other choices might be more convenient. For example, let $U_v \subset GL(n, E_v)$ be a compact open subgroup and τ_v a finite-dimensional irreducible representation of U_v. Let u_v be a matrix coefficient of τ_v, viewed as a function on $U_v \subset GL(n, E_v)$ and extended by zero to $M(n, E_v)$. Then u_v takes values in the integers of some cyclotomic field. It then follows immediately from (3.3.1.3) that:

(3.3.2.2) Lemma. *The functions $\hat{u}_v$ and $W_{\beta,v}(m(A), f_v, 0)$ are locally constant, compactly supported, not identically zero, and takes values in $\mathbb{Q}^{ab}$ with denominators bounded p-adically independently of τ_v.*

Indeed, the integral defining $\hat{u}_v$ is a finite sum of terms, each of which is an algebraic integer multiplied by a volume. The volume lies in $\mathbb{Q}$ and the denominators are bounded in terms of the orders of finite subgroups of $GL(n, E_v)$, independently of τ_v. The remaining factors in (3.3.1.5) are p-units.

(3.3.2.3) Remark 3.3.2.3 Alternatively, we can let u_v be a matrix valued function, namely the function τ_v, with values in $End(\tau_v)$, extended to zero off K_v. The Eisenstein series and its Fourier coefficients will then have values in $End(\tau_v)$. This will allow us to pair the Eisenstein series with forms taking values in the space of τ_v and its dual. The local zeta integral will be essentially a volume.

(3.3.3) *Archimedean places.*

Let $v \in S_\infty$ be a real place of E. We shall regard elements of $H(E_v) \simeq U(n, n)$ as $2n \times 2n$ matrices by means of the basis $\{e_i, f_j\}$ chosen in (3.2.1). Let $j = \sigma_v(\gimel)$. We let $K_v \subset H(E_v)$ be the maximal compact subgroup consisting of those matrices k with ${}^t\bar{k}\ \mathrm{diag}(j^2 I_n, -I_n)k = \ \mathrm{diag}(j^2 I_n, -I_n)$, where I_n denote the identity matrix of size n. Then $K_v \simeq U(n) \times U(n)$. We make this isomorphism explicit as follows. Set

$$\gamma = \begin{pmatrix} 1_n & 1_n \\ j^{-1}1_n & -j^{-1}1_n \end{pmatrix} \in GU(n, n)$$

Then for any $A, B \in U(n)$ one has

$$k(A, B) = \gamma \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \gamma^{-1} \in K_v$$

The map $(A, B) \mapsto k(A, B)$ is an isomorphism from $U(n) \times U(n)$ onto K_v. Let $x \in \mathrm{Her}_n(\mathbb{R})$. One easily checks that the Iwasawa decomposition of $wn(x)$ is given by

$$wn(x) =$$
$$= \begin{pmatrix} 1_n & -\frac{x}{-j^2+x^2} \\ 0 & 1_n \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{-j^2+x^2}} & 0 \\ 0 & \sqrt{-j^2+x^2} \end{pmatrix} k\Big(-\frac{x + j1_n}{\sqrt{-j^2+x^2}}, -\frac{x - j1_n}{\sqrt{-j^2+x^2}}\Big)$$

Let $m = 2\mu + \kappa$ as in (3.1.4.4), so that $\chi_v(-1) = (-1)^m$ (3.1.1.3). We follow Shimura [S82] and take f_v to be (up to sign) the v component of the canonical automorphy factor denoted $\mathbf{J}_{\mu,\kappa}(h, s - \frac{\kappa}{2})$ in (3.1.4.3); thus f_v is holomorphic for $s = s_0 = \frac{m-n}{2}$. More precisely,

$$\begin{aligned} f_v(wn(x), \chi_v, s) &= \det(-j^2 + x^2)^{-s-n/2} \det(\frac{-j1_n - x}{\sqrt{-j^2+x^2}})^m \\ &= (-1)^{mn} \cdot \delta(x - j1_n)^{-s-\frac{m+n}{2}} \delta(x + j1_n)^{-s+\frac{m-n}{2}} \end{aligned} \tag{3.3.3.1}$$

In subsequent articles we will identify f_v with a Siegel-Weil section for the theta lift of the trivial representation of $U(m)$. Continuing the calculation, and making the simple change of variables, $x \mapsto x/\alpha$, where $\alpha = -j/i > 0$, we find

$$\begin{aligned} &W_{\beta,v}(1, f_v, s) = \\ &= (-1)^{mn}(-j/i)^{-2ns} \int_{\mathrm{Her}_n(\mathbb{R})} \delta(x+i1_n)^{-s-\frac{m+n}{2}} \delta(x-i1_n)^{-s+\frac{m-n}{2}} e^{-2\pi i \mathrm{tr}(\beta x)} dx \\ &= (-1)^{mn}(-j/i)^{-2ns} \xi(1_n, \beta; s + \frac{n+m}{2}, s + \frac{n-m}{2}) \end{aligned}$$

([S82], p. 274, (1.25)). By ([S82], p. 275, (1.29)), this is equal to

$$\begin{aligned} &(-i)^{mn} 2^n \pi^{n^2} (-j/i)^{-2ns} \Gamma_n(s + \frac{n+m}{2})^{-1} \Gamma_n(s + \frac{n-m}{2})^{-1} \times \\ &\qquad\qquad \eta(21_n, \pi\beta; s + \frac{n+m}{2}, s + \frac{n-m}{2}) \end{aligned}$$

Choose $A \in GL(n, \mathbb{C})$ with $AA^* = \pi\beta$, where $A^* = {}^t\bar{A}$. By ([S82], p.280-281), we have

$$\begin{aligned} \eta(21_n, \pi\beta; s + \frac{n+m}{2}, s + \frac{n-m}{2}) &= \delta(\pi\beta)^{2s} \cdot \eta(2A^*A, 1_n; s + \frac{n+m}{2}, s + \frac{n-m}{2}) \\ &= (2\pi)^{2ns} \delta(\beta)^{2s} e^{-2\pi \mathrm{tr}(\beta)} \zeta(4A^*A; s + \frac{n+m}{2}, s + \frac{n-m}{2}) \end{aligned}$$

Thus

$$\begin{aligned} W_{\beta,v}(1, f_v, s) = &(-i)^{mn} 2^{n(m-n+1)} \pi^{ns+n(m+n)/2} (-j/i)^-2ns\delta(\beta)^{s-\frac{n-m}{2}} e^{-2\pi \mathrm{tr}(\beta)} \\ &\Gamma_n(s + \frac{n+m}{2})^{-1} \omega(4A^*A; s + \frac{n+m}{2}, s + \frac{n-m}{2}) \end{aligned}$$

The function $\omega(z; \mu, \lambda)$ is analytic in μ, λ and satisfies the functional equation

$$\omega(z; n - \lambda, n - \mu) = \omega(z; \mu, \lambda)$$

By (3.15) of Shimura we know $\omega(z;\mu,0)=1$. So at $s=(m-n)/2$ we obtain (3.3.3.2)

$$\begin{aligned} W_{\beta,v}(1,f_v,\frac{m-n}{2}) &= \\ &= (\beth_v)^{-mn+n^2}(-i)^{-n^2}2^{n(m-n+1)}\pi^{mn}\det(\beta)^{m-n}e^{-2\pi\mathrm{tr}(\beta)}\Gamma_n(m)^{-1} \\ &= \frac{(\beth_v)^{-mn+n^2}(-i)^{-n^2}2^{n(m-n+1)}\pi^{mn-n(n-1)/2}\det(\beta)^{m-n}}{\prod_{j=1}^{n}(m-j)!}\cdot e^{-2\pi\mathrm{tr}(\beta)}. \end{aligned}$$

The factor $e^{-2\pi\mathrm{tr}(\beta)}$ at the end is the value at $h_\infty=1$ of the function denoted q^β in §(1.5.6); more precisely, q^β factors over the archimedean primes, and $e^{-2\pi\mathrm{tr}(\beta)}$ is the factor at v. The coefficient preceding this factor is the local contribution at v to the Fourier coefficient f_β.

(3.3.4) *Local results at primes dividing p (choice of special functions at p)*

First we fix some notation.

(3.3.4.1) Notation. Let v be a place of E dividing p. Then v splits in $\mathcal{K}$ according to our assumptions. Throughout we shall identify E_v with $\mathcal{K}_w$, where w is the divisor of v with $w\in\Sigma_p$ (see (1.1.4)). We denote by $\mathcal{O}_v$ the ring of integers of E_v, and by $\mathfrak{p}_v$ the prime ideal in $\mathcal{O}_v$. For any pair of positive integers a,b we denote by $M_{a,b}$ or $M(a,b)$ the space of $a\times b$ matrices. Let dZ be the normalized Haar measure on $M_{n,n}(E_v)$ that assigns measure 1 to $M_{n,n}(\mathcal{O}_v)$. We write $d^\times Z = dZ/|\det Z|^n$. Let dg_v be the normalized Haar measure on $GL(n,E_v)$ that assigns measure 1 to $GL(n,\mathcal{O}_v)$. Then $d^\times Z = A(n)\cdot dg_v$, where

$$A(n)=\int_{GL(n,\mathcal{O}_v)} d^\times Z = \prod_{j=1}^{n}(1-q^{-j}) = q^{-n^2}\#GL(n,\mathbb{F}_q)$$

This is just the right hand side of (0.2.2). Thus we may assume that $d^\times Z = L_v(1,\varepsilon_{\mathcal{K}})^{-1}d^\tau g_v$ in the notation of (0.2).

Let χ be the character of $\mathbb{A}_{\mathcal{K}}^\times$ that goes into the definition of our Siegel Eisenstein series. At the place v which splits in $\mathcal{K}$, χ is given by the pair of characters $(\chi_{1v},\chi_{2v}^{-1})$.

For the rest of section (3.3.4) we drop the subscript v from our notation, writing χ_1 for χ_{1v}, etc. On $H(E_v)\simeq GL(2n,E_v)$, the inducing character is

$$\begin{pmatrix} A & * \\ 0 & B \end{pmatrix} \mapsto \chi_1(\det A)\chi_2(\det B)\cdot|\det(AB^{-1})|^{s+\rho},$$

with $\rho=n/2$.

Fix a partition

$$n=n_1+\cdots+n_l$$

Let $P=LU$ be the standard parabolic subgroup of $GL(n)$ corresponding to the above partition. Let $\mathcal{I}\subseteq GL(n,\mathcal{O}_v)$ be the paraholic subgroup corresponding to P. Thus $\mathcal{I}$ consists of matrices $Z = (Z_{ij})$ (written in blocks with respect to the above partition of n), such that

- $Z_{jj} \in GL(n_j, \mathcal{O}_v)$ for $1 \leq j \leq l$.
- Z_{ij} has entries in $\mathcal{O}_v$ for $1 \leq i < j \leq l$.
- Z_{ij} has entries in $\mathfrak{p}_v$ for $i > j$.

Note that $\mathcal{I}$ is an open set in the space $M(n,n)$ of all $n \times n$ matrices with entries in E_v. Consider l characters $\nu = (\nu_1, \cdots, \nu_l)$ of $E_v^\times$. We define our Schwartz function ϕ_ν by the formula

$$\phi_\nu(Z) = \begin{cases} \nu_1(\det Z_{11}) \cdots \nu_l(\det Z_{ll}), & Z \in \mathcal{I} \\ 0, & \text{otherwise} \end{cases} \tag{3.3.4.2}$$

We use the same letter ν to denote the character of $L(\mathcal{O})$ given by

$$\nu(\operatorname{diag}(A_1, \cdots, A_l)) = \nu_1(\det A_1) \cdots \nu_l(\det A_l)$$

It is easy to see that the function ϕ_ν satisfies the relation

$$\phi_\nu(mZ) = \phi_\nu(Zm) = \nu(m)\phi_\nu(Z) \qquad (m \in L(\mathcal{O}), \text{any } Z)$$

Define Fourier transform by

$$\mathcal{F}(\phi)(x) = \int \phi(z)\overline{\psi_v(\operatorname{tr}(z^t x))}dz \tag{3.3.4.3}$$

The function $\mathcal{F}(\phi_\nu)$ satisfies the (obvious) condition

$$\mathcal{F}(\phi_\nu)(mx) = \mathcal{F}(\phi_\nu)(xm) = \nu^{-1}(m)\mathcal{F}(\phi_\nu)(x) \qquad (m \in L(\mathcal{O}), \text{any } x) \tag{3.3.4.4}$$

The explicit formula for $\mathcal{F}(\phi_\nu)$ is given in Part II, Appendix B.

Consider another l-tuple of characters $\mu = (\mu_1, \cdots, \mu_l)$. We can define ϕ_μ as above. Take any integer t which is large enough — say larger than the conductors of all the characters μ_j. Let

$$\Gamma = \Gamma(\mathfrak{p}^t) \subseteq GL(n, \mathcal{O})$$

be the subgroup of $GL(n, \mathcal{O})$ consisting of matrices whose off diagonal blocks are divisible by $\mathfrak{p}^t$.

Note that the restriction of ϕ_μ to $\Gamma(\mathfrak{p}^t)$ is a character. We have

$$\phi_\mu(\gamma x) = \phi_\mu(x\gamma) = \phi_\mu(\gamma)\phi_\mu(x) \qquad (\gamma \in \Gamma(\mathfrak{p}^t), \text{any } x) \tag{3.3.4.5}$$

Define a related function $\tilde{\phi}_\mu$ by

$$\tilde{\phi}_\mu(x) = \begin{cases} \operatorname{Vol}(\Gamma(\mathfrak{p}^t); d^\times Z)^{-1} \cdot \phi_\mu(x), & \text{if } x \in \Gamma(\mathfrak{p}^t) \\ 0, & \text{otherwise} \end{cases}$$

Here $\mathrm{Vol}(\Gamma(\mathfrak{p}^t); d^\times Z)$ is the volume of $\Gamma(\mathfrak{p}^t)$ with respect to the measure $d^\times Z$. We have

$$\mathrm{Vol}(\Gamma(\mathfrak{p}^t); d^\times Z)^{-1} = A(n)^{-1}[GL(n,\mathcal{O}) : \Gamma(\mathfrak{p}^t)] = (\prod_{j=1}^{l} A(n_j)^{-1})(\prod_{1\leq i<j\leq l} q^{2tn_in_j})$$

Later on, we shall identify various spaces with $M_{n,n}$, and ϕ_μ, etc, will be viewed as a function on these spaces.
We define a Schwartz function Φ_1 on $M(n,n)$ by

$$\Phi_1(u,v) = \tilde{\phi}_\mu(\frac{u-v}{2}) \cdot \mathcal{F}(\phi_\nu)(u+v) \tag{3.3.4.6}$$

Recall that we have identified $U(2V)(E_v)$ with $GL(2n, E_v)$. Thus it acts on $M(n,2n)$ by right multiplications. We take a global section

$$f(h;\chi,s) = \otimes f_u(h;\chi,s) \in \mathrm{Ind}(\chi|\cdot|^s)$$

with u running through all places of E. At the place v we choose the local section by the following formula:

$$f_v(h;\chi,s) = f_{v,\mu}(h;\chi,s) \overset{def}{=} \chi_1(\det h)\cdot|\det h|^{s+\rho} \tag{3.3.4.7}$$

$$\cdot \int_{GL(n,E_v)} \Phi_1((Z,Z)h)\chi_1\chi_2^{-1}(\det Z)|\det Z|^{2(s+\rho)} d^\times Z.$$

Recall that we have the decomposition

$$2V = V^d \oplus V_d$$

of the doubled space $2V$ into totally isotropic subspaces. We now define a Weyl element w_n that interchanges the two summands above. To make it precise wewrite matrices in blocks corresponding to the decomposition

$$2V = V \oplus (-V)$$

Then we take

$$w = w_n = \begin{pmatrix} 1_n & 0 \\ 0 & -1_n \end{pmatrix}$$

For each index j with $1 \leq j \leq n$ we also define

$$w_j = \begin{pmatrix} 1_j & 0 & 0 & 0 \\ 0 & 1_{n-j} & 0 & 0 \\ 0 & 0 & -1_j & 0 \\ 0 & 0 & 0 & 1_{n-j} \end{pmatrix}$$

(Really, 1_n is the identity on V. But the definition of 1_j for $0 < j < n$ implies an implicit choice of an orthogonal basis for V).

(3.3.4.8) Lemma. *Let $P = P^d$ be the stabilizer of V^d in $U(2V)$. Then as a function of h the local section $f_v(h; \chi, s)$ is supported on the "big cell" $P(E_v)w_nP(E_v)$.*

Proof. We know that $U(2V)$ is the disjoint union of the double cosets Pw_jP. Since f_v is a section, it suffices to show that

$$f_v(w_jp; \chi, s) = 0, \qquad \text{for any } p \in P(E_v),\ j < n$$

As remarked above, the definition of w_j involves an implicit choice of a basis, and therefore a decomposition

$$V = V_j \oplus V^j$$

where V_j is of dimension j. Recall that $U(2V)(E_v) \simeq GL(2n, E_v)$. Under this identification, a typical element of $P(E_v)$, written in blocks with respect to the decomposition $2V = V \oplus -V$, is of the form

$$p = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where A, B, C, D are $n \times n$ matrices, and

$$A + C = B + D$$

In accordance with the decomposition $V = V_j \oplus V^j$, we may write an $n \times n$ matrix as $Z = (X, Y)$ where X is $n \times j$ and Y is $n \times (n - j)$. Then we find

$$(Z, Z)w_jp = (u, v)$$

with

$$u = (X, Y)A + (-X, Y)C, \qquad v = ((X, Y)B + (-X, Y)D$$

Consequently

$$u - v = (X, 0)(A + D - B - C)$$

(Here we have used the condition $A + C = B + D$). The right hand side is a singular matrix unless $j = n$. Since

$$\Phi_1(u, v) = \tilde{\phi}_\mu(\frac{u - v}{2})\mathcal{F}(\phi_\nu)(u + v)$$

and $\tilde{\phi}_\mu$ is supported on invertible matrices, we find

$$\Phi_1((Z, Z)w_jp) = 0 \qquad \text{for all } Z$$

if $j < n$. Hence $f_v(w_jp; \chi, s) = 0$ for $j < n$ and $p \in P(E_v)$.

We define the Eisenstein series $E^f(h;\chi,s) = E^{f_\mu}(h;\chi,s)$ and its Fourier coefficients as before. Let $P = MN$ be a Levi decomposition. We assume that M is normalized by w. We will calculate the v-component of $E^f_\beta(h;\chi,s)$ under the condition that $h_v \in P(E_v)$. In view of the above lemma and Remark 3.2.2.3, we know that the factorization (3.2.2.2) is valid for any β (full rank or otherwise), provided $h_v \in P(E_v)$. However, in (3.3.4.9) we will see that our choice of local data at primes dividing p forces $E^f_\beta(h,\chi,s) = 0$ for $\mathrm{rank}(\beta) < n$, provided $h_v \in P(E_v)$ for at least one place v dividing p.
For the remainder of this section we shall calculate

$$W_{\beta,v}(h_v,f_v,s) = \int_{N(E_v)} f_v(wn_vh_v;\chi_v,s)\psi_{-\beta}(n_v)dn_v$$

The group N can be identified with the space Herm_n of $n \times n$ hermitian matrices. We write this isomorphism as

$$\mathrm{Herm}_n \longrightarrow N, \qquad R \mapsto n(R)$$

If $R \in \mathrm{Herm}_n(\mathbf{A})$ then

$$\psi_\beta(n(R)) = \psi(\mathrm{tr}(\beta^t R))$$

where tr denotes trace of the matrix, followed by $\mathrm{tr}_{\mathcal{K}/E}$. We need to explain what this means at the split place v. We have the isomorphism

$$\mathcal{K} \otimes E_v \simeq E_v \oplus E_v$$

where the first summand E_v is identified with $\mathcal{K}_w$, with w the place of $\mathcal{K}$ dividing v, such that $w \in \Sigma_p$. The second summand is then identified with $\mathcal{K}_{w^c}$. Also, on the right hand side the trace map is identified with the summation of the two coordinates. This gives rise to

$$2V \otimes E_v = (2V)_1 \oplus (2V)_2$$

etc. Now any $R \in \mathrm{Herm}_n(E_v)$ is identified with an arbitrary $n \times n$ matrix with coefficients in E_v, as follows. We consider

$$M_{n,n}(\mathcal{K}) \subset M_{n,n}(\mathcal{K}_w) = M_{n,n}(E_v)$$

Then the embedding

$$M_{n,n}(\mathcal{K}) \longrightarrow M_{n,n}(E_v) \oplus M_{n,n}(E_v), \qquad \gamma \mapsto (\gamma, \bar{\gamma})$$

extends to an isomorphism

$$M_{n,n}(\mathcal{K}) \otimes E_v \longrightarrow M_{n,n}(E_v) \oplus M_{n,n}(E_v)$$

Since $\bar{\gamma} = {}^t\gamma$ for $\gamma \in \mathrm{Herm}_n(E)$, we see that the image of

$$\mathrm{Herm}_n(E_v) = \mathrm{Herm}_n(E) \otimes E_v \subset M_{n,n}(\mathcal{K}) \otimes E_v$$

under the above isomorphism is precisely

$$\{(R, {}^tR) \mid R \in M_{n,n}(E_v)\}$$

Thus we get the identification $\mathrm{Herm}_n(E_v) = M_{n,n}(E_v)$ by the map $(R, {}^tR) \mapsto R$.

Now if a matrix $R \in M_{n,n}(E_v)$ is identified with an element of $\mathrm{Herm}_n(E_v)$ as above then a simple calculation gives

$$\psi_\beta(n(R)) = \psi(2 \cdot \mathrm{tr}_E(\beta^t R))$$

This time, on the right hand side $\mathrm{tr}_E(\beta^t R)$ is the trace of $\beta^t R$ viewed as a matrix with coefficients in E_v.

We may assume $h_v \in M(E_v)$. Then h_v preserves both the diagonal and the anti-diagonal. So there are $n \times n$ invertible matrices A and B such that

$$(Z, -Z)h_v = (ZA, -ZA), \qquad (Z, Z)h_v = (ZB, ZB)$$

for any Z. Suppose $n = n(R)$. A simple calculation gives

$$(Z, Z)wnh_v = (Z(RB + A), Z(RB - A))$$

Recalling the definition of Φ_1 we obtain

$$\Phi_1((Z, Z)wnh_v) = \tilde{\phi}_\mu(ZA)\mathcal{F}(\phi_\nu)(2ZRB) \tag{3.3.4.9}$$

We already know that f_v is supported on the big cell. In the integral expression for f_v given by (3.3.4.7) we may translate the variable Z by any element of $L(\mathcal{O})$ and then integrate over $L(\mathcal{O}) \subseteq GL(n, E_v)$. By formula (3.3.4.9) and the transformation properties of ϕ_μ and $\mathcal{F}(\phi_\nu)$ given by (3.3.4.4)-(3.3.4.5), we see immediately that f_v would be identically 0 unless the following conditions are satisfied:

$$\mu_j = \nu_j \chi_2 \chi_1^{-1} \text{ on } \mathcal{O}_v^\times, \quad \text{for } 1 \leq j \leq l \tag{3.3.4.10}$$

We assume this from now on. Then

$$f_v(wnh_v; \chi, s) = \chi_1(\det B)\chi_2(\det A)|\det BA^{-1}|^{s+\rho}\mathcal{F}(\phi_\nu)(2A^{-1}RB)$$

By Fourier inversion we obtain

(3.3.4.11) Lemma. *For $h_v \in M(E_v)$ as above, the v-component of the β-th Fourier coefficient $E^f_\beta(h,\chi,s) = E^{f_\mu}_\beta(h,\chi,s)$ is given by*
(3.3.4.12)

$$W_{\beta,v}(h_v,f_v,s) = \chi_1(\det B)\chi_2(\det A)|\det AB^{-1}|^{-s+\rho}\phi_\nu({}^tA\beta{}^tB^{-1}),$$

where ν is defined in terms of μ and χ by (3.3.4.10).
In particular, the β-th Fourier coefficient vanishes unless β is of full rank.

The last assertion of the lemma follows from the fact that ϕ_ν is supported on $\mathcal{I}$.

(3.3.5) *Summary.*

Recall that $m = n + 2s_0$. Define

$$C_\infty(n,m,\mathcal{K}) = \prod_{v\in\Sigma}(\gimel_v)^{-mn+n^2}\cdot\left(\frac{(-i)^{-n^2}2^{n(m-n+1)}\pi^{mn-n(n-1)/2}}{\prod_{j=1}^n(m-j)!}\right)^{[E:\mathbb{Q}]},$$

$$C^S(n,m,\mathcal{K}) = c(n,E,\mathcal{K})\prod_{j=0}^{n-1}L^S(m+j,\chi\varepsilon^j)^{-1}C_\infty(n,m,\mathcal{K}); \tag{3.3.5.1}$$

We choose a global section

$$f = f_\mu(h,\chi,s) = \bigotimes_{v\notin S}f^{unr}_v\otimes\bigotimes_{v\in S_\infty}f_v\otimes\bigotimes_{v\in S^p_f}f_{u_v}\otimes_{v|p}f_v(h;\chi,s) \tag{3.3.5.2}$$

in accordance with the preceding sections. The functions f_v for $v \mid \infty$, resp. $v \mid p$, are defined by (3.3.3.1), resp. (3.3.4.7), the characters μ_j being determined by ν_j and χ by (3.3.4.10). Finally, for $v \notin S$, f^{unr}_v is the unramified vector in $I(s,\chi)$ normalized to take value 1 at 1.
Let

$$\mathbb{E}(h,\chi,m,f) = \mathbb{E}(h,\chi,m,f_\mu) \overset{def}{=} C^S(n,\mathcal{K})^{-1}E^f(h,\chi,s_0).$$

We define the factor $T^0(\beta,m(A),s_0)$ by (3.2.2.10). When $h = m(A) \in M(\mathbf{A}_f)$, we write $m(A) = m(A^p)\cdot\prod_{v|p}h_v$, and let A_v be the local component of A at v for v prime to p. The preceding calculations show that the β-Fourier coefficient of $\mathbb{E}(m(A),\chi,m,f)$ equals zero if $rank(\beta) < n$. Otherwise, the Fourier coefficient is given by the following formula, in which χ has been replaced by the (motivic) Hecke character $\chi^* = \chi\cdot N^{\kappa/2}_{\mathcal{K}/E}$ and where for split v in S^p_f we write $\chi^*_v(\det(A_v))$ as an abbreviation for $\chi^*_v(\det(\mathbf{A}_v\cdot\mathbf{B}_v^{-1})$ as in (3.3.2):

$$\begin{aligned}\mathbb{E}_\beta(m(A),\chi,m,f) &= \mathbb{E}_\beta(m(A),\chi,m,f_\mu) = \\ &= T^0(\beta,m(A),s_0)\det(\beta)^{(m-n)[E:\mathbb{Q}]}|\det A|_{\mathbf{A}}^{\frac{n-\kappa}{2}-s_0}\times \\ &\quad\times\prod_{v\in\Sigma_p}\chi^*_1(\det B(h_v))\chi^*_2(\det A(h_v))\phi_\nu({}^tA(h_v)\beta B(h_v)^{-1})\times \\ &\quad\times\prod_{v\in S^p_f}\chi^*_v(\det(A_v))\hat{u}_v({}^t\bar{A}_v\beta A_v)\end{aligned} \tag{3.3.5.3}$$

We have dropped the term q^β of (1.5.6). The complete arithmetic Fourier expansion is

(3.3.5.4)
$$\mathbb{E}(h_\infty m(A),\chi,m,f) = \mathbb{E}(h_\infty m(A),\chi,m,f_\mu) = \sum_\beta \mathbb{E}_\beta(m(A),\chi,m,f)q^\beta$$

with $m(A)\in M(\mathbf{A}_f)$ as before.

Remarks

(3.3.5.5) By (3.1.4.4) the exponent in the absolute value factor $|\det A|_{\mathbf{A}}^{\frac{n-\kappa}{2}-s_0}$ is an integer. Thus these factors are always integers, and in fact are p-units under our standing hypothesis that $A(h_v)$ and $B(h_v)$ are in $GL(n,\mathcal{O}_v)$ for all v dividing p. Similarly, since $m\geq n$, the factor $\det(\beta)^{m-n}$ is p-adically integral provided β is, and this is guaranteed by our hypothesis on $A(h_v)$ and $B(h_v)$ and the definition of $T^0(\beta,m(A))$.

(3.3.5.6) With u_v chosen as in (3.3.1) and (3.3.2) at places in S_f^p, the coefficients are then p-adic integers, and in fact are p-adic units where they are non-zero. Better control of the local theta correspondence at places in S will require different choices of f_v at S_f^p.

(3.3.5.7) In applications to the zeta function we will want to work with finite sums of Siegel-Weil Eisenstein series attached to hermitian spaces V' that differ locally at non-split primes in S, since at such primes we are forced to take the local sections denoted $\tilde{f}_v$ of (3.3.1.2), which are not generally Siegel-Weil sections. These Fourier coefficients of these sums remain p-adically integral and since the different V' represent different β, they are also p-adically primitive.

(3.4) Review of abstract p-adic distributions and measures.

Let T be a torus over $\mathbb{Z}_p$, and let R be a complete $\mathbb{Z}_p$-algebra, assumed $\mathbb{Z}_p$-flat and compact, $R[\frac{1}{p}] = R\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$. For instance, we can take $R=\mathcal{O}_{\mathbb{C}_p}$, so that $R[\frac{1}{p}]=\mathbb{C}_p$. Let $\mathcal{B}$ denote an $R[\frac{1}{p}]$-Banach space, $\mathcal{M}\subset\mathcal{B}$ the unit ball of elements of norm ≤ 1. If $A = R, R[\frac{1}{p}]$, $\mathcal{B}$, or $\mathcal{M}$, let $C(T(\mathbb{Z}_p),A)$ denote the R-module of continuous A-valued functions on $T(\mathbb{Z}_p)$. Since $T(\mathbb{Z}_p)$ is compact, $C(T(\mathbb{Z}_p),\mathcal{B}) = C(T(\mathbb{Z}_p),\mathcal{M})\otimes_R R[\frac{1}{p}])$, and this is true in particular for $\mathcal{M}=R$ itself. The sup norm makes $C(T(\mathbb{Z}_p, R[\frac{1}{p}]$ into an $R[\frac{1}{p}]$-Banach space. The locally constant functions in $C(T(\mathbb{Z}_p),A)$ are denoted $C^\infty(T(\mathbb{Z}_p),A)$.

A *p-adic distribution* on $T(\mathbb{Z}_p)$ with values in an $R[\frac{1}{p}]$-vector space $\mathcal{V}$ is a homomorphism of R-modules
$$\lambda : C^\infty(T(\mathbb{Z}_p,R)\to\mathcal{V}.$$
To define a distribution $\mathcal{V}$ need not be a Banach space. A $\mathcal{B}$-valued *p-adic measure* on $T(\mathbb{Z}_p)$ is a continuous homomorphism of $R[\frac{1}{p}]$-Banach spaces
$$\mu : C(T(\mathbb{Z}_p),R[\frac{1}{p}])\to\mathcal{B}.$$

Let $X_{fin}(T)$ denote the set of characters of finite order of $T(\mathbb{Z}_p)$, viewed as a subset of $C^\infty(T(\mathbb{Z}_p), R)$ for any sufficiently large p-adic ring R, e.g. $R = \mathcal{O}_{\mathbb{C}_p}$. The set $X_{fin}(T)$ forms a *basis* for the $R[\frac{1}{p}]$-vector space $C^\infty(T(\mathbb{Z}_p), R[\frac{1}{p}])$, hence any function $\chi \mapsto v_\chi$ from $X_{fin}(T)$ to $\mathcal{V}$ determines a $\mathcal{V}$-valued distribution on $T(\mathbb{Z}_p)$ by linearity.

(3.4.1) Lemma. *Let $\chi \mapsto m_\chi$ be a function from $X_{fin}(T)$ to $\mathcal{M}$, and let $\lambda(m)$ denote the corresponding $\mathcal{B}$-valued distribution. Then $\lambda(m)$ extends to a p-adic measure if and only if, for every integer n and for any finite sum $\sum_j \alpha_j\chi_j$ with $\alpha_j \in R[\frac{1}{p}]$ and $\chi_j \in X_{fin}(T)$ such that $\sum_j \alpha_j\chi_j(t) \in p^nR$ for all $t \in T(\mathbb{Z}_p)$, we have*

$$\sum_j \alpha_j m_{\chi_j} \in p^n\mathcal{M}. \tag{3.4.2}$$

This is a version of the abstract Kummer congruences stated as Proposition 5.0.6 of [K].

(3.4.3) Corollary. *In Lemma (3.4.1) above, it actually suffices to check (3.4.2) with $n = 0$.*

Indeed, the the condition for n=0 implies the condition for general n: a bounded distribution is a measure.

In the next section we will be constructing measures with values in the Banach space of p-adic modular forms on the Shimura variety $Sh(2V)$. Let $R = \mathcal{O}_{\mathbb{C}_p}$, so that $R[\frac{1}{p}] = \mathbb{C}_p$. Let $\mathcal{V}$ denote the algebra of p-adic modular forms, as in (2.2.9), and let $\mathcal{B} = \mathcal{V} \otimes_{\mathcal{O}_{\mathbb{C}_p}} \mathbb{C}_p$. Let $\mathcal{M}$ denote the right-hand side $\hat{\bigoplus}_{\alpha\in U^*} H^0({}_{K_P(\infty)}S(G_P, X_P), \mathcal{O}_{\mathbb{S}_P})$ of (2.3.2), and let $\mathcal{Q} = \mathcal{M} \otimes_{\mathcal{O}_{\mathbb{C}_p}} \mathbb{C}_p$. The $\mathbb{C}_p$-vector space $\mathcal{B}$ is a Banach space via the sup norm, whereas $\mathcal{Q}$ can be viewed as a ring of formal series over the Banach space $H^0({}_{K_P(\infty)}S(G_P, X_P), \mathcal{O}_{\mathbb{S}_P})$, hence again becomes a Banach space via the sup norm. The q-expansion map $F.J.^P$ (2.3.2) is a continuous homomorphism of Banach spaces.

The following proposition follows from the q-expansion principle, as in [DR] or [K], and represents the primary application of the q-expansion principle to our project:

(3.4.4) Proposition. *Let T be a torus over $\mathbb{Z}_p$, and let μ be a p-adic measure on $T(\mathbb{Z}_p)$ with values in $\mathcal{Q}$. Suppose that $\mu(\chi) = \int_{T(\mathbb{Z}_p)} \chi d\mu$ lies in the image of $F.J.^P$ for all $\chi \in X_{fin}(T)$. Then μ is the image, under $F.J.^P$, of a measure with values in $\mathcal{B}$.*

(3.5) Construction of Eisenstein measures.

Let ℓ be a positive integer and let $T(\ell)^0$ denote the torus over $\mathbb{Z}_p$ given by $(R_{\mathcal{O}_E/\mathbb{Z}_p}\mathbb{G}_{m,\mathcal{O}_E})^\ell$. Thus $T(\ell)^0(\mathbb{Z}_p)$ is canonically isomorphic to $\prod_{w|p} \mathcal{O}_w^{\times,\ell}$, where w runs through places of E. This can also be identified with the product of ℓ copies of $\prod_{v\in\Sigma_p} \mathcal{O}_v^\times$, where now v are places of $\mathcal{K}$. The latter form will be the most useful for us. For brevity we write $\mathcal{O}^\times_{\Sigma_p}$ for $\prod_{v\in\Sigma_p}\mathcal{O}^\times_v$. We let

$$T(\ell) = T(\ell)^0 \times (R_{\mathcal{O}_\mathcal{K}/\mathbb{Z}_p}\mathbb{G}_{m,\mathcal{O}_\mathcal{K}}).$$

Then the set $X_{fin}(T(\ell))$ of finite order characters of $T(\ell)$ can be parametrized by $(\ell+1)$-tuples $(\nu_1,\dots,\nu_\ell,\chi)$, where each ν_i is a character of finite order of $\mathcal{O}^\times_{\Sigma_p}$, and χ is a character of finite order of $\prod_{v|p}\mathcal{O}^\times_v$ where now v runs over all places of $\mathcal{K}$ dividing p. We will further write $\chi = (\chi_1,\chi_2)$, where χ_1 is the restriction of χ to $\prod_{v\in\Sigma_p}\mathcal{O}^\times_v$ and χ_2 is a second character of the same group $\prod_{v\in\Sigma_p}\mathcal{O}^\times_v$ obtained by restricting χ^{-1} to $\prod_{v\in c\Sigma_p}\mathcal{O}^\times_v$ and then composing with c. So in the end, $X_{fin}(T)$ can be viewed as the set of $(\ell+2)$-tuples of characters of $\mathcal{O}^\times_{\Sigma_p}$. The character χ will in practice be the restriction to $\mathcal{O}^\times_{\mathcal{K},p}$ of a character of $\mathcal{K}^\times_p = \prod_{v|p}\mathcal{K}^\times_v$, which in turn will most commonly be the p-adic component of a global Hecke character.
We introduce additional notation: for $j = 1,\dots,\ell$, we let $\mu_j = \nu_j\cdot\chi_2\cdot\chi_1^{-1}$. Let m, n, and s_0 be as in (3.3.5). Let $n = n_1+\cdots+n_\ell$ be a partition of n and Q the corresponding standard parabolic subgroup of $GL(n)$.

(3.5.1) THEOREM. *There is a $\mathcal{B}$-valued measure λ^m_Q on $T(\ell)$ with the property that, for any $\ell+2$-tuple $(\mu,\chi) = (\mu_1,\dots,\mu_\ell,\chi_1,\chi_2)$ of characters of finite order of $\mathcal{O}^\times_{\Sigma_p}$.*

$$F.J.^P \circ \int_{T(\ell)} (\mu_1,\dots,\mu_\ell,\chi)d\lambda^m_Q = \mathbb{E}(\bullet,\chi,m,f_\mu) \tag{3.5.2}$$

where the right hand side is the q-expansion of (3.3.5.4).

Proof. The right-hand side of (3.5.2) defines the value at (μ,χ) of a $\mathcal{Q}$-valued distribution on $T(t)$. To show that this distribution is in fact a $\mathcal{Q}$-valued p-adic measure, it suffices, by Corollary (3.4.3), to show that the right-hand side of (3.5.2) satisfies the abstract Kummer congruences (3.4.2) for $n = 0$. In other words, for any $\beta \in U^*\cap C$, the Fourier coefficients $\mathbb{E}_\beta(m(A),\chi,m,f_\mu)$ as (ν,χ) vary, satisfy the abstract Kummer congruences as functions of $m(A) \in L_P(\mathbf{A}_f)$, with the coefficients $A_v \in GL(n,\mathcal{O}_v)$ for $v \mid p$. Bearing in mind the relation (3.3.4.10) between ν and μ, this follows immediately from (3.3.5.3) and Remarks (3.3.5.5) and (3.3.5.6).
Now the theorem follows from Proposition 3.4.4 and from the fact that $\mathbb{E}(\bullet,\chi,m,f_\mu)$ is a classical modular form for $(\mu,\chi) \in X_{fin}(T(\ell))$.

REFERENCES

[BS] S. Böcherer, C.-G. Schmidt, p-adic measures attached to Siegel modular forms, *Ann. Inst. Fourier*, 50 (2000) 1375-1443.

[Ch] C.-L. Chai, Methods for p-adic monodromy, manuscript (2006).

[Co] J. Coates, Motivic p-adic L-functions, in J. Coates and M. J. Taylor, eds., *L-functions and Arithmetic* London Mathematical Society Lecture Note Series, 153 Cambridge: Cambridge University Press (1991), 141-172.

[D] P. Deligne, Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques, in *Automorphic forms, representations and L-functions*, *Proc. Symp. Pure Math.*, 33, Part 2, (1979) 247–289.

[DR] P. Deligne and K. Ribet, Values of Abelian L-functions at negative integers over totally real fields, *Inv. Math.*, 59, (1980), 227-286.

[F] K. Fujiwara, Arithmetic compactifications of Shimura varieties (I), unpublished manuscript (1992).

[G] P. Garrett, Archimedean zeta integrals for unitary groups, (handwritten notes 1991-1992; revised manuscript, July 19, 2005).

[H1] M. Harris, Arithmetic vector bundles and automorphic forms on Shimura varieties: I, *Invent. Math.*, 82 (1985)-151-189; II. *Compositio Math.*, 60 (1986), 323-378.

[H2] M. Harris, L-functions of 2 by 2 unitary groups and factorization of periods of Hilbert modular forms. *JAMS*, 6 (1993), 637-719.

[H3] M. Harris, L-functions and periods of polarized regular motives, *J.Reine Angew. Math.*, 483, (1997) 75-161.

[H4] M. Harris, Cohomological automorphic forms on unitary groups, I: rationality of the theta correspondence, *Proc. Symp. Pure Math*, 66.2, (1999) 103-200.

[H5] M. Harris, Cohomological automorphic forms on unitary groups, II: in preparation.

[HK] M. Harris, S. Kudla, On a conjecture of Jacquet, in H. Hida, D. Ramakrishnan, F. Shahidi, eds., *Contributions to automorphic forms, geometry, and number theory* (volume in honor of J. Shalika), 355-371 (2004)

[HKS] M. Harris, S. Kudla, W. J. Sweet, Theta dichotomy for unitary groups, *JAMS*, 9 (1996) 941-1004.

[HL] M. Harris and J.-P. Labesse, Conditional base change for unitary groups, *Asian J. Math.* (2005).

[HLS] M. Harris, J.-S. Li, C. Skinner, The Rallis inner product formula and p-adic L-functions, volume in honor of S. Rallis, in press.

[Hi02] H. Hida, Control theorems of coherent sheaves on Shimura varieties of PEL type, *J. Inst. Math. Jussieu*, 1 (2002) 1-76.

[Hi04] H. Hida, *p-adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics (2004).

[Hi05] H. Hida, p-adic automorphic forms on reductive groups, Notes of a course at the IHP in 2000, *Astérisque*, 296 (2005) 147-254.

[Hi06] H. Hida, Irreducibility of the Igusa tower, manuscript of August 30, 2006, available at http://www.math.ucla.edu/ hida/Ig.pdf.

[K] N. Katz, p-adic L-functions for CM fields, *Invent. Math.*, 49 (1978) 199-297.

[Ko] R. Kottwitz, , Points on some Shimura varieties over finite fields, *Jour. of the AMS* 5 (1992) 373-444.

[KR] S. S. Kudla, S. Rallis, Poles of Eisenstein series and L-functions, in Festschrift in Honor of I. I. Piatetski-Shapiro (Part II), *Israel Math. Conf. Proceedings*, 3 (1990) 81-110.

[L1] J.-S. Li, Theta liftings for unitary representations with non-zero cohomology, *Duke Math. J.*, 61 (1990) 913-937.

[L2] J.-S. Li, Non-vanishing theorems for the cohomology of certain arithmetic quotients, *J. reine angew. Math.*, 428 (1992) 177-217.

[Pa] A. A. Panchishkin, Admissible non-archimedean standard zeta functions associated with Siegel modular forms, in *Motives*, Proc. Symp. Pure Math., 55 (1994), Part 2, pp. 251-292.

[PSR] I. I. Piatetski-Shapiro, S. Rallis, L-functions for the classical groups, in S. Gelbart, I. Piatetski-Shapiro, and S. Rallis, Explicit constructions of automorphic L-functions, *Lecture Notes in Math.*, 1254 (1987).

[P] R. Pink, Arithmetical compactification of mixed Shimura varieties *Bonner Math. Schriften*, 209 (1990).

[Pr] K. Prasanna, Integrality of a ratio of Petersson norms and level-lowering congruences, *Annals of Math.*, in press.

[RZ] M. Rapoport and T. Zink: *Period Spaces for p-divisible Groups*, Princeton: Annals of Mathematics Studies 141 (1996).

[S82] G. Shimura, Confluent hypergeometric functions on tube domains, Math. Ann. 260 (1982) 269-302.

[S97] G. Shimura, Euler products and Eisenstein series, *CBMS Regional Conference Series in Mathematics*, 93, Providence, R.I.: American Mathematical Society (1997).

[S00] G. Shimura, Arithmeticity in the theory of automorphic forms, *Mathematical Series and Monographs*, 82, Providence, R.I.: American Mathematical Society (2000).

[SU] C. Skinner and E. Urban, to appear

[T] V. Tan, Poles of Siegel Eisenstein series on $U(n,n)$, *Can. J. Math.*, 51 (1999) 164-175.

[Tate] J. Tate, *Fourier analysis in number fields and Hecke's Zeta-functions* in Algebraic number theory J. W. S. Cassels and A Fröhlich, eds, Academic Press, (1967) 305-347.

[Wed] T. Wedhorn, Congruence Relations on some Shimura varieties *J. f.d. reine und angew. Math.*, 524, (2000), 43–71.

Michael Harris
UFR de Mathématiques
Université Paris 7
2 Pl. Jussieu 75251
Paris cedex 05
FRANCE
harris@math.jussieu.fr

Jian-Shu Li
Department of Mathematics
HKUST and Zhejiang University
Clear Water Bay
Hong Kong
matom@ust.hk

Christopher M. Skinner
Department of Mathematics
Princeton University
Princeton, NJ
USA
cmcls@Math.Princeton.EDU

Anticyclotomic Main Conjectures

To John Coates

Haruzo Hida[1]

Received: August 3, 2005
Revised: May 16, 2006

Abstract. In this paper, we prove many cases of the anticyclotomic main conjecture for general CM fields with p-ordinary CM type.

2000 Mathematics Subject Classification: 11F27, 11F30, 11F33, 11F41, 11F60, 11F80, 11G10, 11G15, 11G18, 11R23, 11R34, 11R42
Keywords and Phrases: Eisenstein series, Main conjecture, CM field, CM abelian variety, Shimura series, Basis problem

Contents

[1] The author is partially supported by the NSF grant: DMS 0244401 and DMS 0456252.

1. Introduction

Iwasawa's theory for elliptic curves with complex multiplication was initiated by J. Coates in the 1970s in a series of papers (for example, [CW] and [CW1]), and it is now well developed (by the effort of a handful of number-theorists) into a solid theory for abelian varieties of CM type (or one may call it Iwasawa's theory for CM fields). In this paper, we prove many cases of the anticyclotomic main conjecture for general CM fields with p-ordinary CM type.

Let M be a CM field with maximal real subfield F. The field F is totally real, and M is a totally imaginary quadratic extension of F (inside a fixed algebraic closure $\overline{F}$ of F). We fix a prime $p > 3$ *unramified* in $M/\mathbb{Q}$. We assume to have a p–ordinary CM type Σ of M. Thus, fixing an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, the embeddings $i_p \circ \sigma$ for $\sigma \in \Sigma$ induce exactly a half Σ_p of the p–adic places of M. We identify Σ_p with a subset of prime factors of p in M. For the generator c of $\mathrm{Gal}(M/F)$, the disjoint union $\Sigma_p \sqcup \Sigma_p^c$ gives the total set of prime factors of p in M. For a multi-index $e = \sum_{\mathfrak{P}|p} e(\mathfrak{P})\mathfrak{P} \in \mathbb{Z}[\Sigma_p \sqcup \Sigma_p^c]$, we write $\mathfrak{P}^e$ for $\prod_{\mathfrak{P}|p} \mathfrak{P}^{e(\mathfrak{P})}$. We choose a complete discrete valuation ring W inside $\overline{\mathbb{Q}}_p$ finite flat and unramified over $\mathbb{Z}_p$. A Hecke character $\psi : M^\times\backslash M_{\mathbb{A}}^\times \to \mathbb{C}^\times$ is called *anticyclotomic* if $\psi(x^c) = \psi(x)^{-1}$. We call ψ has *split* conductor if the conductor of ψ is divisible only by primes split in M/F. We fix a continuous anticyclotomic character $\psi : \mathrm{Gal}(\overline{F}/M) \to W^\times$ of finite order. It is an easy consequence of class field theory(see (7.18) and [HMI] Lemma 5.31) that we can always find another Hecke character $\varphi : M_{\mathbb{A}}^\times/M^\times M_\infty^\times \to \mathbb{C}^\times$ such that $\psi(x) = \varphi^-(x) = \varphi^{-1}(x)\varphi(x^c)$. Regarding φ and ψ as Galois characters, this is equivalent to $\psi(\sigma) = \varphi^{-1}(\sigma)\varphi(c\sigma c^{-1})$ for any complex conjugation c in $\mathrm{Gal}(\overline{F}/F)$. We assume the following four conditions:

(1) *The character ψ has order prime to p with exact conductor $\mathfrak{c}\mathfrak{P}^e$ for $\mathfrak{c}$ prime to p.*
(2) *The conductor $\mathfrak{c}$ is a product of primes split in M/F.*
(3) *The local character $\psi_{\mathfrak{P}}$ is non-trivial for all $\mathfrak{P} \in \Sigma_p$.*
(4) *The restriction ψ^* of ψ to $\mathrm{Gal}(\overline{F}/M[\sqrt{p^*}])$ for $p^* = (-1)^{(p-1)/2}p$ is non-trivial.*

We study arithmetic of the unique $\mathbb{Z}_p^{[F:\mathbb{Q}]}$–extension M_∞^- of M (unramified outside p and ∞) on which $c\sigma c^{-1} = \sigma^{-1}$ for all $\sigma \in \Gamma_M^- = \mathrm{Gal}(M_\infty^-/M)$. The extension M_∞^-/M is called the anticyclotomic tower over M. Let $M(\psi)/M$ be the class field with ψ inducing the isomorphism $\mathrm{Gal}(M(\psi)/M) \cong \mathrm{Im}(\psi)$. Let $L_\infty/M_\infty^- M(\psi)$ be the maximal p–abelian extension unramified outside Σ_p. Each $\gamma \in \mathrm{Gal}(L_\infty/M)$ acts on the normal subgroup $X = \mathrm{Gal}(L_\infty/M_\infty^- M(\psi))$ continuously by conjugation, and by the commutativity of X, this action factors through $\mathrm{Gal}(M(\psi)M_\infty^-/M)$. We have a canonical splitting $\mathrm{Gal}(M(\psi)M_\infty^-/M) = \Gamma_M^- \times G_{tor}(\psi)$ for the maximal torsion subgroup $G_{tor}(\psi) \cong \mathrm{Im}(\psi)$. Since ψ is of order prime to p, it factors through the maximal torsion subgroup $G_{tor}(\psi)$. Then we look into the Γ_M^-–module: $X[\psi] = X \otimes_{\mathbb{Z}_p[G_{tor}(\psi)],\psi} W$.

As is well known, $X[\psi]$ is a $W[[\Gamma_M^-]]$–module of finite type, and it is a torsion module by a result of Fujiwara (cf. [H00] Corollary 5.4 and [HMI] Theorem 5.33) generalizing the fundamental work of Wiles [W] and Taylor-Wiles [TW]. Thus we can think of the characteristic element $\mathcal{F}^-(\psi) \in W[[\Gamma_M^-]]$ of the module $X[\psi]$. As we have seen in [HT1] and [HT2], we have the anticyclotomic p–adic Hecke L–function $L_p^-(\psi) \in \overline{W}[[\Gamma_M^-]]$ (constructed by Katz), where $\overline{W}$ is the completed p–adic integer ring of the maximal unramified extension of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}}_p$. We regard $W \subset \overline{W}$. Then we prove

Theorem. *We have the identity:* $\mathcal{F}^-(\psi) = L_p^-(\psi)$ *up to a unit in* $\overline{W}[[\Gamma_M^-]]$.

The condition $p > 3$ is necessary because at one point we need to choose a prime ideal $\mathfrak{q}$ of F with $N_{F/\mathbb{Q}}(\mathfrak{q}) \not\equiv \pm 1 \mod p$. By implementing our idea more carefully, we might be able to include the prime $p = 3$, but there is no hope (without a new idea) of including $p = 2$. The condition (1) is probably inessential, and it could be avoided by using the nearly ordinary Galois deformation with fixed p–power order nearly ordinary characters instead of the minimal one we used, although some of our argument has to be done more carefully to incorporate p–power order characters. In such a generalization, we probably need to assume (2-4) replacing ψ by the Teichmüller lift of $\psi \mod \mathfrak{m}_W$ for the maximal ideal $\mathfrak{m}_W$ of W. The condition (2) is imposed to guarantee the local representation at the prime $\mathfrak{l}$ given by $\mathrm{Ind}_{M_\mathfrak{l}}^{F_\mathfrak{l}} \varphi_\mathfrak{l}$ is reducible; otherwise, we possibly need to work with quaternionic modular forms coming from a quaternion algebra ramifying at an inert or ramified prime $\mathfrak{l}|\mathfrak{c}$, adding further technicality, though we hope that the obstacle is surmountable. The condition (3) is a rigidity condition for nearly ordinary Galois deformation of $\mathrm{Ind}_M^F \varphi$, assuring the existence of the "universal" (not "versal") deformation ring. To remove this, we need to somehow invent a reasonable requirement to rigidify the deformation problem. The condition (4) is a technical assumption in order to form a Taylor-Wiles system to identify the deformation ring with an appropriate Hecke algebra (see [TW], [Fu] and [HMI] Sections 3.2–3).

The type of the assertion (in the theorem) is called the anticyclotomic main conjecture for CM fields. The main conjecture for imaginary quadratic fields (including the cyclotomic $\mathbb{Z}_p$–extension) and its anticyclotomic version for imaginary quadratic fields have been proved by K. Rubin [R] and [R1] refining Kolyvagin's method of Euler systems, and basically at the same time, the anticyclotomic conjecture was treated by J. Tilouine (and B. Mazur) [Ti] and [MT] (for imaginary quadratic cases) by a method similar to the one exploited here combined with the class number formula of the ring class fields. A partial result towards the general conjecture was studied in [HT1], [HT2] and [H05d].

The present idea of the proof is a refinement of those exploited in [HT1], [HT2] and [H05d] Theorem 5.1, where we have proven $L_p^-(\psi)|\mathcal{F}^-(\psi)$ in $\overline{W}[[\Gamma_M^-]]$. One of the main ingredients of the proof is the congruence power series $H(\psi) \in W[[\Gamma_M^-]]$ of the CM–component of the universal nearly ordinary Hecke algebra $\mathbf{h}$ for $GL(2)_{/F}$. In the joint works with Tilouine, we took $\mathbf{h}$ of (outside p) level $N_{M/F}(\mathfrak{C})d(M/F)$ for the conductor $\mathfrak{C}$ of φ and the relative discriminant $d(M/F)$ of M/F. In this paper, as in [H05d] Section 2.10, we take the Hecke algebra of level $\mathfrak{N}(\psi)$ which is a product of $\mathfrak{c}\cap F$ and $d(M/F)$ (introducing a new type of Neben character determined by φ with $\psi = \varphi^-$). Fujiwara formulated his results in [Fu] using such level groups. Another important ingredient is the divisibility proven in [H05d] Corollary 5.5:

$$\text{(L)} \qquad (h(M)/h(F))L_p^-(\psi^-)\big|H(\psi) \text{ in } \overline{W}[[\Gamma_M^-]].$$

Here $h(M)$ (resp. $h(F)$) is the class number of M (resp. F). On the other hand, Fujiwara's result already quoted implies (see [Fu], [HT2], [H00] and [HMI] Sections 3.2–3 and 5.3):

$$\text{(F)} \qquad H(\psi) = (h(M)/h(F))\mathcal{F}^-(\psi^-) \text{ up to units in } \overline{W}[[\Gamma_M^-]].$$

Thus we need to prove:

$$\text{(R)} \qquad H(\psi)(\kappa)\big|(h(M)/h(F))L_p^-(\psi^-)(\kappa) \text{ in } \overline{W}$$

for a (single) weight κ specialization, where $\Phi(\kappa)$ is the value of a power series $\Phi \in \overline{W}[[\Gamma_M^-]]$ at $\kappa \in \mathrm{Spec}(W[[\Gamma_M^-]])(W)$. By (L) and Nakayama's lemma, the reverse divisibility (R) (specialized at κ) implies the theorem. In the (finite dimensional) space $S_\kappa^{n.ord}(\mathfrak{N}(\psi)p^\infty, \varepsilon_\lambda; W)$ of nearly p–ordinary cusp forms of weight κ with coefficients in W and with suitable Neben character ε_λ, we have a CM Hecke eigenform $f(\lambda)$ of a Hecke character λ of weight κ (regarded as a Galois character) such that λ^- factors through $\mathrm{Gal}(M(\psi)M_\infty^-/M)$ and $\lambda^-|_{G_{tor}(\psi)} = \psi$. We write $\mathfrak{N}(\lambda)$ ($\mathfrak{N}(\lambda)|\mathfrak{N}(\psi)p^\infty$) for the level of $f(\lambda)$. This form studied in [H91] is of minimal level (possibly of level smaller than that of the primitive form). Since the CM local ring $\mathcal{R}$ of $\mathbf{h}$ is a Gorenstein ring (see [Fu], [H00] Corollary 5.3 (3) and [HMI] Proposition 1.53 and Theorem 3.59), the number $H(\psi)(\kappa)$ is the maximal denominator of the numbers $\frac{(f(\lambda),f)}{(f(\lambda),f(\lambda))}$ in W as f running through all elements of $S_\kappa(\mathfrak{N}(\lambda), \varepsilon_\lambda; W)$ (see again [H00] Corollary 5.3 (1) and [H86] Proposition 3.9), where $(\cdot,\cdot)$ is the Petersson inner product of level $\mathfrak{N}(\lambda)$. As seen in [HT1] Theorem 7.1 and [H05d]

Proposition 5.6, we have $\pi^{\kappa_1-\kappa_2+\Sigma}(f(\lambda),f(\lambda)) = c_1(h(M)/h(F))L(1,\lambda^-)$ for an innocuous constant $c_1 \in W$ (for the constant c_1, see (7.17)). The quotient $\frac{\pi^{2(\kappa_1-\kappa_2)}W_p(\lambda^-)(f(\lambda),f(\lambda))}{\Omega^{2(\kappa_1-\kappa_2)}}$ is then the value $(h(M)/h(F))L_p^-(\psi^-)(\kappa) \in \overline{W}$ (up to units in W). Here $W_p(\lambda^-)$ is the local Gauss sum of λ^- at p, Ω is the Néron period of the abelian variety of CM type Σ (defined over $\overline{\mathbb{Q}} \cap W$), and the exponent $\kappa_1 - \kappa_2$ is determined by the weight κ. Since $H(\psi)(\kappa)$ is the maximal denominator of $\frac{(f(\lambda),f)}{(f(\lambda),f(\lambda))}$, what we need to show (to prove (R)) is the W–integrality of $\frac{\pi^{2(\kappa_1-\kappa_2)}W_p(\lambda^-)(f(\lambda),f)}{\Omega^{2(\kappa_1-\kappa_2)}}$ for all $f \in S_\kappa(\mathfrak{N}(\lambda),\varepsilon_\lambda;W)$. This we will show by a detailed analysis of the residue formulas of generalized Eisenstein series, which we call Shimura series, on orthogonal groups of signature $(n,2)$. The series have been introduced in [Sh1] and [Sh2], and we take those associated with a theta series of M and the determinant (quadratic form) of $M_2(F)$. The validity of the q–expansion principle is very important to show the W–integrality, because we write the Petersson inner product as a value of a modular form (with integral q–expansion) at a CM point of (the product of two copies of) the Hilbert modular variety. This modular form is obtained as the residue of a Shimura series. However in the split case, the orthogonal similitude group of signature $(2,2)$ over F is isogenous to the product $GL(2) \times GL(2)_{/F}$; so, basically we are dealing with Hilbert modular forms, and the q–expansion principle is known by a work of Ribet (see [PAF] Theorem 4.21).

Another important point is to write down every W–integral Hilbert cusp form as a W–integral linear combination of theta series of the definite quaternion algebra unramified at every finite (henselian) place. Such a problem over $\mathbb{Q}$ was first studied by Eichler (his basis problem) and then generalized to the Hilbert modular case by Shimizu and Jacquet-Langlands in different manners. We scrutinize the integrality of the Jacquet-Langlands-Shimizu correspondence (mainly using duality between Hecke algebras and their spaces of cusp forms; see [H05b]). At the last step of finalizing the W–integral correspondence, we again need a result of Fujiwara: Freeness theorem in [Fu] of quaternionic cohomology groups as Hecke modules, which is valid again under the assumptions (1-4) for cusp forms with complex multiplication (see [HMI] Corollary 3.42). The everywhere unramified definite quaternion algebra exists only when the degree $[F : \mathbb{Q}]$ is even; so, we will at the end reduce, by a base-change argument, the case of odd degree to the case of even degree.

The identity: $(h(M)/h(F))L_p^-(\psi^-) = H(\psi)$ resulted from our proof of the theorem is the one (implicitly) conjectured at the end of [H86] (after Theorem 7.2) in the elliptic modular case. A similar conjecture made there for Eisenstein congruences has now also been proven by [O] under some mild assumptions.

2. Siegel's theta series for $GL(2) \times GL(2)$

Since the Shimura series has an integral presentation as a Rankin-Selberg convolution of Siegel's theta series and a Hilbert modular form, we recall here the definition and some properties of the theta series we need later.

2.1. Symmetric Domain of $O(n, 2)$.

We describe the symmetric domain associated to an orthogonal group of signature $(n, 2)$, following [Sh1] Section 2. Let V be a $n+2$–dimensional space over $\mathbb{R}$. We consider a symmetric bilinear form $S : V \times V \to \mathbb{R}$ of signature $(n, 2)$ with $n > 0$. We define an orthogonal similitude group G by

$$G(\mathbb{R}) = \left\{\alpha \in \mathrm{End}_{\mathbb{R}}(V) \middle| S(\alpha x, \alpha y) = \nu(\alpha)S(x, y) \text{ with } \nu(\alpha) \in \mathbb{R}^\times\right\}. \tag{2.1}$$

We would like to make explicit the symmetric hermitian domain $G(\mathbb{R})^+/\mathbb{R}^\times C$ for a maximal compact subgroup $C \subset G(\mathbb{R})^+$ for the identity connected component $G(\mathbb{R})^+$ of $G(\mathbb{R})$. We start with the following complex submanifold of $V_{\mathbb{C}} = V \otimes \mathbb{C}$:

$$\mathcal{Y}(S) = \left\{v \in V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C} \middle| S[v] = S(v, v) = 0,\ S(v, \overline{v}) < 0\right\}.$$

Since S is indefinite over $\mathbb{C}$, the space $\mathcal{Y}(S)$ is always non-empty. Obviously $g \in G(\mathbb{R})$ with $\nu(g) > 0$ acts on $\mathcal{Y}(S)$ by $v \mapsto gv$.

Take $v \in \mathcal{Y}(S)$, and write W for the subspace spanned over $\mathbb{R}$ by $v + \overline{v}$ and $iv - i\overline{v}$ for $i = \sqrt{-1}$. Then we have

$$\begin{aligned} &S(v + \overline{v}, v + \overline{v}) = 2S(v, \overline{v}) < 0 \\ &S(iv - i\overline{v}, iv - i\overline{v}) = 2S(v, \overline{v}) < 0 \\ &S(v + \overline{v}, iv - i\overline{v}) = -i \cdot S(v, \overline{v}) + i \cdot S(\overline{v}, v) = 0. \end{aligned}$$

This shows that $S|_W$ is negative definite. Let $W^\perp = \left\{w \in V \middle| S(w, W) = 0\right\}$. Then we have an orthogonal decomposition: $V = W \oplus W^\perp$ and $S|_{W^\perp}$ is positive definite. We then define a positive definite bilinear form

$$P_v(x, y) = -S(x_W, y_W) + S(x_{W^\perp}, y_{W^\perp})$$

for the orthogonal projections x_W to W and $x_{W^\perp}$ to $W^\perp$ of x. The bilinear form P_v is called the *positive majorant* of S indexed by $v \in \mathcal{Y}(S)$. If $g \in G(\mathbb{R})$ fixes $v \in \mathcal{Y}(S)$, g fixes by definition the positive definite form P_v. Thus g has to be in the compact subgroup $O(P_v)$ made up of orthogonal matrices preserving P_v. Thus $G(\mathbb{R})^+/O(P_v) \hookrightarrow \mathcal{Y}(S)$. If we have two $v, w \in \mathcal{Y}(S)$, then by Sylvester's theorem, we find $g \in G(\mathbb{R})^+$ such that $gv = w$, and hence $G(\mathbb{R})^+/O(P_v) \cong \mathcal{Y}(S)$.

Writing $P_v[x] = P_v(x,x)$ for $x = cv + \overline{cv} + z$ with $c \in \mathbb{C}$ and $z \in W^{\perp}$, we see

$$
\begin{aligned}
(2.2)\qquad P_v[x] - S[x] =& P_v(cv + \overline{cv} + z, cv + \overline{cv} + z) - S(cv + \overline{cv} + z, cv + \overline{cv} + z) \\
=& -2c^2 S[v] - 2\overline{c}^2 S[\overline{v}] - 4|c|^2 S(v,\overline{v}) + S[z] - S[z] \\
=& 4|c|^2 S(v,\overline{v}) = -4S(v,\overline{v})^{-1}|S(x,v)|^2 \geq 0.
\end{aligned}
$$

We now make explicit the domain $\mathcal{Y}(S)$ as a hermitian bounded matrix domain.

Proposition 2.1. *We have a $\mathbb{C}$–linear isomorphism $A : V_{\mathbb{C}} \cong \mathbb{C}^{n+2}$ such that*

$$S(x,y) = {}^t(Ax) \cdot RAy,\ \ S(\overline{x},y) = {}^t\overline{(Ax)} \cdot QAy,$$

where R and Q are real symmetric matrices given by

$$R = \left(\begin{smallmatrix} 1_n & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{smallmatrix}\right),\ Q = \left(\begin{smallmatrix} 1_n & 0 \\ 0 & -1_2 \end{smallmatrix}\right).$$

Proof. Choose a base $v_1, \ldots, v_{n+2}$ of V over $\mathbb{R}$, identify V with $\mathbb{R}^{n+2}$ by sending $\sum_{i=1}^{n+2} x_i v_i \mapsto {}^t(x_1, \ldots, x_{n+2}) \in \mathbb{R}^{n+2}$ and use the same symbol S for the symmetric matrix $(S(v_i,v_j))_{i,j}$. Then $S(x,y) = {}^t x \cdot Sy$ for $x, y \in V = \mathbb{R}^{n+2}$. By a theorem of Sylvester, S is equivalent (in $GL_{n+2}(\mathbb{R})$) to Q; so, we find an invertible matrix $X \in GL_{n+2}(\mathbb{R})$ with ${}^t X \cdot SX = Q$.

Choose $B = \mathrm{diag}[1_n, \sqrt{2}^{-1}\left(\begin{smallmatrix} 1 & 1 \\ -i & i \end{smallmatrix}\right)]$. Then by computation ${}^t\overline{B} \cdot QB = Q$ and ${}^t BQB = R$. Then $x \mapsto Ax$ for $A = (XB)^{-1} = B^{-1}X^{-1}$ does the desired job. □

By our choice of A, the map $\alpha \mapsto A\alpha A^{-1}$ gives an isomorphism of Lie groups:

$$
\begin{aligned}
(2.3)\quad & \iota : G(\mathbb{R}) \cong G(Q,R) \\
& = \left\{\alpha \in GL_{n+2}(\mathbb{C}) \middle| {}^t\alpha \cdot R\alpha = \nu(\alpha)R,\ {}^t\overline{\alpha} \cdot q\alpha = \nu(\alpha)Q \ \text{ with } \alpha \in \mathbb{R}^{\times}\right\},
\end{aligned}
$$

and the map: $v \mapsto Av$ gives an isomorphism of complex manifolds:

$$(2.4)\qquad j : \mathcal{Y}(S) \cong \mathcal{Y}(Q,R) = \left\{u \in \mathbb{C}^{n+2} \middle| {}^t u \cdot Ru = 0,\ {}^t\overline{u} \cdot Qu < 0\right\}.$$

These two maps are equivariant:

$$\iota(\alpha) j(v) = j(\alpha v).$$

We are going to show that $\mathcal{Y}(Q,R)$ has two connected components. Write $u = {}^t(u_1, \ldots, u_{n+2}) \in \mathcal{Y}(Q,R)$. Then we have

$$\left(\sum_{i=1}^n u_i^2\right) - 2u_{n+1}u_{n+2} = {}^t u \cdot Ru = 0,$$

$$\sum_{i=1}^n |u_i|^2 < |u_{n+1}|^2 + |u_{n+2}|^2 \Leftrightarrow {}^t\overline{u} \cdot Qu < 0.$$

Assume $|u_{n+1}| = |n_{n+2}|$ towards contradiction. Then we see

$$\sum_{j=1}^{n} |u_j|^2 \geq |\sum_{j=1}^{n} u_j^2| = 2|u_{n+1}u_{n+2}| = |u_{n+1}|^2 + |u_{n+2}|^2,$$

a contradiction; hence we have either $|u_{n+1}| > |u_{n+2}|$ or $|u_{n+1}| < |u_{n+2}|$. These two cases split the domain $\mathcal{Y}(Q,R)$ into two pieces of connected components. To see each component is connected, we may assume that $|u_{n+2}| > |u_{n+1}|$ by interchanging indices if necessary; so, $u_{n+2} \neq 0$. Put $z_j = U_j/u_{n+2}$ for $j \leq n$, and define a column vector $z = {}^t(z_1, z_2, \dots, z_n)$. Then $w = u_{n+1}/u_{n+2} = {}^tz \cdot z/2$, and defining

$$\mathfrak{Z} = \mathfrak{Z}_n = \left\{ z \in \mathbb{C}^n \middle| {}^tz \cdot \overline{z} < 1 + \frac{1}{4}|{}^tz \cdot z|^2 < 2 \right\}, \tag{2.5}$$

$\mathbb{C}^\times \times \mathfrak{Z}$ is isomorphic to the connected component of $\mathcal{Y}(Q,R)$ given by $|u_{n+2}| > |u_{n+1}|$ via $(\lambda, z) \mapsto \lambda\mathcal{P}(z)$, where

$$\mathcal{P}(z) = {}^t(z, ({}^tz \cdot z)/2, 1). \tag{2.6}$$

From this expression, it is plain that $\mathcal{Y}(Q,R)$ has two connected components. We define the action of $\alpha \in G(\mathbb{R})$ on $\mathfrak{Z}$ and a factor of automorphy $\mu(\alpha; z)$ ($z \in \mathfrak{Z}$) by

$$\iota(\alpha)\mathcal{P}(z) = \mathcal{P}(\alpha(z))\mu(\alpha; z). \tag{2.7}$$

We look into spherical functions on $V_{\mathbb{C}}$. Choose a base $v_1, \dots, v_d$ of V over $\mathbb{R}$. By means of this base, we identify V with $\mathbb{R}^d$ ($d = n+2$); so, $v \mapsto (x_1, \dots, x_d)$ if $v = \sum_j x_j v_j$. We take the dual base v_j^* so that $S(v_i^*, v_j) = \delta_{ij}$ for the Kronecker symbol δ_{ij} and define a second-degree homogeneous differential operator Δ by

$$\Delta = \sum_{i,j} S(v_i^*, v_j^*) \frac{\partial^2}{\partial x_i \partial x_j}.$$

A polynomial function $\eta : V \to \mathbb{C}$ is called a spherical function if $\Delta\eta = 0$. Writing $S = (S(v_i, v_j))$, we see that this definition does not depend on the choice of the base v_j, because $\Delta = {}^t\partial S^{-1}\partial$ for $\partial = {}^t(\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_d})$. Since $\partial({}^twSx) = Sw$ for a constant vector $w = (w_1, \dots, w_d)$, we find that, for $k \geq 2$

$$\Delta({}^twSx)^k = k{}^t\partial(S^{-1}Sw)({}^twSx)^{k-1} = k(k-1)({}^twSw)({}^twSx)^{k-2}.$$

Thus the polynomial function $x \mapsto S(w,x)^k$ for $k \geq 2$ is spherical if and only if $S[w] := S(w,w) = 0$. All homogeneous spherical functions of degree $k \geq 2$ are linear combination of $S(w,x)^k$ for a finite set of spherical vectors w with $S[w] = 0$. In particular, for $v \in \mathcal{Y}(S)$, the function $x \mapsto S(v,x)^k$ is a spherical function.

Note here that for $v \in \mathcal{Y}(S)$, $S[v] = 0$ and $S(v,x) = -P_v(v,x)$, because $P(v,x) = P(v, x_W) + P(v, x_{W^\perp}) = -S(v, x_W) = -S(v,x)$. Define $\partial_v = \widetilde{v} \cdot \partial$, where $\widetilde{v} = (\lambda_1, \dots, \lambda_d)$ when $v = \sum_j \lambda_j v_j$. Then we have, by computation,

$$\partial_v S[x] = 2S(v,x), \ \partial_v P_v[x] = 2P_v(v,x) = -S(v,x). \tag{2.8}$$

We define a Schwartz function Ψ on V for each $\tau = \xi + i\eta \in \mathfrak{H}$ and $v \in \mathcal{Y}(S)$ by

$$\Psi(\tau; v; w) = \mathbf{e}(\frac{1}{2}(S[w]\xi + iP_v[w]\eta)) = \exp(\pi i(S[w]\xi + iP_v[w]\eta)).$$

We see by computation using (2.8)

$$(\partial_v^k \Psi)(\tau; v; w) = (2\pi i)^k (\overline{\tau} S(v, w))^k \Psi(\tau; v; w). \tag{2.9}$$

2.2. $SL(2) \times SL(2)$ as an orthogonal group. We realize the product as an orthogonal group of signature $(2, 2)$, and hence this group gives a special case of the orthogonal groups treated in the previous subsection.

Let $V = M_2(\mathbb{R})$, and consider the symmetric bilinear form $S : V \times V \to \mathbb{R}$ given by $S(x, y) = \mathrm{Tr}(xy^\iota)$, where $yy^\iota = y^\iota y = \det(y)$ for 2×2 matrices y. We let $(a, b) \in GL_2(\mathbb{R}) \times GL_2(\mathbb{R})$ act on V by $x \mapsto axb^\iota$. Then

$$\begin{aligned} S(axb^\iota, ayb^\iota) = \mathrm{Tr}(axb^\iota b y^\iota a^\iota) &= \det(b)\mathrm{Tr}(axy^\iota a^\iota) \\ &= \det(b)\mathrm{Tr}(xy^\iota a^\iota a) = \det(a)\det(b) S(x, y). \end{aligned}$$

Thus we have an isomorphism

$$(GL_2(\mathbb{R}) \times GL_2(\mathbb{R})) / \{\pm(1, 1)\} \hookrightarrow G(\mathbb{R})$$

with $\nu(a, b) = \det(a)\det(b)$. Since the symmetric space of $G(\mathbb{R})$ has dimension 2 over $\mathbb{C}$, the above isomorphism has to be onto on the identity connected component. Since $G(\mathbb{R})$ has four connected components (because $\mathcal{Y}(S)$ has two), the above morphism has to be a surjective isomorphism because $GL_2(\mathbb{R}) \times GL_2(\mathbb{R})$ has four connected components:

$$(GL_2(\mathbb{R}) \times GL_2(\mathbb{R})) / \{\pm(1, 1)\} \cong G(\mathbb{R}). \tag{2.10}$$

Since the symmetric domain of $GL_2(\mathbb{R}) \times GL_2(\mathbb{R})$ is isomorphic to $\mathfrak{H} \times \mathfrak{H}$ for the upper half complex plane $\mathfrak{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$, we find that $\mathfrak{Z} \cong \mathfrak{H} \times \mathfrak{H}$.

We are going to make this isomorphism: $\mathfrak{Z} \cong \mathfrak{H} \times \mathfrak{H}$ more explicit. We study $\mathcal{Y} = \mathcal{Y}(S)$ more closely. Since $V_\mathbb{C} = M_2(\mathbb{C})$, writing $v = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{C})$, we have from the definition:

$$\mathcal{Y} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{C}) \middle| ad = bc,\ a\overline{d} - b\overline{c} + d\overline{a} - c\overline{b} < 0 \right\}.$$

Pick $v = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{Y}$, and suppose that $c = 0$. Then by the defining equation of $\mathcal{Y}$, $ad = 0 \Rightarrow 0 = a\overline{d} + d\overline{a} < 0$, which is a contradiction. Thus $c \neq 0$; so, we define for v as above, $z = \frac{a}{c}$ and $w = -\frac{d}{c}$. Then $-zw = \frac{b}{c}$, and hence (see [Sh2] II (4.6))

$$v = cp(z, w) \ \text{ with } \ p(z, w) = \left(\begin{smallmatrix} z & -wz \\ 1 & -w \end{smallmatrix}\right) = -{}^t(z, 1)(w, 1)\varepsilon, \tag{2.11}$$

where $\varepsilon = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Again by the equation defining $\mathcal{Y}$,

$$S(p(z, w), \overline{p(z, w)}) = (w - \overline{w})(z - \overline{z}) = -z\overline{w} + zw - \overline{z}w + \overline{zw} < 0. \tag{2.12}$$

From this, it is clear that $\mathcal{Y} \cong \mathbb{C}^\times \times \left(\mathfrak{H}^2 \sqcup \overline{\mathfrak{H}}^2\right)$. By this isomorphism, for $\alpha \in G(\mathbb{R})$, we can define its action $\alpha(z,w) \in \left(\mathfrak{H}^2 \sqcup \overline{\mathfrak{H}}^2\right)$ and a factor $\mu(\alpha; z, w) \in \mathbb{C}^\times$ of automorphy by

$$\alpha \cdot p(z,w) = p(\alpha(z,w))\mu(\alpha; z, w).$$

By a direct computation, writing $j(v,z) = cz+d$ for $v = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $v(z) = \frac{az+b}{cz+d}$, we have, for $(\alpha,\beta) \in GL_2(\mathbb{R}) \times GL_2(\mathbb{R})$,

$$\alpha p(z,w)\beta^\iota = p(\alpha(z),\beta(w))j(\alpha,z)j(\beta,w). \tag{2.13}$$

Thus

$$(\alpha,\beta)(z,w) = (\alpha(z),\beta(w)) \quad \text{and} \quad \mu((\alpha,\beta);(z,w)) = j(\alpha,z)j(\beta,w).$$

We define a spherical function

$$v \mapsto [v; z, w]^k = S(v, p(z,w))^k \tag{2.14}$$

for a positive integer $k > 0$. This function is spherical because $S[p(z,w)] = 2\det p(z,w) = 0$, and we have

$$[\alpha v \beta^\iota; z, w] = j(\alpha^\iota, z)j(\beta^\iota, w)[v; \alpha^{-1}(z), \beta^{-1}(w)]. \tag{2.15}$$

2.3. Growth of theta series. Let F be a totally real field with integer ring O and B be a quaternion algebra over F. The algebra B can be $M_2(F)$. Let $x \mapsto x^\iota$ be the main involution of B; so, $xx^\iota = N(x)$ and $x + x^\iota = \mathrm{Tr}(x)$ for the reduced norm $N : B \to F$ and the reduced trace $\mathrm{Tr} : B \to F$. We consider the symmetric bilinear form $S : B \times B \to F$ given by $S(x,y) = \mathrm{Tr}(xy^\iota)$.

Writing I for the set of all archimedean places of F, we split $I = I_B \sqcup I^B$ so that $B \otimes_{F,\sigma} \mathbb{R} \cong M_2(\mathbb{R}) \Leftrightarrow \sigma \in I_B$. Thus for $\sigma \in I^B$,

$$B \otimes_{F,\sigma} \mathbb{R} \cong \mathbb{H} = \left\{ \left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right) \middle| a, b \in \mathbb{C} \right\}.$$

We identify $B_\sigma = B \otimes_{F,\sigma} \mathbb{R}$ with $M_2(\mathbb{R})$ or $\mathbb{H}$ for each $\sigma \in I$. Thus $G(\mathbb{Q}) = (B^\times \times B^\times)/\{\pm(1,1)\}$ is the orthogonal group of (B,S). Since S at $\sigma \in I^B$ is positive definite, $G(\mathbb{R}) \cong (GL_2(\mathbb{R}) \times GL_2(\mathbb{R}))^{I_B} \times (\mathbb{H}^\times \times \mathbb{H}^\times)^{I^B}/\{\pm(1,1)\}$. For each $b \in B_\infty = B \otimes_\mathbb{Q} \mathbb{R}$, writing $b = (b_\sigma)$ for σ–component $b_\sigma \in B_\sigma$, we define

$$[b; z, w]^k = \prod_{\sigma \in I_B} [b_\sigma; z_\sigma, w_\sigma]^{k_\sigma} \quad (k = \sum_{\sigma \in I_B} k_\sigma \sigma \in \mathbb{Z}[I_B]), \tag{2.16}$$

where $[b_\sigma; z_\sigma, w_\sigma]$ is as in (2.14) defined for $B_\sigma = M_2(\mathbb{R})$. For $\sigma \in I^B$, we pick a homogeneous spherical polynomial $\varphi_\sigma : B_\sigma \to \mathbb{C}$ of degree κ_σ, and put $\varphi = \prod_{\sigma \in I^B} \varphi_\sigma$ and $\kappa = \sum_\sigma \kappa_\sigma \in \mathbb{Z}[I^B]$. We define an additive character $\mathbf{e}_F : F_\mathbb{C} = F \otimes_\mathbb{Q} \mathbb{C} \to \mathbb{C}^\times$ by $\mathbf{e}_F(z) = \exp(2\pi i \sum_\sigma z_\sigma)$ $(z = (z_\sigma)_{\sigma \in I})$ identifying $F_\mathbb{C}$ with $\mathbb{C}^I$ as $\mathbb{C}$–algebras. Writing $\mathrm{Tr} : F_\mathbb{C} \to \mathbb{C}$ for the trace map, we have $\mathbf{e}_F(z) = \mathbf{e}(\mathrm{Tr}(z))$.

We consider Siegel's theta series defined for $0 \le k \in \mathbb{Z}[I_B]$ and a Schwartz-Bruhat function $\phi : B_{\mathbb{A}(\infty)} \to \mathbb{C}$:

$$\text{(2.17)} \quad \eta^{-I}\theta_k(\tau; z, w; v, \phi\varphi) = \sum_{\ell \in B} [\ell; z, w]^k (\phi\varphi)(\ell) \mathbf{e}_F(\frac{1}{2}(\xi S[\ell] + i\eta P_{p(z,w)}[\ell]))$$
$$= \sum_{\ell \in B} [\ell; z, w]^k (\phi\varphi)(\ell) \mathbf{e}(\frac{1}{2}\mathrm{Tr}(S[\ell]\tau)) \mathbf{e}\left(\frac{i}{2} \sum_{\sigma \in I_B} \frac{\eta_\sigma \left|[\ell_\sigma; z_\sigma, w_\sigma]\right|^2}{\mathrm{Im}(z_\sigma)\,\mathrm{Im}(w_\sigma)} \right),$$

where $\tau = \xi + i\eta \in \mathfrak{H}^I$, $\eta^I(\tau) = \prod_\sigma \eta_\sigma$ and the last equality follows from (2.12). Since the majorant $P_{p(z,w)}$ is positive definite, the theta series is rapidly decreasing with respect to τ towards the cusp ∞, as long as $\varphi(0)[0; z, w]^k = 0$ (in other words, as long as $k + \kappa > 0$). Since the infinity type $k + \kappa$ does not change under the transformation $\tau \mapsto \alpha(\tau)$ for $\alpha \in SL_2(F)$, the theta series is rapidly decreasing towards any given cusp if $k + \kappa > 0$. Otherwise it is slowly increasing (see below Proposition 2.3).

2.4. Partial Fourier transform. We are going to compute in the following subsection the Fourier expansion of the theta series (introduced in the earlier subsections) with respect to (z, w) when $B = M_2(F)$. This is non-trivial, because θ is defined by its Fourier expansion with respect to the variable τ. A key idea is to compute the partial Fourier transform of each term of the theta series and to resort to the Poisson summation formula. In this subsection, we describe the computation of the partial Fourier transform.

The Schwartz function on $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} = M_2(F_\infty)$ which gives rise to the theta series $\theta_0(\tau; z, w; \phi)$ is given by

$$u \mapsto \Psi_0(u) = \eta^I \mathbf{e}_F(\det(u)\tau + \frac{\eta}{2yt}|[u; z, w]|^2)$$

for $\tau = \xi + i\eta$, $z = x + yi$ and $w = r + ti$ with $\xi, x, r \in F_\infty$ and $\eta, y, t \in F^\times_{\infty+}$. Here $F^\times_{\infty+}$ is the identity connected component of $F^\times_\infty$. We define

$$\text{(2.18)} \quad \Psi_k(u) = \prod_\sigma \Psi_{k_\sigma,\sigma}(u_\sigma) \quad (0 \le k = \sum_\sigma k_\sigma \sigma \in \mathbb{Z}[I]) \text{ and}$$
$$\Psi_{k_\sigma,\sigma}(u_\sigma) = \eta_\sigma^{k_\sigma+1}[u_\sigma; z_\sigma, w_\sigma]^{k_\sigma} \mathbf{e}(\det[u_\sigma]\tau_\sigma + i\frac{\eta_\sigma}{2y_\sigma t_\sigma}|[u_\sigma; z_\sigma, w_\sigma]|^2).$$

We write the variable $u = \left(\begin{smallmatrix} u_1 \\ u_2 \end{smallmatrix}\right)$ for two row vectors u_j and write individually $u_1 = (a, b)$ and $u_2 = (c, d)$. The partial Fourier transform ϕ^* of ϕ is given by

$$\text{(2.19)} \qquad \phi^*\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \int_{F^2_\infty} \phi\left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right) \mathbf{e}_F(ab' - ba')da'db',$$

where $ab' - ba' = \frac{1}{2}S\left[\left(\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right)\right]$ and $da' = \otimes_\sigma da'_\sigma$ for the Lebesgue measure da'_σ on the σ–component $\mathbb{R}$ of F_∞. By applying complex conjugation, we have

$$\text{(2.20)} \qquad \overline{\phi^*}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\overline{\phi}\right)^*\left(\begin{smallmatrix} -a & -b \\ c & d \end{smallmatrix}\right).$$

We compute first the partial Fourier transform to the action of $\mathcal{U}(F_\infty) \times GL_2(F_\infty)$, where $\mathcal{U}(X)$ is made up of upper unipotent matrices with right shoulder entry in X. We first deal with $(1, \beta)$ with $\beta \in GL_2(F_\infty)$:

$$\begin{aligned}(\phi\circ(1,\beta))^*\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) &= \int_{F_\infty^2} \phi\left(\left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)\beta^\iota\right)\mathbf{e}_F(-(a',b')\varepsilon^t(a,b))da'db' \\ &\overset{(a',b')\beta^\iota\mapsto(a',b')}{=} |N(\det(\beta)|^{-1}\int_{F_\infty^2}\phi\left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)\mathbf{e}_F(-(a',b')\beta^{-\iota}\varepsilon^t(a,b))da'db' \\ &= |N(\det(\beta)|^{-1}\int_{F_\infty^2}\phi\left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)\mathbf{e}_F(-(a',b')\beta^{-\iota}\varepsilon^t\beta^{-1t}(a,b))da'db' \\ &= |N(\det(\beta)|^{-1}\phi^*\circ\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & \det(\beta)\end{smallmatrix}\right),\beta^{-1}\right)\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right).\end{aligned}$$

We now compute $(\phi\circ(\alpha,1))^*$ for $\alpha\in\mathcal{U}(F_\infty)$:

$$\begin{aligned}(\phi\circ(\left(\begin{smallmatrix} 1 & x \\ 0 & 1\end{smallmatrix}\right),1))^*\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) &= \int_{F_\infty^2}\phi\left(\begin{smallmatrix} a'+xc & b'+xd \\ c & d\end{smallmatrix}\right)\mathbf{e}_F(ab'-ba')da'db' \\ &\overset{(a'+xc,b'+xd)\mapsto(a',b')}{=} \int_{F_\infty^2}\phi\left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)\mathbf{e}_F(ab'-ba')da'db'\mathbf{e}_F(-x(ad-bc)) \\ &= \mathbf{e}_F(-x(ad-bc))\phi^*\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right).\end{aligned}$$

Summarizing the above computation, we get for $(\left(\begin{smallmatrix} 1 & x \\ 0 & 1\end{smallmatrix}\right),1)\in\mathcal{U}(F_\infty)\times SL_2(F_\infty)$

$$(\phi\circ(\left(\begin{smallmatrix} 1 & x \\ 0 & 1\end{smallmatrix}\right),\beta))^*(u) = \mathbf{e}_F(-x\det(u))\phi^*\circ(1,\beta^{-1})(u). \tag{2.21}$$

By (2.15), for $(\alpha,\beta)\in SL_2(F_\infty)\times SL_2(F_\infty)$, we have

$$\begin{aligned}[\alpha u\beta^\iota; z, w] = S(\alpha u\beta^\iota; p(z,w)) &= S(u;\alpha^{-1}p(z,w)\beta^{-\iota}) \\ &= [u,\alpha^{-1}(z),\beta^{-1}(w)]j(\alpha^{-1},z)j(\beta^{-1},z).\end{aligned}$$

To compute the partial Fourier transform of Ψ_k, we may therefore assume that $r = x = 0$. Then the computation for Ψ_0^* is reduced to, writing $u' = \left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)$ (and omitting the subscript σ),

$$\begin{aligned}&\int_{F_\sigma^2}\Psi_{0,\sigma}(u')\mathbf{e}(ab'-ba')da'db' = \\ &\int_{\mathbb{R}^2}\eta\mathbf{e}\left(\xi\det u' + \frac{i\eta}{2}(\frac{ta'^2}{y}+\frac{b'^2}{yt}+\frac{yd^2}{t}+ytc^2)\right)\mathbf{e}(ab'-ba')da'db'.\end{aligned}\tag{2.22}$$

We then invoke the following formula:

$$\int_{-\infty}^{\infty}\exp(-\pi z a'^2)\mathbf{e}(a'b)da' = z^{-1/2}\exp(-\frac{\pi b^2}{z}),$$

where $z \in \mathbb{C} - \mathbb{R}_-$ ($\mathbb{R}_-$: the negative real line) and $z^{-1/2}$ is the branch of the square root which is positive real if z is positive real. Then (2.22) is equal to

(2.23)
$$y_\sigma \exp(-\pi\eta^{-1}\left(\frac{y_\sigma}{t_\sigma}(d\xi_\sigma - b)^2 + y_\sigma t_\sigma(c\xi_\sigma - a)^2\right)\mathbf{e}\left(\frac{i\eta_\sigma}{2}(\frac{y_\sigma}{t_\sigma}d^2 + y_\sigma t_\sigma c^2)\right)$$
$$= y_\sigma \exp\left(-\pi\frac{y_\sigma}{\eta_\sigma}(\frac{1}{t_\sigma}|d\tau_\sigma - b|^2 + t|c\tau_\sigma - a|^2)\right).$$

By computation, we have

$$t|\tau c - a|^2 + t^{-1}|\tau d - b|^2 = t^{-1}|[u;\tau, it]|^2 + 2\eta\det(u). \tag{2.24}$$

Thus we get

$$\Phi_0(u) = \Psi_0^*(u) = \prod_\sigma \Psi_{0,\sigma}^*(u_\sigma),$$
$$\Phi_{0,\sigma}(u) = \Psi_{0,\sigma}^*\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) = y_\sigma \exp\left(-\pi\frac{y_\sigma}{\eta_\sigma}(\frac{1}{t_\sigma}|d\tau_\sigma - b|^2 + t_\sigma|c\tau_\sigma - a|^2)\right) \tag{2.25}$$
$$= y_\sigma \exp\left(-2\pi y_\sigma\det(u) - \pi\frac{y_\sigma}{\eta_\sigma t_\sigma}|[u;\tau_\sigma, it_\sigma]|^2\right).$$

In order to compute the partial Fourier transform of Ψ_k, we consider the following differential operator

$$\partial_\sigma = S\left(p(\tau_\sigma, w_\sigma), {}^t\left(\begin{smallmatrix} \frac{\partial}{\partial a} & \frac{\partial}{\partial b} \\ \frac{\partial}{\partial c} & \frac{\partial}{\partial d}\end{smallmatrix}\right)^\iota\right) = \tau_\sigma\frac{\partial}{\partial a} - w_\sigma\tau_\sigma\frac{\partial}{\partial b} + \frac{\partial}{\partial c} - w_\sigma\frac{\partial}{\partial d}. \tag{2.26}$$

Since we have, for $u = \left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)$,

$$\tau_\sigma\frac{\partial}{\partial a}\mathbf{e}(ab' - ba') = 2\pi i\tau_\sigma b'\mathbf{e}(ab' - ba')$$
$$-w_\sigma\tau_\sigma\frac{\partial}{\partial b}\mathbf{e}(ab' - ba') = 2\pi i w_\sigma\tau_\sigma a'\mathbf{e}(ab' - ba')$$
$$\frac{\partial}{\partial c}\Psi_{0,\sigma}(u) = (-2\pi i b'\tau_\sigma - \pi\frac{\eta_\sigma}{y_\sigma t_\sigma}(w_\sigma z_\sigma\overline{[u;z_\sigma, w_\sigma]} + \overline{w}_\sigma\overline{z}_\sigma[u;z_\sigma, w_\sigma]))\Psi_{0,\sigma}(u)$$
$$-w_\sigma\frac{\partial}{\partial d}\Psi_{0,\sigma}(u)$$
$$= -(2\pi i a'\tau_\sigma w_\sigma - \pi\frac{\eta_\sigma}{y_\sigma t_\sigma}(w_\sigma z_\sigma\overline{[u;z_\sigma, w_\sigma]} + w_\sigma\overline{z}_\sigma[u;z_\sigma, w_\sigma]))\Psi_{0,\sigma}(u).$$

Taking the fact that $\overline{w}_\sigma - w_\sigma = 2it_\sigma$, $z_\sigma = iy_\sigma$ and

$$\partial_\sigma([u;z_\sigma, w_\sigma]) = \partial_\sigma(S_\sigma(u, p(z_\sigma, w_\sigma)) = S_\sigma(p(\tau_\sigma, w_\sigma), p(z_\sigma, w_\sigma)) = 0$$

into account, we have

$$\partial_\sigma(\Psi_{j,\sigma}(u)\mathbf{e}(ab' - ba')) = 2\pi\Psi_{j+1,\sigma}(u)\mathbf{e}(ab' - ba') \tag{2.27}$$

for all integers $j \geq 0$.

To complete the computation, we need to compute $\partial_\sigma \Phi_{j,\sigma}(u)$. We have, noting that we are restricting ourselves to $w_\sigma = it_\sigma$:

$$\begin{aligned}
\tau_\sigma \frac{\partial}{\partial a}\Phi_{0,\sigma}(u) &= \pi\frac{y_\sigma t_\sigma}{\eta_\sigma}(\tau_\sigma(c\overline{\tau}_\sigma - a) + \tau_\sigma(c\tau_\sigma - a))\Phi_{0,\sigma}(u)\\
-it_\sigma\tau_\sigma \frac{\partial}{\partial b}\Phi_{0,\sigma}(u) &= -\pi i\frac{y_\sigma}{\eta_\sigma}(\tau_\sigma(d\overline{\tau}_\sigma - b) + \tau_\sigma(d\tau_\sigma - b))\Phi_{0,\sigma}(u)\\
\frac{\partial}{\partial c}\Phi_{0,\sigma}(u) &= -\pi\frac{y_\sigma t_\sigma}{\eta_\sigma}(\tau_\sigma(c\overline{\tau}_\sigma - a) + \overline{\tau}_\sigma(c\tau_\sigma - a))\Phi_{0,\sigma}(u)\\
-it_\sigma \frac{\partial}{\partial d}\Phi_{0,\sigma}(u) &= \pi i\frac{y_\sigma}{\eta_\sigma}(\tau_\sigma(d\overline{\tau}_\sigma - b) + \overline{\tau}_\sigma(d\tau_\sigma - b))\Phi_{0,\sigma}(u).
\end{aligned}$$

From this we get, taking the fact:

$$it_\sigma(c\tau_\sigma - a) + d\tau_\sigma - b = [u;\tau, it_\sigma]$$

into account, we have

$$\partial_\sigma \Phi_{0,\sigma}(u) = 2\pi y_\sigma[u;\tau_\sigma, it_\sigma]\Phi_{0,\sigma}(u).$$

Since $\partial_\sigma([u;\tau,w]) = 0$, we again obtain, when $z = iy$ and $w = it$,

$$\partial_\sigma(\Phi_{j,\sigma})(u) = 2\pi\Phi_{j+1}(u), \tag{2.28}$$

where $\Phi_{j,\sigma}(u) = y_\sigma^{j+1}[u;\tau,w]^j\Phi_{0,\sigma}(u)$. By (2.27) and (2.28) combined, we get, at this moment for $z = iy$ and $w = it$,

$$\left(\Psi_k\right)^*(u) = \Phi_k(u), \tag{2.29}$$

where $\Phi_k(u) = \prod_\sigma \Phi_{k_\sigma,\sigma}(u_\sigma)$ and $\Psi_k(u) = \prod_\sigma \Psi_{k_\sigma,\sigma}(u_\sigma)$.

We are going to compute the partial Fourier transform for general (z,w) and show that (2.29) is valid in general under a suitable description of Φ for general (z,w): To do this, we write

$$\Psi^{z_\sigma,w_\sigma,\tau_\sigma}_{j,\sigma}(u) = \eta_\sigma^{j+1}[u;z_\sigma,w_\sigma]^j\mathbf{e}\left(\det(u)\tau_\sigma + i\frac{\eta_\sigma}{2y_\sigma t_\sigma}\left|[u;z_\sigma,w_\sigma]\right|^2\right).$$

Since $[u,\alpha(z_\sigma),\beta(w_\sigma)]j(\alpha,z)j(\beta,w) = [\alpha^{-1}u\beta^{-\iota};z_\sigma,w_\sigma]$ by (2.13) and (2.14) combined, we have

$$\Psi^{z_\sigma,w_\sigma,\tau_\sigma}_{j,\sigma} = \Psi^{iy_\sigma,it_\sigma,\tau_\sigma}_{j,\sigma}\circ\left(\left(\begin{smallmatrix}1 & -x_\sigma\\ 0 & 1\end{smallmatrix}\right),\left(\begin{smallmatrix}1 & -r_\sigma\\ 0 & 1\end{smallmatrix}\right)\right).$$

Then by (2.21),

$$\left(\phi\circ\left(\left(\begin{smallmatrix}1 & -x_\sigma\\ 0 & 1\end{smallmatrix}\right),\left(\begin{smallmatrix}1 & -r_\sigma\\ 0 & 1\end{smallmatrix}\right)\right)\right)^*(u) = \mathbf{e}(x_\sigma\det(u))\phi^*\circ\left(1,\left(\begin{smallmatrix}1 & r_\sigma\\ 0 & 1\end{smallmatrix}\right)\right)$$

and applying this to $\Psi^{z_\sigma,w_\sigma,\tau_\sigma}_{j,\sigma}$, we get from (2.29)

$$\left(\Psi^{z_\sigma,w_\sigma,\tau_\sigma}_{j,\sigma}\right)^*(u) = \mathbf{e}(x_\sigma\det(u))\Phi^{iy_\sigma,it_\sigma,\tau_\sigma}_{j,\sigma}\left(u\left(\begin{smallmatrix}1 & -r_\sigma\\ 0 & 1\end{smallmatrix}\right)\right),$$

where

$$\Phi^{iy_\sigma,it_\sigma,\tau_\sigma}_{j,\sigma}(u) = [u_\sigma;\tau_\sigma,it_\sigma]^j y_\sigma^{j+1}\exp\left(-2\pi y_\sigma\det(u) - \pi\frac{y_\sigma}{\eta_\sigma t_\sigma}|[u;\tau_\sigma,it_\sigma]|^2\right).$$

Define

(2.30)

$$\Phi_k(u) = \Phi_k^{z,w,\tau}(u) = \prod_\sigma \Phi_{k_\sigma,\sigma}^{z_\sigma,w_\sigma,\tau_\sigma}(u) \text{ for}$$

$$\Phi_{j,\sigma}(u) = \Phi_{j,\sigma}^{z_\sigma,w_\sigma,\tau_\sigma}(u) = y_\sigma^{j+1}[u;\tau_\sigma,w_\sigma]^j \mathbf{e}\left(\det(u)z_\sigma + \frac{iy_\sigma}{2\eta_\sigma t_\sigma}|[u;\tau_\sigma,w_\sigma]|^2\right).$$

Using this definition, (2.29) is valid for general $(z,w,\tau) \in \mathfrak{H}^I \times \mathfrak{H}^I \times \mathfrak{H}^I$. In other words, we have the reciprocal formula:

$$\Phi_k^{z,w,\tau} = \Psi_k^{\tau,w,z} \text{ and } (\Psi_k^{z,w,\tau})^*(u) = \Psi_k^{\tau,w,z}(u). \tag{2.31}$$

By (2.20) (and (2.15)), we also have

$$\left(\overline{\Psi_k^{z,w,\tau}}\right)^*(u) \tag{2.32}$$

$$= \prod_\sigma \left(y_\sigma^{k_\sigma+1}[u_\sigma;-\overline{\tau}_\sigma,\overline{w}_\sigma]^{k_\sigma}\mathbf{e}\left(\det(u_\sigma)\overline{\tau}_\sigma + \frac{y_\sigma}{2\eta_\sigma t_\sigma}|[u_\sigma;-\overline{\tau}_\sigma,\overline{w}_\sigma]|^2\right)\right).$$

2.5. Fourier expansion of theta series. Write $V = M_2(F)$. We choose on $F_{\mathbb{A}^{(\infty)}} = F \otimes_{\mathbb{Q}} \mathbb{A}^{(\infty)}$ the standard additive Haar measure da so that

$$\int_{\widehat{O}} da = 1 \text{ for } \widehat{O} = O \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \ \ (\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p).$$

At infinity, we choose the Lebesgue measure $\otimes_\sigma da_\sigma$ on $F_\infty = \prod_{\sigma\in I}\mathbb{R}$. Then we take the tensor product measure $du = da\otimes db\otimes dc\otimes dd$ for $u = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in V_{\mathbb{A}}$.

Let $\phi : V_{\mathbb{A}} = M_2(F_{\mathbb{A}}) \to \mathbb{C}$ be a Schwartz-Bruhat function, and assume that $\phi = \prod_v \phi_v$ for $\phi_v : V \otimes \mathbb{Q}_v \to \mathbb{C}$. We define the partial Fourier transform of ϕ for $\phi : V_{\mathbb{A}} \to \mathbb{C}$ by the same formula as in (2.19):

$$\phi^*\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) = \int_{F_{\mathbb{A}}^2} \phi\left(\begin{smallmatrix} a' & b' \\ c & d\end{smallmatrix}\right)\mathbf{e}_{\mathbb{A}}(ab'-ba')da'db', \tag{2.33}$$

where $\mathbf{e}_{\mathbb{A}} : F_{\mathbb{A}}/F \to \mathbb{C}^\times$ is the additive character with $\mathbf{e}_{\mathbb{A}}(x_\infty) = \mathbf{e}_F(x_\infty)$ for $x_\infty \in F_\infty$. We further assume that $\phi_\infty = \Psi_k^{z,w,\tau}$ studied in the previous subsection. Then we define

$$\Theta(\phi) = \sum_{\ell\in V}\phi(\ell). \tag{2.34}$$

Writing $\phi^{(\infty)}$ for the finite part of ϕ and regarding it as a function on $V \subset V_{\mathbb{A}^{(\infty)}}$, we find

$$\Theta(\phi) = \eta^k\theta_k(\tau;z,w;\phi^{(\infty)}).$$

Since $\int_{F_{\mathbb{A}}/F} da = \sqrt{|D|}$ for the discriminant D of F, the measure $|D|^{-1}da'db'$ has volume 1 for the quotient $F_{\mathbb{A}}^2/F^2$. Thus $|D|^{-1}\phi^*$ gives the partial Fourier transform with respect to volume 1 measure $|D|^{-1}da'db'$. The Poisson summation formula (with respect to the discrete subgroup $F^2 \subset F_{\mathbb{A}}^2$) is valid for the volume 1 measure (cf. [LFE] Section 8.4), we have the following result:

Proposition 2.2. *We have $\Theta(\phi) = |D|^{-1}\Theta(\phi^*)$. In terms of θ_k, we have*

$$\eta^k\theta_k(\tau; z, w; \phi^{(\infty)}) = |D|^{-1}y^k\theta_k(z; \tau, w; \phi^{*(\infty)}).$$

We could say that the right-hand-side of this formula gives the Fourier expansion of the theta series in terms of the variable z.

Proposition 2.3. *Let*

$$\Gamma^\tau(\phi^*) = \{\gamma \in SL_2(F) | \phi^{*(\infty)}(\gamma u) = \chi_\tau(\gamma)\phi^{*(\infty)}(u)\}$$
$$\Gamma^{z,w}(\phi) = \{(\gamma, \delta) \in SL_2(F)^2 | \phi^{(\infty)}(\gamma u \delta^{-1}) = \chi_{z,w}(\gamma, \delta)\phi^{(\infty)}(u)\}.$$

for characters $\chi_\tau : \Gamma^\tau(\phi^*) \to \mathbb{C}^\times$ and $\chi_{z,w} : \Gamma^{z,w}(\phi) \to \mathbb{C}^\times$ Suppose that $\phi_\infty = \Psi_k^{z,w,\tau}$. Then for $(\alpha, \beta, \gamma) \in \Gamma^\tau(\phi^*) \times \Gamma^{z,w}(\phi)$, we have

$$\begin{aligned}&\Theta(\phi)(\alpha(\tau); \beta(z), \gamma(w)) \\ &\qquad = \Theta(\phi)(\tau; z, w)\chi_\tau(\alpha)^{-1}\chi_{z,w}(\beta, \gamma)^{-1}j(\alpha, \tau)^{-k}j(\beta, z)^{-k}j(\gamma, w)^{-k}.\end{aligned}$$

More generally, for general $\alpha \in SL_2(F)$, we have

$$\Theta(\phi)(\alpha(\tau); z, w)j(\alpha, \tau)^k = |D|^{-1}\Theta(\phi^* \circ \alpha) = \Theta(\Phi),$$

where $\phi^* \circ \alpha(u) = \phi^*(\alpha u)$ and $\Phi\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (\phi^* \circ \alpha)^*\left(\begin{smallmatrix} -a & -b \\ c & d \end{smallmatrix}\right)$. Similarly, for $(\beta, \gamma) \in SL_2(F)$, we have

$$\Theta(\phi)(\tau; z, w)j(\beta, z)^k j(\gamma, w)^k = \Theta(\phi \circ (\beta, \gamma)),$$

where $\phi \circ (\beta, \gamma)(u) = \phi(\beta u \gamma^{-1})$.

Proof. Since the argument is similar, we prove the formula in details for the action on τ. Write $\Gamma = \Gamma^\tau(\phi^*)$. We use the expression $\Theta(\phi) = |D|^{-1}\Theta(\phi^*)$. By (2.15), we have

$$\frac{|[\gamma^{-1}\ell; \tau_\sigma, w_\sigma]|^2}{\eta(\tau_s)} = \frac{|[\ell; \gamma(\tau_\sigma), w_\sigma]|^2}{\eta(\gamma(\tau_s))}, \quad [\gamma^{-1}\ell; \tau, w]^k = [\ell; \gamma(\tau), w]^k j(\gamma, \tau)^k.$$

Then, up to $y^{k+I}\mathbf{e}_F(\det(\ell)z)$ (independent of τ), $\Theta(\phi^*)$ is the sum of the following terms over $\ell \in \Gamma\backslash M_2(F)$ and $\gamma \in \Gamma$:

$$\chi_\tau(\gamma)\phi^*(\ell)Y_\ell(\gamma(\tau))j(\gamma, \tau)^k,$$

where $Y_\ell(\tau) = [\ell; \tau, w]^k \exp(-\pi\sum_\sigma \frac{y_\sigma}{t_\sigma}\frac{|[\ell;\tau_\sigma,w_\sigma]|^2}{\eta_\sigma(\tau_\sigma)})$. Thus we need to prove the automorphic property with respect to τ for

$$f(\tau) = \sum_{\gamma \in \Gamma/\Gamma_\ell} \chi_\tau(\gamma)Y_\ell(\gamma(\tau))j(\gamma, \tau)^k,$$

where $\Gamma_\ell \subset \Gamma$ is the stabilizer of ℓ. We see

$$\begin{aligned}f(\alpha(\tau)) &= \sum_{\gamma \in \Gamma/\Gamma_\ell} \chi_\tau(\gamma)Y_\ell(\gamma\alpha(\tau))j(\gamma, \alpha(\tau))^k \\ &= \sum_{\gamma \in \Gamma/\Gamma_\ell} \chi_\tau(\gamma)Y_\ell(\gamma\alpha(\tau))j(\gamma\alpha, \tau)^k j(\alpha, \tau)^{-k} \overset{\gamma\alpha\mapsto\gamma}{=} \chi_\tau(\alpha)^{-1}f(\tau)j(\alpha, \tau)^{-k}.\end{aligned}$$

This shows the first assertion for τ. As for the assertion with respect to (z,w), we argue similarly looking into the terms of $\Theta(\phi)$.

For the action of general α, the argument is similar for $\Theta(\phi^*)$. To return to $\Theta(\phi)$, we need to use the Fourier inversion formula $(\phi^*)^*\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \phi\left(\begin{smallmatrix} -a & -b \\ c & d \end{smallmatrix}\right)$. We leave the details to the attentive readers. □

3. q–Expansion of Shimura series

The Shimura series for $GL(2)\times GL(2)$ is defined for $0 < k \in \mathbb{Z}[I]$ and $0 \le m \in \mathbb{Z}[I]$ in [Sh2] II (4.11) by

$$(3.1)\quad H(z,w;s) = H_{k,m}(z,w;s;\phi^{(\infty)},f)$$
$$= [U] \sum_{0\neq\alpha\in M_2(F)/U} \phi^{(\infty)}(\alpha)a(-\det(\alpha),f)|\det(\alpha)|^m[\alpha;z,w]^{-k}\left|[\alpha;z,w]\right|^{-2sI}$$

for $(z,w)\in\mathfrak{H}^I\times\mathfrak{H}^I$. When $m=0$, we simply write H_k for $H_{k,0}$. The positivity of k means that $k\ge 0$ and $k_\sigma > 0$ for at least one $\sigma\in I$. Here f is a Hilbert modular form given by the Fourier expansion: $\sum_{\xi\in F} a(\xi,f)\mathbf{e}_F(\xi\tau)$ for $\tau\in\mathfrak{H}^I$ of weight ℓ ($\mathbf{e}_F(\xi\tau) = \exp(2\pi i\sum_\sigma \xi^\sigma\tau_\sigma)$) with $a(\xi,f)=0$ if $\xi^\sigma<0$ for some $\sigma\in I$, U is a subgroup of finite index of the group $O_+^\times$ of all totally positive units for which each term of the above sum is invariant, $[U]=[O_+^\times : U]^{-1}$ and $\phi^{(\infty)} : M_2(F_{\mathbb{A}^{(\infty)}})\to\mathbb{C}$ is a locally constant compactly supported function (a Schwartz-Bruhat function). To have invariance of the terms under the unit group U, we need to assume

$$(3.2)\quad k-\ell-2m = [k-\ell-2m]I\ \ (I=\sum_{\sigma\in I}\sigma)\ \text{ for an integer } [k-\ell-2m].$$

The series (3.1) converges absolutely and locally uniformly with respect to all variables s,z,w if

$$(3.3)\qquad \mathrm{Re}(s) > n+2+2\theta(f)-[k-\ell-2m]$$

as was shown in [Sh2] I Proposition 5.1 and Theorem 5.2, where $\theta(f)=-1$ when f is a constant, and otherwise, $\theta(f)=\theta\ge -\frac{1}{2}$ with $|a(\xi,f)\xi^{-\ell/2}| = O(|N(\xi)|^\theta)$ for the norm map $N=N_{F/\mathbb{Q}}$. This series is a generalization of Eisenstein series, because if we take $f=1$ (so $\ell=0$ and $m=0$), the series gives an Eisenstein series for $GL(2)\times GL(2)$ over F.

We are going to compute the Fourier expansion of the Shimura series. We summarize here how we proceed. We have already computed the Fourier expansion of $\Theta(\phi)(\tau;z,w)$ with respect to z, and it is equal to $|D|^{-1}\Theta(\phi^*)(z;\tau,w)$ for the partial Fourier transform ϕ^* of ϕ. By the integral expression of the series given in [Sh2] I Section 7, the series (actually its complex conjugate) is the Rankin-Selberg convolution product of $\Theta(\phi)$ and f with respect to the variable

τ. Since integration with respect to τ preserves Fourier expansion of $\Theta(\phi)$ with respect to z, what we need to compute is

$$\int_{\Gamma\backslash\mathfrak{H}^I} \Theta(\phi^*)(z;\tau,w)f(\tau)E(\tau;0)d\mu(\tau)$$

for the invariant measure $d\mu(\tau)$ for a suitable holomorphic Eisenstein series $E(\tau;0)$. This has been actually done, though without referring the result as the Fourier expansion of the series $H_k(z,w;0)$, in [Sh2] II Proposition 5.1 (replacing $f(w)$ and variable w there by $E(\tau;0)f(\tau)$ and τ). We recall the integral expression in Subsection 3.1 and the computation of Proposition 5.1 in [Sh2] II in Subsection 3.2. We shall do this to formulate our result in a manner optimal for our later use.

3.1. Integral expression. Let Γ be a congruence subgroup of $SL_2(F)$ which leaves $\theta_k(\tau;z,w;\phi^{(\infty)})$ and f fixed; thus, $\Gamma\subset\Gamma^\tau(\phi^*)$. The stabilizer Γ_∞ of the infinity cusp has the following canonical exact sequence:

$$\begin{array}{ccccccc} 0\to & \mathfrak{a} & \longrightarrow & \Gamma_\infty & \longrightarrow & U & \to 1 \\ & a & \mapsto & \left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right) & & & \\ & & & \left(\begin{smallmatrix}\epsilon & a\\ 0 & \epsilon^{-1}\end{smallmatrix}\right) & \mapsto & \epsilon & \end{array} \tag{3.4}$$

for a fractional ideal $\mathfrak{a}$ and a subgroup $U\subset O^\times$ of finite index. By shrinking Γ a little, we may assume that $U\subset O_+^\times$. We recall the integral expression of the Shimura series involving Siegel's theta series given in [Sh2] I (7.2) and II (6.5b):

$$[U]N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{F^\times_{\infty+}/U^2}\left(\int_{F_\infty/\mathfrak{a}}\Theta(\phi)d^mf(\tau)d\xi\right)\eta^{(s-1)I}d^\times\eta, \tag{3.5}$$

where $d^m=\prod_\sigma\left(\frac{1}{2\pi i}\frac{\partial}{\partial\tau_\sigma}\right)^{m_\sigma}$, $\phi(u)=\phi^{(\infty)}(u^{(\infty)})\Psi_k^{z,w,\tau}(u_\infty)$ and $d^\times\eta$ is the multiplicative Haar measure given by $\otimes_\sigma(\eta_\sigma^{-1}d\eta_\sigma)$. We first compute the inner integral: if $\mathrm{Re}(s)\gg 0$,

$$\begin{aligned} &N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{F_\infty/\mathfrak{a}}\Theta(\phi)d^mf(\tau)d\xi= \\ &\sum_{\alpha\in V,\beta\in F}\phi^{(\infty)}(\alpha)a(\beta,f)|\beta|^m[\alpha;z,w]^k\exp(-\pi(2\beta+P_{z,w}(\alpha))\eta)\eta^{k+I}\delta_{\det(\alpha),-\beta},\end{aligned}$$

because for $C=N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}$

$$C\int_{F_\infty/\mathfrak{a}}\mathbf{e}_F((\det(\alpha)+\beta)\xi)d\xi=\delta_{\det(\alpha),-\beta}=\begin{cases}1 & \text{if } \det(\alpha)=-\beta,\\ 0 & \text{otherwise.}\end{cases}$$

To compute the outer integral, when $\det(\alpha)=-\beta$, we note from (2.2) that $P_{z,w}[\alpha]=S[\alpha]+\frac{|[\alpha;z,w]|^2}{yt}$ for $S[\alpha]=2\det(\alpha)$ and that

$$\exp(-\pi(2\beta+P_{z,w}(\alpha))\eta)=\exp(\pi(2\det(\alpha)-P_{z,w}(\alpha))\eta)=\exp(-\pi\frac{|[\alpha;z,w]|^2}{yt}\eta).$$

Here we have integrated term wise (with respect to) the summation of Θ and the Fourier expansion of f, which can be justified by the locally uniform and absolute convergence of the Fourier expansions of Θ and f as long as the resulting series is absolutely convergent (Lebesgue's term wise integration theorem). The convergence of the series is guaranteed by (3.3) if $\mathrm{Re}(s)$ is large. Again spreading the integral $\int_{F^\times_{\infty+}/U^2}\sum_{\epsilon\in U}\Phi(\varepsilon^2\eta)d^\times\eta$ to the whole $F^\times_{\infty+}$ for $\Phi(\eta)=\exp(-\pi\frac{|[\alpha;z,w]|^2\eta}{yt})$, we see that (as long as the latter integral is absolutely convergent) the integral (3.5) is equal to

$$\begin{aligned}(3.6)\qquad &[U]\sum_{\alpha\in V/U}\phi^{(\infty)}(\alpha)a(-\det(\alpha),f)|\det(\alpha)|^m[\alpha;z,w]^k\\ &\qquad\qquad\times\int_{F^\times_{\infty+}}\exp(-\pi\mathrm{Tr}(\frac{|[\alpha;z,w]|^2}{yt}\eta))\eta^{k+sI}d^\times\eta.\end{aligned}$$

We know

$$\begin{aligned}&[\alpha;z,w]^k\int_{F^\times_{\infty+}}\exp(-\pi\frac{|[\alpha;z,w]|^2}{yt}\eta)\eta^{k+sI}d^\times\eta\\ &\quad=2^{1-[F:\mathbb{Q}]}\pi^{-k-sI}\Gamma_F(k+sI)y^{k+sI}t^{k+sI}[\alpha;z,w]^k|[\alpha;z,w]|^{-2s-2k}\\ &\qquad=2^{1-[F:\mathbb{Q}]}\pi^{-k-sI}\Gamma_F(k+sI)y^{k+sI}t^{k+sI}[\alpha;\overline{z},\overline{w}]^{-k}|[\alpha;z,w]|^{-2s},\end{aligned}$$

where $\Gamma_F(k)=\prod_\sigma\Gamma(k_\sigma)$, and as for the factor $2^{1-[F:\mathbb{Q}]}$, see [LFE] page 271. Thus we conclude

$$\begin{aligned}&2^{1-[F:\mathbb{Q}]}\pi^{-k-sI}\Gamma_F(k+sI)y^{k+sI}t^{k+sI}\overline{H_{k,m}(z,w;\overline{s};\overline{\phi}^{(\infty)},f_c)}\\ &\qquad=[U]N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{F^\times_{\infty+}/U^2}\int_{F_\infty/\mathfrak{a}}\Theta(\phi)d^mf(\tau)\eta^{(s-1)I}d\xi d^\times\eta,\end{aligned}$$

where $f_c(z)=\overline{f(-\overline{z})}$. In other words, by taking complex conjugation, we have, for $\widetilde{\phi}=\overline{\phi}^{(\infty)}\phi_\infty$,

$$\begin{aligned}(3.7)\quad &2^{1-[F:\mathbb{Q}]}\pi^{-k-sI}\Gamma_F(k+sI)y^{k+sI}t^{k+sI}H_{k,m}(z,w;s;\phi^{(\infty)},f)\\ &\qquad=[U]N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{F^\times_{\infty+}/U^2}\int_{F_\infty/\mathfrak{a}}\overline{\Theta(\widetilde{\phi})}\,\overline{d^mf_c(\tau)}\eta^{(s-1)I}d\xi d^\times\eta.\end{aligned}$$

The above formula (3.7) is only valid for s satisfying (3.3). However, by Rankin-Selberg convolution, we can analytically continue the function H to a meromorphic function on the whole s–plane (see [Sh2] I Section 7). We recall the process. We first assume that $m=0$. Since $\Gamma_\infty\backslash\mathfrak{H}^I\cong(F^\times_{\infty+}/U^2)\times(F_\infty/\mathfrak{a})$, we can rewrite the above integral as

$$\begin{aligned}
&2^{1-[F:\mathbb{Q}]}\pi^{-k-sI}\Gamma_F(k+sI)y^{k+sI}t^{k+sI}H_k(z,w;s;\phi^{(\infty)},f)\\
&=[U]N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{\Gamma_\infty\backslash\mathfrak{H}^I}\overline{\Theta(\widetilde{\phi})}\overline{f_c(\tau)}\eta^{sI}d\mu(\tau)\\
(3.8)\qquad&=N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{\Gamma\backslash\mathfrak{H}^I}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\left(\overline{\Theta(\widetilde{\phi})}\overline{f_c(\tau)}\eta^{sI}\right)\circ\gamma d\mu(\tau)\\
&=N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}\int_{\Gamma\backslash\mathfrak{H}^I}\overline{\Theta(\widetilde{\phi})}\overline{f_c(\tau)E(\tau;\overline{s})}d\mu(\tau),
\end{aligned}$$

where $d\mu(\tau)$ is the invariant measure $\eta^{-2I}d\xi d\eta$ on $\mathfrak{H}^I$, and by Proposition 2.3,

$$(3.9)\qquad E(\tau;s)=E_{k-\ell}(\tau;s)=\eta^{sI}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}j(\gamma,\tau)^{\ell-k}|j(\gamma,\tau)|^{-2sI}.$$

In general, if $m\neq 0$, we use the formula (see [Sh2] I (1.16a)):

$$d^m=\sum_{0\leq j\leq m}\binom{m}{j}\frac{\Gamma_F(\ell+m)}{\Gamma_F(\ell+j)}(4\pi\eta)^{j-m}\delta_\tau^j(\ell)$$

for $\delta_\tau^\sigma(j)=\frac{1}{2\pi i}\left(\frac{j}{\tau_\sigma-\overline{\tau}_\sigma}+\frac{\partial}{\partial\tau_\sigma}\right)$ and

$$\delta_\tau^j(\ell)=\prod_\sigma\left(\delta_\tau^\sigma(\ell_\sigma+2j_\sigma-2)\cdots\delta_\tau^\sigma(\ell_\sigma+2)\delta_\tau^\sigma(\ell_\sigma)\right).$$

The binomial coefficients $\binom{m}{j}$ is the product of individual ones $\binom{m_\sigma}{j_\sigma}$ over $\sigma\in I$. Since $\delta_\tau^j(\ell)$ preserves automorphy (but not holomorphy), we can write d^mf_c as a linear combination of $\delta_\ell^u f_c$, which is an automorphic form of weight $\ell+2u$ on the same Γ, and therefore the above computation still works.

The integral (3.8) (in general for $m\geq 0$) is convergent for all $s\in\mathbb{C}$ except for s giving rise to a singularity of the Eisenstein series, because $\Theta(\phi)$ for $k>0$ does not have constant term at any cusp; so, it is rapidly decreasing. Thus the integral of (3.8) converges absolutely for any slowly increasing automorphic form $f(\tau)$ as long as $E(\tau;s)$ is finite. This is the proof of the analytic continuation given in [Sh1] Section 13. This proof works well even when $k=0$ for cusp forms f.

3.2. Computation of q–expansion. We assume that $m=0$. We are going to compute the Fourier expansion of $\int_{\Gamma\backslash\mathfrak{H}^I}\Theta(\phi)g(\tau)d\mu(\tau)$ for an eigenform $g(\tau)$ of Laplacian Δ_σ: $\Delta_\sigma g=(s_\sigma^2-\frac{1}{4})g$ ($s_\sigma\in\mathbb{C}$) for all $\sigma\in I$, where $\Delta_\sigma=\eta_\sigma^2\left(\frac{\partial^2}{\partial\xi_\sigma^2}+\frac{\partial^2}{\partial\eta_\sigma^2}\right)$. We assume that $(\Theta(\phi)g)(\gamma(\tau))=(\Theta(\phi)g)(\tau)$ for all $\gamma\in\Gamma$. By (2.2), $\Theta(\phi)=|D|^{-1}\Theta((\phi)^*)$ is the sum of the following terms:

$$\prod_\sigma y_\sigma^{k_\sigma+1}[\alpha^\sigma;\tau_\sigma,w_\sigma]^{k_\sigma}\mathbf{e}\left(\det(\alpha^\sigma)z_\sigma+\frac{iy_\sigma}{2\eta_\sigma t_\sigma}|[\alpha^\sigma;\tau_\sigma,w_\sigma]|^2\right).$$

By (2.15), we have, for $\gamma \in \Gamma$,

$$\begin{aligned}\log(Y_\sigma(\tau_\sigma)) &= \frac{-\pi y_\sigma}{\eta_\sigma t_\sigma}||[(\gamma\alpha)^\sigma;\tau_\sigma,w_\sigma]||^2\\ &= \frac{-\pi y_\sigma}{\eta_\sigma t_\sigma}||[\alpha^\sigma;\gamma^{-1}(\tau_\sigma),w_\sigma]||^2|j(\gamma^{-1},z)|^2\\ &= \frac{-\pi y_\sigma}{\mathrm{Im}(\gamma^{-1}(\tau_\sigma))t_\sigma}||[\alpha^\sigma;\gamma^{-1}(\tau_\sigma),w_\sigma]||^2.\end{aligned}$$

This shows

(3.10)
$$\begin{aligned}&y^{-(k+I)}\int_{\Gamma\backslash\mathfrak{H}^I}\Theta(\phi)g(\tau)d\mu(\tau)\\ &= \sum_{\alpha\in\Gamma\backslash M_2(F)}\mathbf{e}_F(\det(\alpha)z)\phi^{(\infty)}(\alpha)\int_{\Gamma\backslash\mathfrak{H}^I}\sum_{\gamma\in\Gamma_\alpha\backslash\Gamma}[\alpha;\gamma(\tau),w]^k g(\gamma(\tau))Y(\gamma(\tau))d\mu\\ &= \sum_{\alpha\in\Gamma\backslash M_2(F)}\mathbf{e}_F(\det(\alpha)z)\phi^{(\infty)}(\alpha)\int_{\Gamma_\alpha\backslash\mathfrak{H}^I}[\alpha;\tau,w]^kY(\tau)g(\tau)d\mu,\end{aligned}$$

where $\Gamma_\alpha = \{\gamma \in \Gamma|\gamma\alpha = \alpha\}$ and $Y(z) = \prod_\sigma \mathbf{e}(Y(z_\sigma))$. If $\det(\alpha) \neq 0$, then $\Gamma_\alpha = \{1\}$.

We first compute the general term: $\int_{\mathfrak{H}^I}[\alpha;\tau,w]^kY(\tau)g(\tau)d\mu(\tau)$. For that, we recall [Sh2] Lemma 5.2 and the discussion after the lemma:

Lemma 3.1. *Let $\alpha \in GL_2(F)$. Let $P(\tau,w) = \exp(-\sum_\sigma \frac{u_\sigma}{\eta_\sigma t_\sigma}||[\alpha,\overline{\tau}_\sigma,w_\sigma]||^2)$ for $\tau, w \in \mathfrak{H}^I$ with $0 < u_\sigma \in \mathbb{R}$. Assume that the integral $\int_{\mathfrak{H}^I}P(\tau,w)g(\tau)d\mu(\tau)$ is convergent. If $\Delta_\sigma g = (s_\sigma^2 - \frac{1}{4})g$ and $\det(\alpha)$ is totally positive, we have*

$$\begin{aligned}(3.11)\quad &\int_{\mathfrak{H}^I}P(\tau,w)g(\tau)d\mu(\tau)\\ &= \pi^{[F:\mathbb{Q}]/2}(\det(\alpha)u^{-1})^{I/2}\exp(-2\sum_\sigma\det(\alpha^\sigma)u_\sigma)K(\det(\alpha)u,s)g|_k\alpha(w)\end{aligned}$$

for the modified Bessel function:

$$K(u,s) = \prod_\sigma\int_0^\infty \exp(-u_\sigma(x_\sigma + x_\sigma^{-1}))x_\sigma^{s_\sigma-1}dx_\sigma,$$

where $g|_k\alpha(w) = \det(\alpha)^{k-I}g(\alpha(w))j(\alpha,z)^{-k}$. If $\det(\alpha)$ is not totally positive and g is holomorphic, the integral (3.11) vanishes, as long as it converges.

By the above lemma, taking $g = f$ (so, $g = f$ is holomorphic), only non-trivial case is when $\det(\alpha)$ is totally negative, and noting the fact that $K(u,\frac{1}{2}) =$

$\pi^{[F:\mathbb{Q}]/2}u^{-I/2}\exp(-2\sum_\sigma u_\sigma)$, we have

$$\begin{aligned}
&\int_{\mathfrak{H}^I}\exp(-\pi\sum_\sigma\frac{y_\sigma}{\eta_\sigma(\tau_\sigma)t_\sigma}|[\alpha^\sigma;\tau_\sigma,w_\sigma]|^2)[\alpha;\tau,w]^k f(\tau)d\mu(\tau)\\
&\overset{\tau\mapsto\alpha(\overline{\tau})}{=}\int_{\mathfrak{H}^I}\exp(-\pi\sum_\sigma\frac{y_\sigma}{|\eta_\sigma(\alpha(\tau_\sigma))|t_\sigma}|[\alpha^\sigma;\alpha(\overline{\tau}_\sigma),w_\sigma]|^2)[\alpha;\alpha(\overline{\tau}),w]^k f(\tau)d\mu(\tau)\\
&\qquad\overset{(2.15)}{=}\int_{\mathfrak{H}^I}\exp(-\pi\sum_\sigma\frac{|\det(\alpha^\sigma)|y_\sigma}{\eta_\sigma(\tau_\sigma)t_\sigma}|[1;\overline{\tau}_\sigma,w_\sigma]|^2)\\
&\qquad\qquad\times[1;\overline{\tau},w]^k\det(\alpha)^k j(\alpha,\overline{\tau})^{-k}f(\alpha(\overline{\tau}))d\mu(\tau)\\
&\qquad\overset{s_\sigma=1/2}{=}(-1)^{[F:\mathbb{Q}]}(-2i)^k t^k y^{-I}\exp(-4\pi\sum_\sigma|\det(\alpha^\sigma)|y_\sigma)f|_k\alpha(\overline{w}).
\end{aligned}$$

If $\alpha\neq 0$ and $\det(\alpha)=0$, then Γ_α is equal to $\Gamma\cap\beta\mathcal{U}(F)\beta^{-1}$ for $\beta\in GL_2(F)$. By a variable change, we may assume that $\alpha=\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. Then $\Gamma_\alpha=\Gamma\cap\mathcal{U}(F)$, and we have an isomorphism: $\mathfrak{a}\cong\Gamma_\alpha$ by $\mathfrak{a}\ni a\mapsto\left(\begin{smallmatrix}1&a\\0&1\end{smallmatrix}\right)$, where $\mathfrak{a}$ is a fractional ideal of F. In this case, $[\alpha;\tau,w]=-w$. We then have

$$\begin{aligned}
(3.12)\quad&\int_{\Gamma_\alpha\backslash\mathfrak{H}^I}[\alpha;\tau,w]^k Y(\tau)f(\tau)d\mu(\tau)\\
&\qquad=\int_{F^\times_{\infty+}}[\alpha;\tau,w]^k Y(\tau)\int_{F_\infty/\mathfrak{a}}f(\xi+i\eta)d\xi\eta^{-2I}d\eta\\
&=N(\mathfrak{a})\sqrt{|D|}a(0,f)\int_{F^\times_{\infty+}}(-w)^k\exp(-\pi\sum_\sigma\frac{y_\sigma}{\eta_\sigma t_\sigma}|w|^2)\eta^{-2I}d\eta\\
&\overset{\eta\mapsto\eta^{-1}}{=}N(\mathfrak{a})\sqrt{|D|}a(0,f)(-w)^k\int_{F^\times_{\infty+}}\exp(-\pi\sum_\sigma\frac{\eta_\sigma y_\sigma}{t_\sigma}|w|^2)d\eta\\
&\qquad\qquad=\pi^{-1}N(\mathfrak{a})\sqrt{|D|}a(0,f)(-w)^k\frac{t_\sigma}{y_\sigma}|w|^{-2I},
\end{aligned}$$

where $f(\tau)=\sum_{\delta\in F}a(\delta,f)\mathbf{e}_F(\delta\tau)$.

Thus we obtain the following version of [Sh2] II Proposition 5.1 for $B=M_2(F)$:

Theorem 3.2. *Suppose that f is a holomorphic cusp form of weight $k>0$. Let Γ be a congruence subgroup of $SL_2(F)$ fixing $f(\tau)\Theta(\phi)(\tau)$. Then we have*

$$\begin{aligned}
&(-1)^{[F:\mathbb{Q}]}|D|\int_{\Gamma\backslash\mathfrak{H}^I}\Theta(\phi)(\tau;z,w)f(\tau)d\mu(\tau)\\
&\qquad=(-2i)^k t^k y^k\sum_{\alpha\in\Gamma\backslash M_2(F);\det(\alpha)\ll 0}\phi^{*(\infty)}(\alpha)\mathbf{e}_F(\det(\alpha)\overline{z})f|_k\alpha(\overline{w}),
\end{aligned}$$

where $f|\alpha(\overline{w})=\det(\alpha)^{k-I}f(\alpha(\overline{w}))j(\alpha,\overline{w})^{-k}$ for $\alpha\in M_2(F)$ with totally negative determinant.

Taking complex conjugate of the above expansion and replacing the pair (ϕ,f) in the above theorem by $(\widetilde{\phi}=\overline{\phi}^{(\infty)}\phi_\infty,f_cE(w;0))$, we get

Corollary 3.3. *We have, if f is a holomorphic cusp form of weight ℓ with $k - \ell = [k - \ell]I$ for an integer $[k - \ell] > 0$,*

$$H_k(z, w; 0; \phi^{(\infty)}, f) = 2^{[F:\mathbb{Q}]-1}[U]|D|^{-3/2}N(\mathfrak{a})^{-1}\frac{(2\pi i)^k}{\Gamma_F(k)} \times \sum_{\alpha\in\Gamma\backslash M_2(F);\det(\alpha)\gg 0} \phi^{*(\infty)}(\epsilon\alpha)\mathbf{e}_F(\det(\alpha)z)(fE_{k-\ell}(w;0))|_k\alpha(w),$$

where $\epsilon = \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$.

We can apply the above theorem to the following integral:

$$\int_{\Gamma\backslash\mathfrak{H}^I} \Theta(\widetilde{\phi})(s-1)E_{k-\ell}(\tau; s)\overline{f}_c(\tau)d\mu(\tau)$$

at $s = 1$ when $k = \ell$, because $E(\tau, s)$ has a simple pole at $s = 1$ whose residue is a constant $c_\Gamma \neq 0$ (independent of τ). We then have

Corollary 3.4. *We have, if f is a holomorphic cusp form of weight k,*

$$\mathrm{Res}_{s=1}H_k(z, w; s; \phi^{(\infty)}, f) = c_\Gamma(-i)^{[F:\mathbb{Q}]}2^{-1}[U]|D|^{-3/2}N(\mathfrak{a})^{-1}\frac{(2\pi i)^{k+I}}{\Gamma_F(k+I)} \times y^{-I}t^{-I} \sum_{\alpha\in\Gamma\backslash M_2(F);\det(\alpha)\gg 0} \phi^{*(\infty)}(\epsilon\alpha)\mathbf{e}_F(\det(\alpha)z)f|_k\alpha(w),$$

where $c_\Gamma = \mathrm{Res}_{s=1}E(w; s)$.

For the exact value of the constant $c_\Gamma \neq 0$, see [H99] (RES3) page 173.

4. Evaluation at CM points

We follow [Sh2] I Sections 5 and 8 to write down the evaluation of the Shimura series at some special CM points in terms of Rankin-Selberg L–functions.

4.1. CM points. We fix the "identity" embedding $(\sigma_0 : F \to \overline{\mathbb{Q}}) \in I$. Let (z_0, w_0) be a point in $\mathfrak{H}^I$ such that $M = F[z_{0,\sigma_0}]$ and $L = F[w_{0,\sigma_0}]$ are totally imaginary quadratic extensions of F (so, CM fields). Let $Y = M \otimes_F L$, and we embed Y into $M_2(F) \otimes_F M_2(F) = M_4(F)$ by $(a, b) \mapsto \rho_M(a) \otimes \rho_L(b)$ with

$$\left(\begin{smallmatrix} z_0 a\\ a\end{smallmatrix}\right) = \rho_M(a)\left(\begin{smallmatrix} z_0\\ 1\end{smallmatrix}\right) \quad\text{and}\quad \left(\begin{smallmatrix} w_0 b\\ b\end{smallmatrix}\right) = \rho_L(b)\left(\begin{smallmatrix} w_0\\ 1\end{smallmatrix}\right).$$

We see easily that $\rho_M(a)^\iota = \rho_M(a^c)$ and $\rho_L(b)^\iota = \rho_L(b^c)$ for complex conjugation c. We regard $V = M_2(F)$ as a Y–module for the multiplicative semi-group Y via $\rho_M \otimes \rho_L$; in other words, $(a, b)v = \rho_M(a)v\rho_L^\iota(b)$.

We have four distinct Y–eigenvectors $p(z_{0,\sigma}, w_{0,\sigma})$, $p(z_{0,\sigma}, \overline{w}_{0,\sigma})$, $p(\overline{z}_{0,\sigma}, w_{0,\sigma})$ and $p(\overline{z}_{0,\sigma}, \overline{w}_{0,\sigma})$ in $M_2(\mathbb{C}) = V \otimes_{F,\sigma} \mathbb{C}$, whose eigenvalues of (a, b) are $(a^{\widetilde{\sigma}}b^{\widetilde{\sigma}c})$, $(a^{\widetilde{\sigma}}b^{\widetilde{\sigma}})$, $(a^{\widetilde{\sigma}c}b^{\widetilde{\sigma}c})$ and $(a^{\widetilde{\sigma}c}b^{\widetilde{\sigma}})$, respectively, for an extension $\widetilde{\sigma}$ of σ to the composite LM. Since $V \otimes_{F,\sigma} \mathbb{C}$ is free of rank 1 over $Y_\sigma = Y \otimes_{F,\sigma} \mathbb{C}$, $V = M_2(F)$ is free of rank 1 over Y (because $\mathbb{C}$ is faithfully flat over F). Thus we find $v \in V$ such that $V = Yv$. Then $S_Y : (y, y') \mapsto S(yv, y'v)$ gives a non-degenerate symmetric F–bilinear form on Y with $S_Y(yy',y'')=S_Y(y',y^cy'')$, and we can write $S_Y(x,y)=\mathrm{Tr}_{Y/F}(\delta xy^c)$ for $\delta\in Y^\times$ with $\delta^c=\delta$.

Suppose now that $L=M$. Then $Y\cong M\oplus Y_0$ with $Y_0\cong M$, the first projection to M is given by $a\otimes b\mapsto ab^c$ and the second to Y_0 is given by $a\otimes b\mapsto ab$. Since c is an automorphism of M, $p(z,w)$ and $p(\overline{z}_{0,\sigma},\overline{w}_{0,\sigma})$ belongs to $Mv\otimes_{F,\sigma}\mathbb{C}\subset Y_\sigma v=V_\sigma$. The vectors $p(z_{0,\sigma},w_{0,\sigma})$ and $p(\overline{z}_{0,\sigma},\overline{w}_{0,\sigma})$ are orthogonal to $Y_0\otimes_{F,\sigma}\mathbb{C}$. In other words,

$$Y_0=\left\{y\in Y\middle|\widetilde{\sigma}(y)=c\widetilde{\sigma}(y)=0\ \text{ for all }\sigma\in I\right\}.$$

Thus $\Sigma=\sum_{\sigma\in I}\widetilde{\sigma}$ gives rise to a CM type of M (with $\Sigma\sqcup\Sigma c$ giving all complex embeddings of M). This shows: writing $V\ni\alpha=av\oplus bv$ with $a\in M$ and $b\in Y_0$

$$\begin{aligned}[]
[\alpha^\sigma;z_{0,\sigma},w_{0,\sigma}]&=S(\alpha^\sigma,p(z_{0,\sigma},w_{0,w_0}))=S(av_\sigma,p(z_{0,\sigma},w_{0,w_0}))\\
&=S(v_\sigma,a^cp(z_{0,\sigma},w_{0,w_0}))=a^{\widetilde{\sigma}c}[v_\sigma;z_{0,\sigma},w_{0,\sigma}],\\
[\alpha;z_0,w_0]^{-k}\left|[\alpha;z_0,w_0]\right|^{-2sI}&=C^{-k\Sigma}|C^\Sigma|^{-2s}a^{-ck\Sigma}N(a)^{-s},
\end{aligned}\tag{4.1}$$

where $C=[v_\sigma;z_{0,\sigma},w_{0,\sigma}]$ and $N(a)$ is the absolute norm of $a\in M$. Here we have written $k\Sigma=\sum_{\sigma\in I}k_\sigma\widetilde{\sigma}$ and $ck\Sigma=\sum_{\sigma\in I}k_\sigma\widetilde{\sigma}c$.

Since $p(z_{0,\sigma},w_{0,\sigma})$ and $p(\overline{z}_{0,\sigma},\overline{w}_{0,\sigma})$ span (by the definition of $\mathcal{Y}(S)$ in Subsection 2.1) a scalar extension to $\mathbb{C}$ of a subspace on which S_σ is negative definite, S is totally positive definite on $W=Y_0v$, because every vector in W is orthogonal to $p(z_{0,\sigma},w_{0,\sigma})$ and $p(\overline{z}_{0,\sigma},\overline{w}_{0,\sigma})$. We write S_W for the restriction of S to W. By this fact, writing $\delta=-\delta_M\oplus\delta_0$ for $\delta_M\in M$ and $\delta_0\in Y_0$, then δ_M is a totally positive element of F; so, we may assume that $\delta_M=\frac{1}{2}$ by changing v if necessary. Similarly, we may choose $\delta_0=\frac{1}{2}$.

4.2. Special values of Shimura series. As we have explained already, we choose v as in previous subsection so that

$$S_Y((a,b),(a',b'))=\frac{1}{2}\mathrm{Tr}_{M/F}(-aa'^c+bb'^c).\tag{4.2}$$

We see, supposing

$$\phi^{(\infty)}(u)=\phi_M\otimes\phi_0\tag{4.3}$$

for functions $\phi_M:Mv\to\mathbb{C}$ and $\phi_0:Y_0v\to\mathbb{C}$,

$$\begin{aligned}
&C^{k\Sigma}|C^\Sigma|^{2s}H_k(z_0,w_0;s;\phi^{(\infty)},f)\\
&\qquad=[U]\sum_{\alpha\in M/U}\phi_M(\alpha v)\sum_{\beta\in Y_0/U}\phi_0(\beta v)a(\alpha\alpha^c-\beta\beta^c,f)\alpha^{-ck\Sigma}N(\alpha)^{-s},
\end{aligned}$$

where C is as in (4.1). We now define $\theta(\phi_0)=\sum_{\beta\in Y_0}\phi_0(\beta v)\mathbf{e}_F(\beta\beta^cz)$. Then for $f'(z)=\theta(\phi_0)f(z)=\sum_{\xi\in F}a(\xi,f')\mathbf{e}_F(\xi z)$, we have

$$a(\xi,f')=\sum_{\beta\in Y_0/U}a(\xi-\beta\beta^c,f)\phi_0(\beta v),$$

which is a finite sum because $\{x \in Y_0 \otimes_F \mathbb{R} | x^\sigma x^{\sigma c} < \xi^\sigma \ \forall \sigma\}$ is a compact set. Thus we have, under (4.2) and (4.3)

$$\begin{aligned} C^{k\Sigma}|C^\Sigma|^{2s} H_k(z_0, w_0; s; \phi^{(\infty)}, f) \\ = [U] \sum_{\alpha \in M/U} \phi_M(\alpha v) a(\alpha\alpha^c, f')\alpha^{-ck\Sigma} N(\alpha)^{-s}. \end{aligned} \tag{4.4}$$

In general, $\phi^{(\infty)}|\det^m|$ is a constant linear combination of the functions satisfying (4.3); so, $H(z_0, w_0; s)$ is a linear combination of the series of the above type. The series (4.4) is the Rankin convolution of f' and the theta series $\theta(\phi_{k,M})$ of the norm form of M for $\phi_{k,M}(\alpha) = \alpha^{k\Sigma}\phi_M(\alpha v)$ (see (4.9)).

4.3. An explicit formula of Petersson inner product. For a given theta series $\theta_M(\phi)$ of weight $k + I$ of a CM field M/F, we are going to write down the inner product $\langle \theta_M(\phi), f'_c \rangle$ for a special value of a modular form on $GL(2) \times GL(2)$, taking $f' = f\theta_M(\phi')$ for another theta series $\theta_M(\phi')$ of weight I of M. Here $f'_c(z) = \overline{f'(-\overline{z})}$; so, f'_c is a holomorphic modular form whose Fourier coefficients (at the infinity) are the complex conjugate of those of f'. The modular form is given by, up to an explicit constant,

$$\mathrm{Res}_{s=1} H_k(z, w; s; \phi' \otimes \phi^{(\infty)}, f).$$

We will later in Section 7 deduce from this the integrality of $\frac{\pi^{2k+2I}\langle g, \theta(\phi)\rangle}{\Omega^{2(k+I)}}$ for the period Ω of the Néron differential of the abelian variety of CM-type sitting at the evaluation point (z_0, w_0).

Let f and g be Hilbert modular forms on $\Gamma \subset SL_2(F)$ with Fourier expansion $f = \sum_{\xi \in F} a(\xi, f)\mathbf{e}_F(\xi\tau)$ and $g = \sum_{\xi \in F} a(\xi, g)\mathbf{e}_F(\xi\tau)$ for $z \in \mathfrak{H}^I$. We take the ideal $\mathfrak{a} \subset F$ and the unit group $U \subset O_+^\times$ as in (3.4). Let ℓ and κ be the weights of f and g respectively. We suppose that one of f and g is a cusp form so that $\overline{f}g$ is rapidly decreasing.

We let $\epsilon \in U$ act on $\mathfrak{H}^I$ by $\tau \mapsto \epsilon^2\tau$. Then $f(\epsilon^2\tau) = \epsilon^{-\ell}f(\tau)$ and $g(\epsilon^2\tau) = \epsilon^{-\kappa}g(\tau)$. Then the function $\overline{f}g(\tau)\eta^{(\ell+\kappa)/2}$ is U–invariant. We then consider

$$D(s; f, g) = [U^2]N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1} \int_{F_\infty/\mathfrak{a}} \int_{F^\times_{\infty+}/U^2} \overline{f}(\tau)g(\tau)\eta^{sI+(\ell+\kappa)/2} d\xi d^\times\eta. \tag{4.5}$$

We now assume that

$$\ell \equiv \kappa \mod 2\mathbb{Z}[I] + \mathbb{Z}I. \tag{4.6}$$

Thus we find $m \in \mathbb{Z}[I]$ such that $\ell - \kappa - 2m \in \mathbb{Z}I$. Replacing Γ by

$$\left\{\gamma \in \Gamma \big| (\overline{f}g\eta^{(\ell+\kappa)/2} \circ \gamma)(\tau) = (\overline{f}g\eta^{(\ell+\kappa)/2})(\tau) j(\gamma, \overline{\tau})^\ell j(\gamma, \tau)^\kappa |j(\gamma, \tau)^{-\ell-\kappa}|\right\}$$

if necessary, we have

$$\begin{aligned}(4.7)\quad &[U^2]^{-1}N(\mathfrak{a})\sqrt{|D|}D(s;f,g)\\ &=\int_{\Gamma\backslash\mathfrak{H}^I}\overline{f}(\tau)g(\tau)\eta^{\ell-m}E_{[\ell-\kappa-2m]I,m}(\tau;s+1-\frac{[\ell-\kappa-2m]}{2})d\mu(\tau),\end{aligned}$$

where

$$E_{nI,m}(\tau;s)=\eta^{sI}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\left(\frac{j(\gamma,\overline{\tau})}{j(\gamma,\tau)}\right)^m j(\gamma,\tau)^{-nI}|j(\gamma,\tau)|^{-2sI}.$$

When $m=0$, we write simply E_{nI} for $E_{nI,0}$ ($n\in\mathbb{Z}$). Since $E_{nI,m}(\tau;s)$ has meromorphic continuation on the whole s–plane as a slowly increasing function (outside its singularity), the above integral gives an analytic continuation of $D(s;f,g)$ to the whole complex s–plane. In particular if $\ell=\kappa$, the L–function $D(s;f,g)$ can have a pole at $s=0$ because in that case, we can choose $m=0$ and $E_0(\tau,s)$ has a simple pole at $s=1$ with a constant residue.

By the same calculation as in Subsection 3.1, we have

$$\begin{aligned}&2^{[F:\mathbb{Q}]-1}(4\pi)^{sI+(\ell+\kappa)/2}D(s;f,g)\\ (4.8)\quad &=[U^2]\Gamma_F(sI+(\ell+\kappa)/2)\sum_{0\ll\xi\in F^\times/U^2}\overline{a(\xi,f)\xi^{-\ell/2}}a(\xi,g)\xi^{-\kappa/2}N(\xi)^{-s}\end{aligned}$$

if $\mathrm{Re}(s)>\theta(f)+\theta(g)+1$ for $\theta(f)$ as in Section 3.

Let us recall the theta series defined below (4.4):

$$\theta(\phi_{k,M})=\sum_{a\in M}\phi_{k,M}(a)\mathbf{e}_F(aa^c\tau)$$

for $\phi_{k,M}(a)=a^{k\Sigma}\phi_M(a)$ as in (4.4). We compute $D(s;f'_c,\theta(\phi_{k,M}))$ for a cusp form f' of weight $\ell+I$:

$$\begin{aligned}&2^{[F:\mathbb{Q}]-1}\frac{(4\pi)^{sI+(\ell+k+2I)/2}}{\Gamma_F(sI+(\ell+k+2I)/2)}D(s;f'_c,\theta(\phi_{k,M}))\\ &=[U^2]\sum_{0\ll\xi\in F^\times/U^2}a(\xi,f')\xi^{-(\ell+I)/2}a(\xi,\theta(\phi_{k,M}))\xi^{-(k+I)/2}N(\xi)^{-s}\\ &=[U^2]\sum_{\alpha\in M^\times/U}\phi_M(\alpha)a(\alpha\alpha^c,f')\alpha^{k\Sigma}(\alpha\alpha^c)^{-(k+\ell+2I)/2}N(\alpha)^{-s}\\ &=[U^2]\sum_{\alpha\in M^\times/U}\phi_M(\alpha)a(\alpha\alpha^c,f')\alpha^{k\Sigma}(\alpha^{-k\Sigma}\alpha^{-kc\Sigma})N(\alpha)^{-s-1+(k-\ell)/2}\\ &=[U^2]\sum_{\alpha\in M^\times/U}\phi_M(\alpha)a(\alpha\alpha^c,f')\alpha^{-kc\Sigma}N(\alpha)^{-s-1+(k-\ell)/2}\end{aligned}$$

From this, we get under the notation and the assumption of (4.4)

$$\begin{aligned}(4.9)\quad & 2^{1-[F:\mathbb{Q}]}C^{k\Sigma}|C^{\Sigma}|^{2s}(4\pi)^{-sI-k}\Gamma_F(sI+k)H_k(z_0,w_0;s;\phi^{(\infty)},f)\\ &\qquad = [U:U^2]D(s-1+\frac{[k-\ell]}{2};f'_c,\theta(\phi_{k,M})),\end{aligned}$$

where ℓ is the weight of f (so, weight of f'_c is $\ell+I$). Note here that $[U:U^2]=2^{[F:\mathbb{Q}]-1}$.

Since $E_0(\tau;s)$ has a simple pole at $s=1$ with constant residue $c_\Gamma\neq 0$, if $k=\ell$ and $\phi^{(\infty)}=\phi_M\otimes\phi_0$, we have from (4.7)

$$\begin{aligned}(4.10)\quad & 4^{1-[F:\mathbb{Q}]}C^{k\Sigma}|C^{\Sigma}|^{2}(4\pi)^{-k-I}\Gamma_F(k+I)\mathrm{Res}_{s=1}H_k(z_0,w_0;s;\phi^{(\infty)},f)\\ &\qquad = \mathrm{Res}_{s=1}D(s-1;f'_c,\theta(\phi_{k,M}))\\ &\qquad = [U^2]N(\mathfrak{a})^{-1}\sqrt{|D|}^{-1}c_\Gamma\langle\theta(\phi_{k,M}),f'_c\rangle_\Gamma,\end{aligned}$$

where

$$\langle g,f\rangle_\Gamma=\int_{\Gamma\backslash\mathfrak{H}^I}g(\tau)\overline{f(\tau)}\eta^k d\mu(\tau).$$

Let $\Psi_f(z,w)$ be the modular from on $GL(2)\times GL(2)$ given by the Fourier expansion:

$$\Psi_f(z,w)=\sum_{\alpha\in\Gamma\backslash M_2(F),\det(\alpha)\gg 0}\phi^{*(\infty)}(\epsilon\alpha)\mathbf{e}_F(\det(\alpha)z)f|_k\alpha(w)$$

as in Corollary 3.4. Then taking Γ sufficiently small and combining Corollary 3.4 and (4.10), we get the following explicit formula:

Theorem 4.1. *Let f be a Hilbert modular cusp form of weight k. Then we have*

$$\langle\theta(\phi_{k,M}),f'_c\rangle_\Gamma=2^{-k-2I}|D|^{-1}C^{k\Sigma}|C^{\Sigma}|^2 i^k\,\mathrm{Im}(z_0)^{-I}\,\mathrm{Im}(w_0)^{-I}\Psi_f(z_0,w_0)$$

under the notation of (4.4).

This type of results enabled Shimura to get a rationality result of the Petersson inner product of quaternionic cusp forms of CM type with respect to CM periods (for example, see [Sh2] II Section 3).

5. Jacquet-Langlands-Shimizu correspondence

It is a well known result of Jacquet-Langlands and Shimizu that if we choose level appropriately, the space of quaternionic automorphic forms can be embedded into the space of Hilbert modular forms keeping the Hecke operator action. We are going to recall the result, scrutinizing integrality of the correspondence.

5.1. Hilbert modular forms and Hecke algebras. Let us recall the definition of the adelic Hilbert modular forms and their Hecke ring of level $\mathfrak{N}$ for an integral ideal $\mathfrak{N}$ of F (cf. [H96] Sections 2.2-4).

We first recall formal Hecke rings of double cosets. We consider the following open compact subgroup of $GL_2(F_{\mathbb{A}^{(\infty)}})$:

$$U_0(\mathfrak{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\widehat{O}) \middle| c \equiv 0 \mod \mathfrak{N}\widehat{O} \right\}, \tag{5.1}$$

where $\widehat{O} = O \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ and $\widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$. Then we introduce the following semi-group

$$\Delta_0(\mathfrak{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(F_{\mathbb{A}^{(\infty)}}) \cap M_2(\widehat{O}) \middle| c \equiv 0 \mod \mathfrak{N}\widehat{O}, d_{\mathfrak{N}} \in O_{\mathfrak{N}}^\times \right\}, \tag{5.2}$$

where $d_{\mathfrak{N}}$ is the projection of $d \in \widehat{O}$ to $\prod_{\mathfrak{l}|\mathfrak{N}} O_{\mathfrak{l}}$ for prime ideals $\mathfrak{l}$. Writing T_0 for the maximal diagonal torus of $GL(2)_{/O}$ and putting

$$D_0 = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in T_0(F_{\mathbb{A}^{(\infty)}}) \cap M_2(\widehat{O}) \middle| d_{\mathfrak{N}} = 1 \right\}, \tag{5.3}$$

we have (e.g. [MFG] 3.1.6)

$$\Delta_0(\mathfrak{N}) = U_0(\mathfrak{N}) D_0 U_0(\mathfrak{N}). \tag{5.4}$$

Formal finite linear combinations $\sum_\delta c_\delta U_0(\mathfrak{N})\delta U_0(\mathfrak{N})$ of double cosets of $U_0(\mathfrak{N})$ in $\Delta_0(\mathfrak{N})$ form a ring $R(U_0(\mathfrak{N}), \Delta_0(\mathfrak{N}))$ under convolution product (see [IAT] Chapter 3 or [MFG] 3.1.6). The algebra is commutative and is isomorphic to the polynomial ring with variables $\{T(\mathfrak{l}), T(\mathfrak{l}, \mathfrak{l})\}_{\mathfrak{l}}$, $T(\mathfrak{l})$ for primes $\mathfrak{l}$ corresponding to the double coset $U_0(\mathfrak{N}) \left(\begin{smallmatrix} \varpi_{\mathfrak{l}} & 0 \\ 0 & 1 \end{smallmatrix}\right) U_0(\mathfrak{N})$ and $T(\mathfrak{l}, \mathfrak{l})$ for primes $\mathfrak{l} \nmid \mathfrak{N}$ corresponding to $U_0(\mathfrak{N})\varpi_{\mathfrak{l}} U_0(\mathfrak{N})$, where $\varpi_{\mathfrak{l}}$ is a prime element of $O_{\mathfrak{l}}$.

The double coset ring $R(U_0(\mathfrak{N}), \Delta_0(\mathfrak{N}))$ naturally acts on the space of adelic modular forms whose definition we now recall. Since $T_0(O/\mathfrak{N}')$ is canonically a quotient of $U_0(\mathfrak{N}')$, a character $\varepsilon : T_0(O/\mathfrak{N}') \to \mathbb{C}^\times$ can be considered as a character of $U_0(\mathfrak{N}')$. Writing $\varepsilon \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) = \varepsilon_1(a)\varepsilon_2(d)$, if $\widetilde{\varepsilon} = \varepsilon_1\varepsilon_2^{-1}$ factors through $O/\mathfrak{N}$ for $\mathfrak{N}|\mathfrak{N}'$, then we can extend the character ε of $U_0(\mathfrak{N}')$ to $U_0(\mathfrak{N})$ by putting $\varepsilon(u) = \varepsilon_2(\det(u))\widetilde{\varepsilon}(a)$ for $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in U_0(\mathfrak{N})$. Writing $\varepsilon^- = \widetilde{\varepsilon}^{-1}$, $\varepsilon(u)$ has another expression $\varepsilon(u) = \varepsilon_1(\det(u))\varepsilon^-(d)$, because they induce the same character on $U_0(\mathfrak{N}')$ and on $U_0(\mathfrak{N}) \cap SL_2(\widehat{O})$. Hereafter we use the expression $\varepsilon(u) = \varepsilon_1(\det(u))\varepsilon^-(d)$ (although $\varepsilon(u) = \varepsilon_2(\det(u))\widetilde{\varepsilon}(a)$ is used in [Fu] and [HMI]; we note that (κ_1, κ_2) in this paper corresponds to (κ_2, κ_1) in [HMI] and [PAF]). We fix an arithmetic character $\varepsilon_+ : F_{\mathbb{A}}^\times/F^\times \to \mathbb{C}^\times$ with $\varepsilon_+|_{\widehat{O}^\times} = \varepsilon_1\varepsilon_2$ and $\varepsilon_\infty(x) = x^{-(\kappa_1+\kappa_2-I)}$. We use the symbol ε for the triple $(\varepsilon_1, \varepsilon_2, \varepsilon_+)$; thus, we may regard ε as a character of $U_0(\mathfrak{N})F_{\mathbb{A}}^\times$ by $\varepsilon(uz) = \varepsilon(u)\varepsilon_+(z)$ for $z \in F_{\mathbb{A}}^\times$ and $u \in U_0(\mathfrak{N})$. If we replace ε_+ by its p–adic avatar $\widehat{\varepsilon}_+$, we get a p–adic character $\widehat{\varepsilon}$ of $U_0(\mathfrak{N})F_{\mathbb{A}}^\times$.

We identify the group of algebraic characters $X^*(T_0)$ of T_0 with $\mathbb{Z}[I]^2$ so that $\kappa = (\kappa_1, \kappa_2) \in \mathbb{Z}[I]^2$ sends $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$ to $x^{-\kappa_1}y^{-\kappa_2} = \prod_{\sigma \in I}(\sigma(x)^{-\kappa_{1,\sigma}}\sigma(y)^{-\kappa_{2,\sigma}})$. To each $\kappa \in X^*(T_0)$, we associate a factor of automorphy:

$$(5.5)\qquad J_\kappa(g,\tau) = \det(g)^{\kappa_2 - I} j(g,\tau)^{\kappa_1-\kappa_2+I} \quad \text{for } g \in GL_2(F_\infty) \text{ and } \tau \in \mathfrak{H}^I.$$

Then we define $S_\kappa(\mathfrak{N},\varepsilon;\mathbb{C})$ to be the space of functions $f : GL_2(F_\mathbb{A}) \to \mathbb{C}$ satisfying the following conditions (e.g. [H96] Section 2.2):

(S1) We have $f(\alpha x u z) = \varepsilon_+(z)\varepsilon(u)f(x)J_\kappa(u_\infty,\mathbf{i})^{-1}$ for all $\alpha \in GL_2(F)$, $z \in F_\mathbb{A}^\times$ and $u \in U_0(\mathfrak{N})C_\mathbf{i}$ for the stabilizer $C_\mathbf{i}$ in $GL_2^+(F_\infty)$ of $\mathbf{i} = (\sqrt{-1},\dots,\sqrt{-1}) \in \mathfrak{Z} = \mathfrak{H}^I$, where $GL_2^+(F_\infty)$ is the identity connected component of $GL_2(F_\infty)$;

(S2) Choosing $u \in GL_2(F_\infty)$ with $u(\mathbf{i}) = \tau$ for each $\tau \in \mathfrak{H}^I$, define $f_x(\tau) = f(xu_\infty)J_\kappa(u_\infty,\mathbf{i})$ for each $x \in GL_2(F_{\mathbb{A}^{(\infty)}})$. Then f_x is a holomorphic function on $\mathfrak{Z}$ for all x;

(S3) $f_x(\tau)$ is rapidly decreasing towards the cusp ∞.

If we replace the word: "rapidly decreasing" in (S3) by "slowly increasing", we get the definition of the space of modular forms $M_\kappa(\mathfrak{N},\varepsilon;\mathbb{C})$. It is easy to check (e.g. [MFG] 3.1.5 and [HMI] 2.3.5) that the function f_x in (S2) satisfies the classical automorphy condition:

$$(5.6)\qquad f(\gamma(\tau)) = \varepsilon(x^{-1}\gamma x)^{-1} f(\tau) J_\kappa(\gamma,\tau) \quad \text{for all } \gamma \in \Gamma_{0,x}(\mathfrak{N}),$$

where $\Gamma_{0,x}(\mathfrak{N}) = xU_0(\mathfrak{N})x^{-1}GL_2^+(F_\infty) \cap GL_2(F)$, and $GL_2^+(F_\infty)$ is the subgroup of $GL_2(F_\infty)$ made up of matrices with totally positive determinant. Also by (S3), f_x is rapidly decreasing towards all cusps of Γ_x (e.g. [MFG] (3.22)). It is well known that $M_\kappa = 0$ unless $\kappa_1 + \kappa_2 = [\kappa_1+\kappa_2]I$ for $[\kappa_1+\kappa_2] \in \mathbb{Z}$. We write simply $[\kappa]$ for $[\kappa_1+\kappa_2] \in \mathbb{Z}$ if $M_\kappa \neq 0$. In [H88a] Section 2, the space S_κ is written as $S^*_{k,\widehat{w}}$ for $k = \kappa_1 - \kappa_2 + I$ and $\widehat{w} = I - \kappa_2$, and the action of Hecke operators is the same as specified in [H88a] (2.9e), which we recall now.

In order to define the Hecke operator action on the space of automorphic forms, we fix a prime element $\varpi_\mathfrak{l}$ of the $\mathfrak{l}$–adic completion $O_\mathfrak{l}$ of O for each prime ideal $\mathfrak{l}$ of F. We extend $\varepsilon^- : \widehat{O}^\times \to \mathbb{C}^\times$ to $F^\times_{\mathbb{A}^{(\infty)}} \to \mathbb{C}^\times$ just by putting $\varepsilon^-(\varpi_\mathfrak{l}^m) = 1$ for $m \in \mathbb{Z}$. This is possible because $F_\mathfrak{l}^\times = O_\mathfrak{l}^\times \times \varpi_\mathfrak{l}^\mathbb{Z}$ for $\varpi_\mathfrak{l}^\mathbb{Z} = \{\varpi_\mathfrak{l}^m | m \in \mathbb{Z}\}$. Similarly, we extend ε_2 to $F^\times_{\mathbb{A}^{(\infty)}}$. Then we define $\varepsilon(u) = \varepsilon_1(\det(u))\varepsilon^-(d)$ for $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_0(\mathfrak{N})$. Let $\mathcal{U}$ be the unipotent algebraic subgroup of $GL(2)_{/F}$ defined by

$$\mathcal{U}(A) = \left\{ \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \middle| a \in A \right\}.$$

For each $U_0(\mathfrak{N})yU_0(\mathfrak{N}) \in R(U_0(\mathfrak{N}),\Delta_0(\mathfrak{N}))$, we can decompose

$$U_0(\mathfrak{N})yU_0(\mathfrak{N}) = \bigsqcup_{t \in T_0(F_\mathbb{A}^{(\infty)}),\, u \in \mathcal{U}(\widehat{O})} utU_0(\mathfrak{N})$$

for finitely many u and t (see [IAT] Chapter 3 or [MFG] 3.1.6). We define

$$(5.7)\qquad f|[U_0(\mathfrak{N})yU_0(\mathfrak{N})](x) = \sum_{t,u} \varepsilon(t)^{-1} f(xut).$$

It is easy to check that this operator preserves the space $M_\kappa(\mathfrak{N},\varepsilon;\mathbb{C})$ and $S_\kappa(\mathfrak{N},\varepsilon;\mathbb{C})$ by verifying (S1-3) for $f|[U_0(\mathfrak{N})yU_0(\mathfrak{N})]$. This action for y with

$y_{\mathfrak{N}} = 1$ is independent of the choice of the extension of ε to $T_0(F_{\mathbb{A}})$. When $y_{\mathfrak{N}} \neq 1$, we may assume that $y_{\mathfrak{N}} \in D_0 \subset T_0(F_{\mathbb{A}})$, and in this case, t can be chosen so that $t_{\mathfrak{N}} = y_{\mathfrak{N}}$ (so $t_{\mathfrak{N}}$ is independent of single right cosets in the double coset). If we extend ε to $T(F_{\mathbb{A}}^{(\infty)})$ by choosing another prime element $\varpi'_{\mathfrak{l}}$ and write the extension as ε', then we have

$$\varepsilon(t_{\mathfrak{N}})[U_0(\mathfrak{N})yU_0(\mathfrak{N})] = \varepsilon'(t_{\mathfrak{N}})[U_0(\mathfrak{N})yU_0(\mathfrak{N})]',$$

where the operator on the right-hand-side is defined with respect to ε'. Thus the sole difference is the root of unity $\varepsilon(t_{\mathfrak{N}})/\varepsilon'(t_{\mathfrak{N}}) \in \mathrm{Im}(\varepsilon|_{T_0(O/\mathfrak{N})})$. Since it depends on the choice of $\varpi_{\mathfrak{l}}$, we make the choice once and for all, and write $T(\mathfrak{l})$ for $[U_0(\mathfrak{N}) \left(\begin{smallmatrix} \varpi_{\mathfrak{l}} & 0 \\ 0 & 1 \end{smallmatrix}\right) U_0(\mathfrak{N})]$ (if $\mathfrak{l}|\mathfrak{N}$). By linearity, these action of double cosets extends to the ring action of the double coset ring $R(U_0(\mathfrak{N}), \Delta_0(\mathfrak{N}))$.

To introduce rationality structure on the space of modular forms, we recall Fourier expansion and q–expansion of modular forms (cf. [H96] Sections 2.3–4 and [HMI] Proposition 2.26, where the order of κ_j $(j = 1, 2)$ is reversed; so, (κ_1, κ_2) here corresponds to (κ_2, κ_1) in [HMI]). We fix an embedding $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ once and for all and identify $\overline{\mathbb{Q}}$ with the subfield of all algebraic numbers in $\mathbb{C}$. We also choose a differental idele $d \in F_{\mathbb{A}}^\times$ with trivial prime-to–$\mathfrak{d}$ part: $d^{(\mathfrak{d})} = 1$. Thus $d\widehat{O} = \mathfrak{d}\widehat{O}$ for the absolute different $\mathfrak{d}$ of F. Each member f of $M_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$ has Fourier expansion of the following form:

(5.8)

$$f\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) = |y|_{\mathbb{A}} \left\{ a_0(yd, f)|u|_{\mathbb{A}}^{[\kappa_2]} + \sum_{0 \ll \xi \in F} a(\xi yd, f)(\xi y_\infty)^{-\kappa_2} \mathbf{e}_F(i\xi y_\infty)\mathbf{e}_{\mathbb{A}}(\xi x) \right\}.$$

Here $y \mapsto a(y, f)$ and $a_0(y, f)$ are functions defined on $y \in F_{\mathbb{A}}^\times$ only depending on its finite part $y^{(\infty)}$. The function $a(y, f)$ is supported by the set $(\widehat{O} \times F_\infty) \cap F_{\mathbb{A}}^\times$. When $f \in S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$, $a_0(y, f) = 0$; so, we just ignore the constant term $a_0(y, f)$. When κ_2 is not in $\mathbb{Z}I$, we have $S_\kappa = M_\kappa$; so, we ignore the constant term if $[\kappa_2] \in \mathbb{Z}$ is not well defined. Let $F[\kappa]$ be the field fixed by $\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F) | \kappa\sigma = \kappa\}$, which is the field of rationality of the character $\kappa \in X^*(T_0)$. Write $O[\kappa]$ for the integer ring of $F[\kappa]$. We also define $O[\kappa, \varepsilon]$ for the integer ring of the field $F[\kappa, \varepsilon]$ generated by the values of ε (on finite ideles) over $F[\kappa]$. We call an idele $y \in F_{\mathbb{A}}^\times$ *integral* if $y^{(\infty)} \in \widehat{O}$. Then for any $F[\kappa, \varepsilon]$–algebra A inside $\mathbb{C}$, we define

(5.9)

$$\begin{aligned} M_\kappa(\mathfrak{N}, \varepsilon; A) &= \left\{ f \in M_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C}) \middle| a_0(y, f), a(y, f) \in A \text{ as long as } y \text{ is integral} \right\} \\ S_\kappa(\mathfrak{N}, \varepsilon; A) &= M_\kappa(\mathfrak{N}, \varepsilon; A) \cap S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C}). \end{aligned}$$

Using rationality of (the canonical models of) the Hilbert modular variety (studied by Shimura and others), we can interpret $S_\kappa(\mathfrak{N}, \varepsilon; A)$ (resp. $M_\kappa(\mathfrak{N}, \varepsilon; A)$) as the space of A–rational global sections of a line bundle of the variety defined over A; so, we have, by the flat base-change theorem (e.g.

[GME] Lemma 1.10.2),

(5.10) $M_\kappa(\mathfrak{N},\varepsilon;A)\otimes_A\mathbb{C}=M_\kappa(\mathfrak{N},\varepsilon;\mathbb{C})$ and $S_\kappa(\mathfrak{N},\varepsilon;A)\otimes_A\mathbb{C}=S_\kappa(\mathfrak{N},\varepsilon;\mathbb{C})$

Since Hecke operators are induced by algebraic correspondences on the product of two Hilbert modular varieties defined over A (e.g. [GME] 4.2.1 and [PAF] 4.2.5), the action of the Hecke operators $T(\mathfrak{l})$ and $T(\mathfrak{l},\mathfrak{l})$ preserves the A–rational space of modular forms (see below (5.15) for a more concrete argument showing the Hecke operator stability). We define the Hecke algebra $h_\kappa(\mathfrak{N},\varepsilon;A)\subset\mathrm{End}_A(S_\kappa(\mathfrak{N},\varepsilon;A))$ by the A–subalgebra generated by the Hecke operators $T(\mathfrak{l})$ and $T(\mathfrak{l},\mathfrak{l})$ for all prime ideals $\mathfrak{l}$ (here we agree to put $T(\mathfrak{l},\mathfrak{l})=0$ if $\mathfrak{l}|\mathfrak{N}$). In the same manner, we define $H_\kappa(\mathfrak{N},\varepsilon;A)\subset\mathrm{End}_A(M_\kappa(\mathfrak{N},\varepsilon;A))$.

5.2. q–Expansion of p–integral modular forms. We recall the rational prime p and the embedding $i_p:\overline{\mathbb{Q}}\hookrightarrow\overline{\mathbb{Q}}_p$. Then for any $\overline{\mathbb{Q}}_p$–algebras A, we define

(5.11)
$$M_\kappa(\mathfrak{N},\varepsilon;A)=M_\kappa(\mathfrak{N},\varepsilon;\overline{\mathbb{Q}})\otimes_{\overline{\mathbb{Q}},i_p}A \text{ and } S_\kappa(\mathfrak{N},\varepsilon;A)=S_\kappa(\mathfrak{N},\varepsilon;\overline{\mathbb{Q}})\otimes_{\overline{\mathbb{Q}},i_p}A.$$

By linearity, $y\mapsto a(y,f)$ and $a_0(y,f)$ extend to functions on $F^\times_\mathbb{A}\times M_\kappa(\mathfrak{N},\varepsilon;A)$ with values in A. Let $\mathcal{N}:F^\times_\mathbb{A}/F^\times\to\overline{\mathbb{Q}}_p^\times$ be the p–cyclotomic character defined by $\mathcal{N}(y)=y_p^{-I}|y^{(\infty)}|^{-1}_\mathbb{A}$. Then we define the q–expansion coefficients (at p) of $f\in M_\kappa(\mathfrak{N},\varepsilon;A)$ by

$$(5.12)\qquad \mathbf{a}_p(y,f)=y_p^{-\kappa_2}a(y,f)\ \text{ and }\ \mathbf{a}_{0,p}(y,f)=\mathcal{N}(yd^{-1})^{[\kappa_2]}a_0(y,f).$$

Here we note that $a_0(y,f)=0$ unless $[\kappa_2]\in\mathbb{Z}$ is well defined. We now define for any p–adically complete $O[\kappa,\varepsilon]$–algebra A in $\widehat{\overline{\mathbb{Q}}}_p$ (the p–adic completion of $\overline{\mathbb{Q}}_p$)

(5.13)
$$M_\kappa(\mathfrak{N},\varepsilon;A)=\Big\{f\in M_\kappa(\mathfrak{N},\varepsilon;\widehat{\overline{\mathbb{Q}}}_p)\big|\mathbf{a}_{0,p}(y,f),\mathbf{a}_p(y,f)\in A\text{ for integral }y\Big\}$$
$$S_\kappa(\mathfrak{N},\varepsilon;A)=M_\kappa(\mathfrak{N},\varepsilon;A)\cap S_\kappa(\mathfrak{N},\varepsilon;\widehat{\overline{\mathbb{Q}}}_p).$$

These spaces have geometric meaning as the space of A–integral global sections of a line bundle of the Hilbert modular variety of level $\mathfrak{N}$ (e.g. [HT1] 1.3 and [HMI] 4.3.7).

The formal q–expansion of f has values in the space of functions on $F^\times_{\mathbb{A}^{(\infty)}}$ with values in the formal monoid algebra $A[[q^\xi]]_{\xi\in F_+}$ of the multiplicative semi-group F_+ made up of totally positive elements, which is given by

$$(5.14)\qquad f(y)=\mathcal{N}(y)^{-1}\left\{\mathbf{a}_{0,p}(yd,f)+\sum_{\xi\gg0}\mathbf{a}_p(\xi yd,f)q^\xi\right\}.$$

We choose a complete representative set $\{a_i\}_{i=1,\dots,h}$ in finite ideles for the strict idele class group $F^\times\backslash F^\times_\mathbb{A}/\widehat{O}^\times F^\times_{\infty+}$. Let $\mathfrak{a}_i=a_iO$. Write $t_i=\left(\begin{smallmatrix}a_id^{-1}&0\\0&1\end{smallmatrix}\right)$ and consider $f_i = f_{t_i}$ as defined in (S2). The collection $(f_i)_{i=1,\dots,h}$ determines f, because

$$GL_2(F_{\mathbb{A}}) = \bigsqcup_{i=1}^{h} GL_2(F)t_iU_0(\mathfrak{N})GL_2^+(F_\infty)$$

by the approximation theorem. Then as observed in [H88a] Section 4 (and [PAF] 4.2.10), $f(a_id^{-1})$ gives the q–expansion over A of f_i at the Tate abelian variety with a_iO–polarization $\mathrm{Tate}_{\mathfrak{a}_i^{-1},O}(q)$ as in [HT1] 1.7. Thus by the q–expansion principle ([HT1] 1.7 and [HMI] 4.2.8), the q–expansion: $y \mapsto f(y)$ determines f uniquely (for any algebra A for which the space of A–integral modular forms is well defined).

We write $T(y)$ for the Hecke operator acting on $M_\kappa(\mathfrak{N},\varepsilon;A)$ corresponding to the double coset decomposition of

$$\mathcal{T}(y) = \left\{x \in \Delta_0(\mathfrak{N}) \middle| \det(x)\widehat{O} = y\widehat{O}\right\}$$

for $y \in \widehat{O} \cap F^\times_{\mathbb{A}^{(\infty)}}$. We renormalize $T(y)$ to create a new operator $\mathbb{T}(y)$ by $\mathbb{T}(y) = y_p^{-\kappa_2}T(y)$. Since this only affects $T(y)$ with $y_p \neq 1$, $\mathbb{T}(\mathfrak{l}) = T(\varpi_\mathfrak{l}) = T(\mathfrak{l})$ if $\mathfrak{l} \nmid p$. However $\mathbb{T}(\mathfrak{p}) \neq T(\mathfrak{p})$ for primes $\mathfrak{p}|p$. This renormalization is optimal to have the stability of the A–integral spaces under Hecke operators. We define $\langle\mathfrak{l}\rangle = N(\mathfrak{l})T(\mathfrak{l},\mathfrak{l})$ for $\mathfrak{l} \nmid \mathfrak{N}$. This new action also preserves the integrality as long as $[\kappa] \geq 0$ (cf. [H96] Section 2.2 and [HMI] Theorem 2.28). We have the following formula of the action of $T(\mathfrak{l})$ and $T(\mathfrak{l},\mathfrak{l})$ (e.g. [H96] Section 2.4):

$$\mathbf{a}_p(y, f|\mathbb{T}(\mathfrak{l})) = \begin{cases} \mathbf{a}_p(y\varpi_\mathfrak{l}, f) + \mathbf{a}_p(y\varpi_\mathfrak{l}^{-1}, f|\langle\mathfrak{l}\rangle) & \text{if } \mathfrak{l} \nmid \mathfrak{N} \\ \mathbf{a}_p(y\varpi_\mathfrak{l}, f) & \text{if } \mathfrak{l}|\mathfrak{N}. \end{cases} \tag{5.15}$$

From this, it is plain that $T(\mathfrak{l})$ preserves the space $S_\kappa(\mathfrak{N},\varepsilon;A)$ if either $p|\mathfrak{N}$ or $[\kappa] \geq 0$, because $\mathbf{a}_p(y\varpi_\mathfrak{l}^{-1}, f|\langle\mathfrak{l}\rangle) = \varpi_{\mathfrak{l},p}^{-2\kappa_2}N(\mathfrak{l})\varepsilon_+(\mathfrak{l})\mathbf{a}_p(y,f)$. We hereafter assume

$$\text{Either } p|\mathfrak{N} \text{ or } [\kappa] \geq 0 \text{ and } \kappa_1 - \kappa_2 \geq I. \tag{5.16}$$

We define $h_\kappa(\mathfrak{N},\varepsilon;A)$ again by the A–subalgebra of $\mathrm{End}_A(S_\kappa(\mathfrak{N},\varepsilon;A))$ generated by $\mathbb{T}(\mathfrak{l})$ and $\langle\mathfrak{l}\rangle$ over A for all primes $\mathfrak{l}$ (for a p–adically complete $O[\kappa,\varepsilon]$–algebra A).

We can think of the subgroup $U(\mathfrak{N})$ of $U_0(\mathfrak{N})$ made of matrices $u \in U_0(\mathfrak{N})$ whose reduction modulo $\mathfrak{N}$ are upper unipotent. Then for any subgroup U with $U(\mathfrak{N}) \subset U \subset U_0(\mathfrak{N})$, we can think of the space of cusp forms $S_\kappa(U,\varepsilon;\mathbb{C})$ made up of cusp forms satisfying (S1-3) for U in place of $U_0(\mathfrak{N})$. We have Hecke operators $\mathbb{T}(y)$ corresponding to $(U \cdot D_0U) \cap \mathcal{T}(y)$ acting on $S_\kappa(U,\varepsilon;A)$. Then in the same manner of $S_\kappa(\mathfrak{N},\varepsilon;A)$, we define $S_\kappa(U,\varepsilon;A)$ and the Hecke algebra $h_\kappa(U,\varepsilon;A)$ as the A–subalgebra of $\mathrm{End}_A(S_\kappa(U,\varepsilon;A))$ generated by $\mathbb{T}(y)$ and $\langle\mathfrak{l}\rangle$.

Proposition 5.1. *Let A be an $O[\kappa,\varepsilon]$–algebra for which the space of cusp forms $S_\kappa(\mathfrak{N},\varepsilon;A)$ is well defined (by* (5.9) *or* (5.11) *or* (5.13)*). Write $H =$*

$h_\kappa(\mathfrak{N},\varepsilon;A)$ and $S = S_\kappa(\mathfrak{N},\varepsilon;A)$. Let V be an H–module and V' be an A–module of finite type with an A–bilinear product $\langle\ ,\ \rangle : V \times V' \to A$. Then we have:

(1) *The formal q–expansion for $v \in V$ and $w \in V'$:*

$$f(v \otimes w)(y) = \mathcal{N}(y)^{-1}\left\{\sum_{\xi \gg 0} \langle v|\mathbb{T}(\xi y d), w\rangle q^\xi\right\}$$

gives a unique element of S.

(2) *The map $v \otimes w \mapsto f(v \otimes w)$ gives an A–linear map of $V \otimes_A V'$ into S with $f((v|\mathbb{T}(y)) \otimes w) = f(v \otimes w)|\mathbb{T}(y)$. If further V' is an H–module and $\langle v|h, w\rangle = \langle v, w|h\rangle$ for all $v \in V$, $w \in V'$ and $h \in H$, then the map f induces an H–linear map: $V \otimes_H V' \to S_\kappa(\mathfrak{N},\varepsilon;A)$.*

(3) *Suppose that R is an A–algebra direct summand of H, and put $V(R) = RV$ and $S(R) = RS$. If $V(R)$ is R–free of finite rank and $\mathrm{Hom}_A(V(R),A)$ is embedded into V' by the pairing $\langle\ ,\ \rangle$, then the map $f : V(R) \otimes_A V' \to S(R)$ is surjective.*

The formulation of this proposition is suggested by the expression of the theta correspondence given in [Sh2] II, Theorem 3.1.

Proof. We have an isomorphism $\iota : \mathrm{Hom}_A(H,A) \cong S$ given by $\mathbf{a}_p(y,\iota(\phi)) = \phi(\mathbb{T}(y))$ (see [H88a] Theorem 5.11, [H91] Theorem 3.1 and [H96] Section 2.6), which is an H–linear map (that is, $\iota(\phi \circ h) = \iota(\phi)|h)$. Since V is an H–module, $h \mapsto \langle v|h, w\rangle$ gives an element of $\mathrm{Hom}_A(H,A)$ and hence an element in S. The element has the expression as in (1) by the above explicit form of ι. The assertion (2) is then clear from (1). As for (3), by the isomorphism $\mathrm{Hom}_A(V(R),A) \hookrightarrow V'$, each element of $\mathrm{Hom}(R,A) \cong S(R)$ is a finite A–linear combination of $h \mapsto \langle v|h, w\rangle$ for $v \in V(R)$ and $w \in V'$; so, the surjectivity follows. □

5.3. Integral correspondence. In order to create a proto-typical example of the module V in Proposition 5.1, we study here cohomology groups on quaternionic Shimura varieties. See [H94] and [H88a] for more details of such cohomology groups.

Let B be a quaternion algebra over F. We write G for the algebraic group defined over $\mathbb{Q}$ such that $G(A) = (B \otimes_\mathbb{Q} A)^\times$ for each $\mathbb{Q}$–algebra A. Let $d(B)^2$ be the discriminant of B. We assume that $p \nmid d(B)$ and that

$$B \otimes_{F,\sigma} \mathbb{R} \cong \begin{cases} M_2(\mathbb{R}) & \text{if } \sigma \in I_B \\ \mathbb{H} & \text{if } \sigma \in I - I_B = I^B, \end{cases} \tag{5.17}$$

where $\mathbb{H}$ is the Hamilton quaternion algebra over $\mathbb{R}$.

We fix once and for all an extension of $\sigma : F \hookrightarrow \overline{\mathbb{Q}}$ to $\sigma : \overline{F} \cong \overline{\mathbb{Q}}$ for an algebraic closure $\overline{F}/F$. We take a quadratic extension K/F inside $\overline{F}$ so that $K \otimes_{F,\sigma} \mathbb{R} \cong \mathbb{R} \times \mathbb{R}$ as F–algebras for $\sigma \in I_B$, $K \otimes_F F_\mathfrak{p} \cong F_\mathfrak{p} \times F_\mathfrak{p}$ for primes $\mathfrak{p}|p$

and $B\otimes_F K \cong M_2(K)$. We can always choose such a quadratic extension K as long as $p \nmid d(B)$. These condition automatically implies $K\otimes_F\mathbb{R} \cong \mathbb{C}$ for $\sigma \in I^B$.

We identify $B \otimes_F K$ with $M_2(K)$ by the above isomorphism. We fix maximal orders O_B and O_K of B and K, respectively, and we suppose that

$$O_B \otimes_O O_K \subset M_2(O_K). \tag{5.18}$$

We fix an isomorphism $O_{B,\mathfrak{l}} \cong M_2(O_\mathfrak{l})$ so that for the p–adic place $\mathfrak{p}|p$ induced by $i_p \circ \sigma$, this isomorphism coincides with the one: $O_B \hookrightarrow M_2(O_K) \xrightarrow{i_p\circ\sigma} M_2(O_\mathfrak{p})$. For an integral ideal $\mathfrak{N}_0$ of F prime to $d(B)$, putting $\mathfrak{N} = \mathfrak{N}_0 d(B)$, we define

$$U_0^B(\mathfrak{N}) = \left\{x \in G(\mathbb{A}) \middle| x_{\mathfrak{N}_0} = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \text{ with } c \in \mathfrak{N}_0 O_{\mathfrak{N}_0}\right\}, \tag{5.19}$$

where $O_{\mathfrak{N}_0} = \prod_{\mathfrak{l}|\mathfrak{N}_0} O_\mathfrak{l}$. Similarly we define $\Delta_0^B(\mathfrak{N}) \subset B \otimes_\mathbb{Q} \mathbb{A}^{(\infty)}$ so that it is the product of local components $\Delta_\mathfrak{l}$ which coincide with the local components of $\Delta_0(\mathfrak{N})$ as long as $\mathfrak{l} \nmid d(B)$ and $\Delta_\mathfrak{l} = O_{B,\mathfrak{l}}$ if $\mathfrak{l}|d(B)$. Again we can think of the double coset ring $R(U_0^B(\mathfrak{N}), \Delta_0^B(\mathfrak{N}))$. We have $T(\mathfrak{l})$ and $T(\mathfrak{l},\mathfrak{l})$ in $R(U_0^B(\mathfrak{N}), \Delta_0^B(\mathfrak{N}))$ for $\mathfrak{l} \nmid d(B)$, because the local component at $\mathfrak{l}$ of $\Delta_0^B(\mathfrak{N})$ is identical to that of $\Delta_0(\mathfrak{N})$. For $\mathfrak{l}|d(B)$, we take $\alpha_\mathfrak{l} \in O_{B,\mathfrak{l}}$ so that its reduced norm generates $\mathfrak{l}O_\mathfrak{l}$. Then we define $T(\mathfrak{l}) = -U_0^B(\mathfrak{N})\alpha_\mathfrak{l}U_0^B(\mathfrak{N})$ for $\mathfrak{l}|d(B)$, and we have

$$R(U_0(\mathfrak{N}), \Delta_0(\mathfrak{N})) \cong R(U_0^B(\mathfrak{N}), \Delta_0^B(\mathfrak{N})). \tag{5.20}$$

The above isomorphism brings $T(\mathfrak{l})$ and $T(\mathfrak{l},\mathfrak{l})$ to the corresponding elements in the right-hand-side.

For a given ring A, we consider the following module $L(\kappa; A)$ over the multiplicative semi-group $M_2(A)$: Let $n = \kappa_1 - \kappa_2 - I \in \mathbb{Z}[I]$. We suppose that $n \geq 0$ (implying $n_\sigma \geq 0$ for all $\sigma \in I$), and we consider polynomials with coefficients in A of $(X_\sigma, Y_\sigma)_{\sigma\in I}$ homogeneous of degree n_σ for each pairs (X_σ, Y_σ). The collection of all such polynomials forms an A–free module $L(\kappa; A)$ of rank $\prod_\sigma(n_\sigma + 1)$.

Suppose that A is a closed $O_K[\kappa,\varepsilon]$-algebra (via i_p) of $\widehat{\mathbb{Q}}_p$. Then $i_p(\sigma(\delta_p))$ (which we write simply $\sigma(\delta_p)$) for $\delta \in G(\mathbb{A})$ can be regarded as an element in $M_2(A)$. We let $\Delta_0^B(\mathfrak{N})$ act on $L(\kappa; A)$ as follows:

$$\delta\Phi\left(\left(\begin{smallmatrix} X_\sigma \\ Y_\sigma\end{smallmatrix}\right)\right) = \varepsilon(\delta)N(\delta)^{\kappa_2}\Phi\left(\left(\sigma(\delta^\iota)\left(\begin{smallmatrix} X_\sigma \\ Y_\sigma\end{smallmatrix}\right)\right)\right). \tag{5.21}$$

Here $N(\delta)$ is the reduced norm of B. We also let $z \in F_\mathbb{A}^\times$ act on $L(\kappa; A)$ through scalar multiplication by $\widehat{\varepsilon}_+(z) = \varepsilon_+(z)z_p^{-\kappa_1-\kappa_2+I}$ (the p–adic avatar of ε_+). We write $L(\kappa\varepsilon; A)$ for the module $L(\kappa; A)$ with this $\Delta_0^B(\mathfrak{N})F_\mathbb{A}^\times$–action. By the condition: $\kappa_1 + \kappa_2 \in \mathbb{Z}I$, if $U \subset U_0^B(\mathfrak{N})$ is sufficiently small open compact subgroup, central elements in $\Gamma_x = xUx^{-1} \cap G(\mathbb{Q})$ acts trivially on $L(\kappa\varepsilon; A)$.

We let $g \in G(\mathbb{R})$ with $N(g) \gg 0$ act on $\mathfrak{H}^{I_B}$ (by the linear fractional transformation) component-wise via $g_\sigma = \sigma(g) \in GL_2(K \otimes_{K,\sigma} \mathbb{R}) = GL_2(\mathbb{R})$. We put $C_{\sigma+}$ for the stabilizer of $\sqrt{-1}$ in the identity connected component of $(B \otimes_{F,\sigma} \mathbb{R})^\times$ and define

$$C_{\infty+} = \prod_{\sigma\in I_B} C_{\sigma+} \times \prod_{\sigma\in I^B} (B \otimes_{F,\sigma} \mathbb{R})^\times.$$

Thus we have $\mathfrak{H}^{I_B} \cong G(\mathbb{R})^+/C_{\infty+}$ by $g(\mathbf{i}) \leftrightarrow g$ ($\mathbf{i} = (\sqrt{-1},\dots,\sqrt{-1}) \in \mathfrak{H}^{I_B}$) for the identity connected component $G(\mathbb{R})^+$ of $G(\mathbb{R})$. For any open compact subgroup $U \subset U_0^B(\mathfrak{N})$, we think of the complex manifold associated to the Shimura variety:

$$Y(U) = G(\mathbb{Q})\backslash G(\mathbb{A})/F_{\mathbb{A}}^\times U \cdot C_{\infty+}.$$

We write simply $Y_0^B(\mathfrak{N})$ for $Y(U_0^B(\mathfrak{N}))$.

If U is sufficiently small so that the image $\overline{\Gamma}_{U,x}$ of $\Gamma_{U,x} = xUx^{-1}G^+(\mathbb{R}) \cap G(\mathbb{Q})$ in $G(\mathbb{R})/F_\infty^\times$ acts freely on $\mathfrak{H}^{I_B}$ for all $x \in G(\mathbb{A}^{(\infty)})$, and the action of $\Gamma_{U,x}$ on $L(\kappa\varepsilon;A)$ factors through $\overline{\Gamma}_{U,x}$. Then we can define an étale space over $Y(U)$:

$$\mathcal{L}(\kappa\varepsilon;A) = G(\mathbb{Q})\backslash \left(G(\mathbb{A}) \times L(\kappa\varepsilon;A)\right)/F_{\mathbb{A}}^\times U \cdot C_{\infty+},$$

where $\gamma(x,\Phi)uz = (\gamma xuz, u^\iota \widehat{\varepsilon}_+(z)\Phi)$ for $u \in U\cdot C_{\infty+}$, $z \in F_{\mathbb{A}}^\times$ and $\gamma \in G(\mathbb{Q})$. This étale space gives rise to the sheaf $L(\kappa\varepsilon;A)_{/Y(U)}$ of locally constant sections. We consider the sheaf cohomology group $H^q(Y(U), L(\kappa\varepsilon;A))$.

Since $Y(U) \cong \sqcup_x \overline{\Gamma}_x\backslash\mathfrak{H}^{I_B}$ for finitely many x with $x_p = 1$, we have a canonical isomorphism (cf. [H94] page 470):

$$H^q(Y(U), L(\kappa\varepsilon;A)) \cong \bigoplus_x H^q(\overline{\Gamma}_{U,x}, L(\kappa\varepsilon;A)), \tag{5.22}$$

where the right-hand-side is the direct sum of the group cohomology of the $\overline{\Gamma}_x$–module $L(\kappa\varepsilon;A)$. The kernel $E = \mathrm{Ker}(\Gamma_{U,x} \to \overline{\Gamma}_{U,x})$ is a subgroup of units $O^\times$. Since $\kappa_1+\kappa_2 \in \mathbb{Z}I$, the action of $\epsilon \in E$ on $L(\kappa\varepsilon;A)$ is the multiplication by $\widehat{\varepsilon}_+(\epsilon)N(\epsilon)^{[\kappa]+1} = 1$. Even if $\overline{\Gamma}_{U,x}$ does not act freely on the module $L(\kappa\varepsilon;A)$, we still have $Y(U) \cong \bigsqcup_x \overline{\Gamma}_x\backslash\mathfrak{H}^{I_B}$ for finitely many x with $x_p = 1$, we can *define* the left-hand-side of (5.22) by the right hand side of (5.22).

We choose U sufficiently small as above so that $[U_0^B(\mathfrak{N}) : U]$ is prime to p (this is a condition on p). Then we have the trace map Tr (that is, the transfer map in group cohomology) and the restriction map Res:

$$\mathrm{Tr} : H^q(Y^B(U), L(\kappa\varepsilon;A)) \to H^q(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon;A))$$
$$\mathrm{Res} : H^q(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon;A)) \to H^q(Y^B(U), L(\kappa\varepsilon;A)).$$

Since $\mathrm{Tr}\circ\mathrm{Res}$ is the multiplication by $[U_0(\mathfrak{N}) : U]$, we have

$$H^q(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon;A)) = H^q(Y^B(U), L(\kappa\varepsilon;A))/\mathrm{Ker}(\mathrm{Tr}) = \mathrm{Im}(\mathrm{Res}). \tag{5.23}$$

We can always choose a multiple $\mathfrak{N}' = \mathfrak{N}\mathfrak{q}$ (by a prime $\mathfrak{q}$) of $\mathfrak{N}$ so that $\overline{\Gamma}_{0,x}(\mathfrak{N}')$ acts freely on $\mathfrak{H}^{I_B}$.

As defined in [H88a] Section 7 and [H94] Section 4, where $L(\kappa\varepsilon;A)$ is written as $L(n,v,\varepsilon;A)$ for $v=\kappa_2$ and $n=\kappa_1-\kappa_2-I$, we have a natural action of the ring $R(U_0^B(\mathfrak{N}),\Delta_0^B(\mathfrak{N}))$ on the cohomology group $H^q(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;A))$. For our later use, we recall the definition of the action when $q=0$: In this case, we may regard each cohomology class as a global section $f:B_{\mathbb{A}}^{\times}\to L(\kappa\varepsilon;A)$ with $f(\alpha xu)=u^{\iota}f(x)$ for $\alpha\in B^{\times}$ and $u\in U_0^B(\mathfrak{N})B_{\infty}^{\times}$. Decomposing $U_0^B(\mathfrak{N})\left(\begin{smallmatrix}y&0\\0&1\end{smallmatrix}\right)U_0^B(\mathfrak{N})=\bigsqcup_{\varpi}\varpi U_0^B(\mathfrak{N})$, we have

$$f|\mathbb{T}(y)=y_p^{-\kappa_2}\sum_{\varpi}\varpi f(x\varpi^{-\iota}). \tag{5.24}$$

Let W be a valuation ring as in the introduction. We assume that $h_{\kappa}(\mathfrak{N},\varepsilon;W)$ is well defined and $O_K[\kappa,\varepsilon]$ is embedded into W via i_p. Let V be the image of $H^q(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W))$ in $H^q(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q}))$. By the Eichler-Shimura isomorphism (between the space of cusp forms on $G(\mathbb{A})$ and the cohomology group; e.g. [H94] Proposition 3.1 and (10.4)) combined with the Jacquet-Langlands-Shimizu correspondence (e.g. [H88a] Theorem 2.1, Proposition 2.3 and [H81] 2.12), the above cohomology group and its compactly supported version (denoted by $H_c^q(Y_0^B(\mathfrak{N}),\cdot)$) are the module over the Hecke algebra $H_{\kappa}(\mathfrak{N},\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})$. Since

$$H_{\kappa}(\mathfrak{N},\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})=h_{\kappa}(\mathfrak{N},\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})\oplus E$$

as an algebra direct sum for the Eisenstein part E, for the idempotent 1_h of the cuspidal part $h_{\kappa}(\mathfrak{N},\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})$, we can define the cuspidal cohomology groups by

$$H^q_{cusp}(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q}))=1_hH^q(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})).$$

The natural map from compactly supported cohomology group into the cohomology group without support condition actually induces an isomorphism

$$1_hH^q_c(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q}))\cong H^q_{cusp}(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})).$$

We then put

$$H^q_{cusp}(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W))=H^q_{cusp}(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q}))\cap\mathrm{Im}(i) \tag{5.25}$$

for the natural morphism

$$i:H^q(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W))\to H^q(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;W\otimes_{\mathbb{Z}}\mathbb{Q})).$$

We consider the duality pairing [,] on $L(\kappa\varepsilon;A)$ (for $\mathbb{Q}$–algebra A) introduced in [H94] Section 5:

$$\left[\sum_{0\le j\le n}b_jX^{n-j}Y^j,\sum_{0\le j\le n}a_jX^{n-j}Y^j\right]=\sum_j(-1)^j\binom{n}{j}^{-1}b_{n-j}a_j\in A, \tag{5.26}$$

where $n=\kappa_1-\kappa_2-I$, $\binom{n}{j}=\prod_{\sigma\in I}\binom{n_\sigma}{j_\sigma}$ and for example $X^j=\prod_{\sigma\in I}X_\sigma^{j_\sigma}$. As $U_0(\mathfrak{N})F_{\mathbb{A}}^{\times}$-modules, this pairing satisfies:

$$[uz\Phi,uz\Phi']=\varepsilon^2(u)\widehat{\varepsilon}_+(z)^2N_{B/F}(u_p)^{\kappa_1+\kappa_2-I}[\Phi,\Phi'], \tag{5.27}$$

where $N_{B/F} : B \to F$ is the reduced norm map.

Define $\kappa^* = (-\kappa_2, 1-\kappa_1)$ and $\varepsilon^* = \varepsilon^{-1}$. Thus $[\kappa^*] \leq 1 \Leftrightarrow [\kappa] \geq 0$. Then the pairing $[\ ,\ ]$ induces $U_0(\mathfrak{N})F_{\mathbb{A}}^{\times}$–equivariant pairing

$$[\ ,\ ] : L(\kappa\varepsilon; A) \times L(\kappa^*\varepsilon^*; A) \to A.$$

We now choose $q = |I_B| = \dim_{\mathbb{C}} \mathfrak{H}^{I_B}$. Then the cup product pairing induces ([H94] (5.3)) a non-degenerate pairing:

$$(\ ,\ ) : H^q_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W)) \times H^q_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa^*\varepsilon^*; W)) \to W \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Thus we obtain from Proposition 5.1 the following result:

Proposition 5.2. *Let $V = H^q_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W))$. Let V^* be the dual W–lattice of V in $H^q_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa^*\varepsilon^*; W \otimes_{\mathbb{Z}} \mathbb{Q}))$ under the Poincaré duality:*

$$(\ ,\ ) : H^q_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W)) \times H^q_{cusp}(Y_0^B(\mathfrak{N}), L^*(\kappa^*\varepsilon^*; W)) \to W \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then we have a $h_\kappa(\mathfrak{N}, \varepsilon; W)$–linear map

$$f : V \otimes_W V^* \to S_\kappa(\mathfrak{N}, \varepsilon; W)$$

defined by the q–expansion:

$$f(v \otimes w) = \mathcal{N}(y)^{-1} \sum_{0 \ll \xi} (v|\mathbb{T}(\xi y d), w) q^\xi,$$

where we regard $V \otimes_W V^*$ as an $h_\kappa(\mathfrak{N}, \varepsilon; W)$–module through the left factor V.

A similar fact for the matrix coefficients of $T(y)$ in place of $(v|T(y), w)$ has been proven in [Sh2] Theorem 3.1 by analytic means without using the Jacquet-Langlands-Shimizu correspondence.

We have $H^q_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W)) = H^q(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W))$ under the following two conditions:

(V1) The character $\kappa\varepsilon : T_0(\widehat{O}) \to W^\times$ does not factor through the reduced norm map $N : T_0(\widehat{O}^{(d(B))}) \hookrightarrow G(\widehat{O}^{(d(B))}) \to (\widehat{O}^{(d(B))})^\times$. In particular, if $\kappa_1 \neq \kappa_2$, this condition is satisfied.

(V2) The quaternion algebra B is a division algebra. In particular, this condition is satisfied if $|I_B| < [F : \mathbb{Q}]$.

6. Ordinary cohomology groups

We are going to prove that the morphism $f : V(R) \otimes_W V(R) \to S(R)$ in Proposition 5.1 for V in Proposition 5.2 is surjective for the nearly ordinary local ring R (associated to a mod p irreducible Galois representation), when B is unramified at every finite place and $q = |I_B| \leq 1$. A key to the proof is the R–freeness of $V(R)$ proven by Fujiwara [Fu] (see [HMI] Corollary 3.42). Another important ingredient of the proof is the self duality of $V(R)$ over W.

6.1. Freeness as Hecke modules. We recall here a special case of Fujiwara's result in [Fu] "Freeness Theorem" of the component $V(R)$ for a local ring R of the Hecke algebra $h_\kappa(\mathfrak{N},\varepsilon;W)$ (see also [HMI] Corollary 3.42). To state the result, we need to have a good description of the modular nearly ordinary Galois representation; so, we recall the description. We call a local ring R of $h_\kappa(\mathfrak{N},\varepsilon;W)$ nearly ordinary if the projection of $\mathbb{T}(p)$ to R is a unit. We hereafter always assume

(ord) *R is nearly ordinary with $\kappa_1-\kappa_2\geq I$, that is, $\kappa_{1,\sigma}-\kappa_{2,\sigma}\geq 1$ for all σ.*

(unr) *$F/\mathbb{Q}$ is unramified at $\mathbb{Q}$.*

We write $\mathfrak{N}'$ for the product of primes $\mathfrak{l}\nmid p$ for which one of ε_1 and ε_2 ramifies; so, $\mathfrak{N}'\subset\mathfrak{N}^{(p)}$. For a W–algebra homomorphism $\lambda:h_\kappa(\mathfrak{N},\varepsilon;W)\to W$ factoring through R (such a λ is called *nearly ordinary*), we have a Galois representation $\rho=\rho_\lambda:\mathrm{Gal}(\overline{F}/F)\to GL_2(W)$ (e.g. [H96] 2.8 and [MFG] 5.6.1) such that

(G1) ρ is continuous and is absolutely irreducible over $W\otimes_{\mathbb{Z}}\mathbb{Q}$;

(G2) ρ is unramified outside $\mathfrak{N}'p$;

(G3) For primes $\mathfrak{l}$ outside $\mathfrak{N}'p$, we have
$$\det(1_2-\rho(Frob_{\mathfrak{l}})X)=1-\lambda(T(\mathfrak{l}))X+\lambda(\langle\mathfrak{l}\rangle)X^2;$$

(G4) For the decomposition group $D_{\mathfrak{p}}\subset\mathrm{Gal}(\overline{F}/F)$ at each prime $\mathfrak{p}|p$, we have an exact sequence of $D_{\mathfrak{p}}$–modules: $0\to\epsilon_{\mathfrak{p}}\to\rho|_{D_{\mathfrak{p}}}\to\delta_{\mathfrak{p}}\to 0$ with one dimensional character $\delta_{\mathfrak{p}}$ satisfying $\delta_{\mathfrak{p}}([y;F_{\mathfrak{p}}])=\lambda(\mathbb{T}(y))$ for the local Artin symbol $[y;F_{\mathfrak{p}}]$ of $y\in F_{\mathfrak{p}}^\times$.

Writing $\mathbb{F}$ for the residue field of W, the semi-simplification $\overline{\rho}=\overline{\rho}_R$ of the reduction of ρ modulo the maximal ideal $\mathfrak{m}_W$ of W is independent of λ by (G2-3) (cf. [MFG] Corollary 2.8 combined with the Chebotarev density). In particular, if $\overline{\rho}$ is irreducible, the isomorphism class of $\rho \mod \mathfrak{m}_W$ for the maximal ideal $\mathfrak{m}_W$ is unique, and always we have $(\rho \mod \mathfrak{m}_W)\cong\overline{\rho}$.

We shall recall some terminology from (formal) deformation theory of Galois representations. See [MFG] Section 2.3 for basics of formal deformation theory of representations. Let H be a subgroup of $\mathrm{Gal}(\overline{F}/F)$. We call a representation $\rho:H\to GL_2(A)$ for a local proartinian W–algebra A with residue field $\mathbb{F}$ a *deformation* over H of $\overline{\rho}$ if $\rho\equiv\overline{\rho}|_H \mod \mathfrak{m}_A$. Let $\chi=\det(\rho_\lambda)/\mathcal{N}^{[\kappa]}$ for the p–adic cyclotomic character $\mathcal{N}$. Then χ is of finite order. For any character $\varphi:D_{\mathfrak{l}}\to A^\times$, let $C(\varphi)$ denote the conductor of φ; thus, $C(\varphi)=1$ if φ is unramified, and $C(\varphi)=\mathfrak{l}^m$ if $y\mapsto\varphi([y,F_{\mathfrak{l}}])$ factors through $F_{\mathfrak{l}}^\times/(1+\mathfrak{l}^mO_{\mathfrak{l}})$ but not $F_{\mathfrak{l}}^\times/(1+\mathfrak{l}^{m-1}O_{\mathfrak{l}})$ for $m>0$. We assume the following four conditions on ρ_λ:

(H1) χ is of order prime to p.

(H2) For primes $\mathfrak{l}|\mathfrak{N}p$, write $D_{\mathfrak{l}}$ for the decomposition group at $\mathfrak{l}$. Then we have $\rho|_{D_{\mathfrak{p}}}\cong\left(\begin{smallmatrix}\epsilon_{\mathfrak{l}} & *\\ 0 & \delta_{\mathfrak{l}}\end{smallmatrix}\right)$ with $\delta([y,F_{\mathfrak{l}}])=\lambda(\mathbb{T}(y))$. This condition actually follows for $\mathfrak{l}|p$ from near ordinarity of λ as already remarked in (G4).

(H3) If a prime $\mathfrak{l}|\mathfrak{N}$ but $\mathfrak{l}\nmid p$, then the restriction of $\delta_{\mathfrak{l}}$ and $\epsilon_{\mathfrak{l}}$ to the inertia subgroup $I_{\mathfrak{l}}$ of $D_{\mathfrak{l}}$ is of order prime to p.

(H4) If $\epsilon_{\mathfrak{p}} \equiv \delta_{\mathfrak{p}}\mathcal{N} \mod \mathfrak{m}_W$ on $I_{\mathfrak{p}}$ for a prime $\mathfrak{p}|p$, the following five conditions have to be met: (i) the character $\epsilon_{\mathfrak{p}}$ is of order prime to p, (ii) $\kappa = (I, 0)$, (iii) $\rho_\lambda|_{I_{\mathfrak{p}}}$ is associated to a p–divisible group over an unramified extension of $O_{\mathfrak{p}}$, (iv) $\mathfrak{p} \nmid \mathfrak{N}$, and (v) $\epsilon_{\mathfrak{p}}\delta_{\mathfrak{p}}^{-1}(y)y^{-I} = 1$ for all $y \in O_{\mathfrak{p}}^{\times}$.

We write $\overline{\delta}_{\mathfrak{l}} = (\delta_{\mathfrak{l}} \mod \mathfrak{m}_W)$ and $\overline{\epsilon}_{\mathfrak{l}} = (\epsilon_{\mathfrak{l}} \mod \mathfrak{m}_W)$. We assume the following two local conditions on $\overline{\rho}$.

(H5) For all $\mathfrak{p}|p$, $\overline{\delta}_{\mathfrak{p}} \neq \overline{\epsilon}_{\mathfrak{p}}$.

(H6) For $\mathfrak{l}|\mathfrak{N}$ and $\mathfrak{l} \nmid p$, the $\mathfrak{l}$–primary part of $\mathfrak{N}$ coincides with $C(\overline{\epsilon}_{\mathfrak{l}}\overline{\delta}_{\mathfrak{l}}^{-1})$.

Thus $\overline{\rho}$ could ramify at a prime $\mathfrak{l} \nmid \mathfrak{N}$, and by (H3), $\mathfrak{N}'$ gives the product of primes (outside p) at which $\overline{\rho}$ ramifies. We assume the following global condition on $\overline{\rho}$:

(H7) $\overline{\rho}$ is absolutely irreducible over $\mathrm{Gal}(\overline{F}/F[\sqrt{p^*}])$ for $p^* = (-1)^{(p-1)/2}p$.

We choose a quaternion algebra $B_{/F}$ so that $d(B) = 1$ and ramified at most infinite places (that is I^B is as large as possible). This implies:

$$I_B = \{\sigma_1\} \text{ if } [F:\mathbb{Q}] \text{ is odd, and } I_B = \emptyset \text{ if } [F:\mathbb{Q}] \text{ is even.} \tag{6.1}$$

We now quote the following special case of "Freeness Theorem" in Section 0 in [Fu] (see [HMI] Corollary 3.42 for a proof of this Fujiwara's result):

Theorem 6.1. *Suppose the conditions* (6.1), (ord), (unr), (H1-7) *and* $p > 3$. *Then* $V(R)$ *for* $V = H^q(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W))$ $(q = |I_B|)$ *is free of rank* 2^q *over the local ring R. Even if we ease the condition* (H4) *to allow the case where the* $\mathfrak{p}$*–primary part of* $\mathfrak{N}$ *is equal to* $\mathfrak{p}$ *for primes* $\mathfrak{p}|p$*, the same assertion holds as long as* $[F:\mathbb{Q}]$ *is even.*

This is a special case of Fujiwara's result. In particular, we do not need to assume unramifiedness of p in F, but we use the assumption (unr) anyway in our later application; so, we have imposed it.

Proof. Here is a brief account of how to deduce the above theorem either from [HMI] Corollary 3.42 or from [Fu], because the set of the assumptions imposed in these works appears different. In [HMI] Corollary 3.42, the theorem is proven under the assumptions:

(A) $[F:\mathbb{Q}]$ is even;

(B) $\kappa = (I, 0)$;

(C) the assumptions (H1–3) and (H5–7);

(D) the milder condition than (H4) as stated in the theorem.

As can be easily seen, the conditions (A–D) implies the assumptions actually stated in Corollary 3.42 of [HMI]: the absolute irreducibility of $\overline{\rho}$ over $F[\mu_p]$ (written as $(\mathrm{ai}_F[\mu_p])$ in [HMI]) which follows from (H7), the conditions (h1–4) in [HMI] 3.2.1, (ds_Q) which is (H5) and (H6), and the conditions (Q1–6) (for $Q = \emptyset$) in [HMI] Section 3.2.1. These conditions exhaust all the assumptions of Corollary 3.42 of [HMI] except for the condition (sm1). The condition: $p > 3$ and the unramifiedness of p in $F/\mathbb{Q}$ implies $[F[\mu_p]:F] > 2$, which is the last assumption (sm1) in Corollary 3.42 of [HMI]. We only use this theorem under the four conditions (A–D); so, logically, for the proof of the main theorem of this paper, it is sufficient to quote [HMI] Corollary 3.42.

For the sake of completeness, we now reduce the theorem in the case not covered under (A–D) to [Fu] (the version of 1999). Recall that $\mathfrak{N}'$ is the product of all primes (outside p) at which $\overline{\rho}$ ramifies. We consider an open compact subgroup $U(\overline{\rho}) = \prod_{\mathfrak{l}} U_{\mathfrak{l}}(\overline{\rho}) \subset U_0(\mathfrak{N})$ and a character $\nu_{\mathfrak{l}}$ of $U_{\mathfrak{l}}(\overline{\rho})$ with values in $W^{\times}$ defined as follows:

(1) $U_{\mathfrak{l}}(\overline{\rho}) = GL_2(O_{\mathfrak{l}})$ in $B_{\mathfrak{l}}^{\times}$ if $\mathfrak{l} \nmid \mathfrak{N}p$, and $\nu_{\mathfrak{l}}$ is the trivial character;

(2) Suppose that $\mathfrak{l}|\mathfrak{N}'$. If $\overline{\epsilon}_{\mathfrak{l}} \neq \overline{\delta}_{\mathfrak{l}}$ on $I_{\mathfrak{l}}$, then $\mathfrak{l}|\mathfrak{N}$,

$$U_{\mathfrak{l}}(\overline{\rho}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in U_0(\mathfrak{N})_{\mathfrak{l}} \middle| a \equiv 1 \mod \mathfrak{l}, (d \mod \mathfrak{l}) \text{ is of } p\text{–power order} \right\}$$

and $\nu_{\ell}(u) = \delta_{\mathfrak{l}}([\det(u), F_{\mathfrak{l}}])$. If $\overline{\epsilon}_{\mathfrak{l}} = \overline{\delta}_{\mathfrak{l}}$ on $I_{\mathfrak{l}}$, $U_{\mathfrak{l}}(\overline{\rho}) = GL_2(O_{\mathfrak{l}})$ (so $\mathfrak{l} \nmid \mathfrak{N}$) and $\nu_{\mathfrak{l}}(u) = \delta_{\mathfrak{l}}([\det(u), F_{\mathfrak{l}}])$.

(3) For $\mathfrak{p}|p$, define $\nu_{\mathfrak{p}}(u) = \epsilon_{\mathfrak{p}}([\det(u), F_{\mathfrak{p}}])(\det(u))^{-\kappa_2}$ for $u \in GL_2(O_{\mathfrak{p}})$, which is a finite order character and can be regarded as a character with values in $W^{\times}$. If $\overline{\epsilon}_{\mathfrak{p}} \neq \overline{\delta}_{\mathfrak{p}}\overline{\omega}$ on $I_{\mathfrak{p}}$ for $\overline{\omega} = (\mathcal{N} \mod \mathfrak{m}_W)$, then $\mathfrak{p}|\mathfrak{N}$ and

$$U_{\mathfrak{p}}(\overline{\rho}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in U_0(p)_{\mathfrak{p}} \middle| a \equiv 1 \mod \mathfrak{p}, (d \bmod \mathfrak{p}) \text{ is of } p\text{–power order} \right\}.$$

If $\overline{\epsilon}_{\mathfrak{p}} = \overline{\delta}_{\mathfrak{p}}\overline{\omega}_{\mathfrak{p}}$ on $I_{\mathfrak{p}}$, then $U_{\mathfrak{p}} = GL_2(O_{\mathfrak{p}})$ (and $\mathfrak{p} \nmid \mathfrak{N}$).

Let $U = \mathrm{Ker}(\prod_{\mathfrak{l}} \nu_{\mathfrak{l}} : U(\overline{\rho}) \to W^{\times})$. Since the restriction of operators of $h_{\kappa}(U, \varepsilon; W)$ to $S_{\kappa}(\mathfrak{N}, \varepsilon; W)$ induces a surjective algebra homomorphism $\pi : h_{\kappa}(U, \varepsilon; W) \twoheadrightarrow h_{\kappa}(\mathfrak{N}, \varepsilon; W)$, we have a unique local ring R_U of $h_{\kappa}(U, \varepsilon; W)$ through which $\lambda \circ \pi$ factors. Then R_U is nearly ordinary. For a smaller open compact subgroup U' with $U(\mathfrak{N}\mathfrak{q}) \subset U' \subset U$ for a suitable prime $\mathfrak{q}$ outside $\mathfrak{N}'p$, it is proven in [Fu] that

(1) For all $x \in G(\mathbb{A}^{(\infty)})$, $\overline{\Gamma}_{U',x}$ is torsion-free and acts on $\mathfrak{H}^{I_B}$ freely;

(2) The action of $\Gamma_{U',x}$ on $L(\kappa\varepsilon; A)$ factors through $\overline{\Gamma}_{U',x}$ for all $x \in G(\mathbb{A}^{(p\infty)})$;

(3) The Hecke algebra $h_{\kappa}(U', \varepsilon; W)$ has a local ring R' with $R' \cong R$ as W–algebras;

(4) Let $V_U = H^q(Y^B(U), L)$ and $V' = H^q(Y^B(U'), L)$ for $L = L(\kappa\varepsilon; W))$ and $q = |I_B|$. Then the restriction map Res : $H^q(Y_0^B(\mathfrak{N}), L) \to H^q(Y^B(U), L)$ composed with the multiplication by the idempotent of R' induces a W–linear map: $V_U(R_U) \cong V'(R')$ which is $\mathbb{T}(y)$–equivariant as long as $y_{\mathfrak{q}} = 1$;

(5) R_U is generated by $\mathbb{T}(y)$ with $y_{\mathfrak{q}} = 1$;

(6) $V'(R') \cong R'^{r}$ for some r.

In [Fu], U' and U are written as $K_{\mathcal{D},y}$ and $K_{\mathcal{D}}$, respectively. This is enough to conclude that $V(R_U)$ is R_U–free. On the other hand, for the Sylow p–subgroup S of $U_0(\mathfrak{N})/U$, R_U is $W[S]$–free of finite rank. Then $R \cong R_U \otimes_{W[S],\varepsilon} W$, where ε is the algebra homomorphism $W[S] \to W$ induced by the character ε of S.

This fact follows from the freeness of the Hecke algebra over the group algebra (under (unr) and $p > 2$), for example, [H02] Corollary 4.3, [H05a] Corollary 9.3 or [PAF] 4.2.11–12. In the above papers, the symbol N is used for the prime-to-p–part of the present level $\mathfrak{N}$. Similarly, V_U is $W[S]$–free of finite rank by [H89] Theorem 3.8. Thus we have

$$V(R) = V_U(R) \otimes_{W[S],\varepsilon} W \cong (R_U \otimes_{W[S],\varepsilon} W)^r \cong R^r$$

for a suitable integer r. Actually $r = 2^q \leq 2$, because $V \otimes \mathbb{Q}$ is of rank 2^q over the (rational) Hecke algebra.

As for the easing of the condition (H4) on $\mathfrak{N}$, it follows from the same argument, replacing $\mathfrak{N}$ by $\mathfrak{N} \cap \prod_{\mathfrak{p}\in P} \mathfrak{p}$, because this is the case where the deformation is unrestricted at $\mathfrak{p} \in P$, which has been dealt with in [Fu] assuming that, for example, $[F : \mathbb{Q}]$ is even (see [HMI] Section 3.2). □

By the theory of p–adic analytic families of nearly ordinary cusp forms (see [H89], [H96] Section 2.7 and [HMI] 3.2.8, 3.3.4 and 4.3.9), we can ease slightly the conditions necessary to have freeness of $V(R)$ over R. We shall describe this generalization for our later use. Let $\mathbf{G} = \mathbf{G}(\mathfrak{N}') = Cl_F^+(\mathfrak{N}'p^\infty) \times (O_p \times O/\mathfrak{N}'^{(p)})^\times$, where $Cl_F^+(\mathfrak{N}'p^n)$ is the strict ray class group modulo $\mathfrak{N}'p^n$ of F, and

$$Cl_F^+(\mathfrak{N}'p^\infty) = \varprojlim_n Cl_F^+(\mathfrak{N}'p^n) = F_\mathbb{A}^\times / F^\times U_F(\mathfrak{N}')^{(p)} F_{\infty+}^\times$$

with $U_F(\mathfrak{N}') = \widehat{O}^\times \cap (1+\mathfrak{N}'\widehat{O})$. We have a natural homomorphism $\iota : T_0(O_p) \to \mathbf{G}$ sending (a, b) to $(a^{-1}, a^{-1}b)$. Each element $(z, y) \in \mathbf{G}$ acts on $f \in S_\kappa(U, \varepsilon; A)$ by $f|(z, y)(x) = f|\mathbb{T}(y)(xz)$ (for $U \subset U_0(\mathfrak{N}')$). Let Γ_0 be the maximal torsion-free quotient of $\mathbf{G}$ (which is independent of $\mathfrak{N}'$ up to isomorphisms), and fix a splitting $\mathbf{G} = \Gamma_0 \times \mathbf{G}_{tor}$. We consider the Iwasawa algebra $W[[\Gamma_0]]$. For an integral domain $\mathbb{I}$ finite flat over $W[[\Gamma_0]]$, we define

$$\mathcal{A}(\mathbb{I}) = \left\{P \in \mathrm{Hom}_W(\mathbb{I}, \overline{\mathbb{Q}}_p)\middle| P \circ \iota \sim \kappa \text{ with } \kappa_1 - \kappa_2 \geq I \text{ and } [\kappa] \geq 0\right\},$$

where $\varphi \sim \psi$ if $\varphi = \psi$ locally on $T_0(O_p)$ (in other words, $\varphi\psi^{-1}$ is of finite order). For each $P \in \mathcal{A}(\mathbb{I})$, we write $\kappa(P)$ and ε_P for the corresponding algebraic character of T_0 and the character of

$$g = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) z \in T_0(O_p \times (O/\mathfrak{N}'^{(p)}) F_\mathbb{A}^\times \subset GL_2(F_\mathbb{A})$$

given by $\mathbf{G} \ni g \mapsto P(T(ab^{-1}))P(\langle bz \rangle)\varepsilon_{tor}(g)$, where ε_{tor} is the restriction of ε to the torsion part $\mathbb{G}_{tor}$ (regarded as a character of $\mathbf{G}$). Thus we can form a triple $(\varepsilon_{P,1}, \varepsilon_{P,2}, \varepsilon_{P+})$ out of ε_P so that $\varepsilon_P(g) = \varepsilon_{P,1}(a)\varepsilon_{P,2}(b)\varepsilon_{P+}(z)$. For a given nearly ordinary Hecke eigenform $f \in S_\kappa(\mathfrak{N}, \varepsilon; W)$ with $\kappa_1 - \kappa_2 \geq I$, decomposing $\mathbf{G}$ into a product $\Gamma_0 \times \Delta$ for a finite subgroup Δ, we write $\varepsilon(P) = \varepsilon_P \varepsilon|_\Delta$. Thus for a suitable $P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ whose weight is κ, we find $\varepsilon(P) = \varepsilon$. Then there exist $\mathbb{I}_{/W[[\Gamma_0]]}$ as above and a unique family of Hecke eigenforms $\{f_P\}_{P\in\mathcal{A}(\mathbb{I})}$ containing f and satisfying the following two conditions:

(1) $f_P \in S_{\kappa(P)}(\mathfrak{N}_P, \varepsilon(P); W[\varepsilon_P])$ for the conductor $\mathfrak{N}_P$ of the character $\varepsilon(P)^-$, where $W[\varepsilon_P]$ is a subring of $\overline{\mathbb{Q}}_p$ generated over W by the values of ε_P;

(2) There exists a function $\mathbf{a} : F_{\mathbb{A}}^\times \to \mathbb{I}$ such that $\mathbf{a}_p(y, f_P) = \mathbf{a}(y)(P)$ for all $y \in F_{\mathbb{A}}^\times$ and all $P \in \mathcal{A}(\mathbb{I})$.

Corollary 6.2. *Let $\{f_P\}_{P\in\mathcal{A}(\mathbb{I})}$ be the family of nearly p–ordinary Hecke eigenforms as above. Write R_P be the local ring of $h_{\kappa(P)}(\mathfrak{N}_P, \varepsilon(P); W[\varepsilon_P])$ through which the algebra homomorphism λ_P of the Hecke algebra given by $f_P|\mathbb{T}(y) = \lambda_P(\mathbb{T}(y))f_P$ factors. If one member $f \in S_\kappa(\mathfrak{N}, \varepsilon; W)$ satisfies the assumptions* (H1-7)*, $V(R_P)$ is R_P–free of rank 2^q, where $V = H^q(Y_0^B(\mathfrak{N}_P), L(\kappa(P)\varepsilon(P); W[\varepsilon_P]))$ and $q = 0, 1$ by* (6.1)*.*

Proof. We choose U' as in the proof of Theorem 6.1 and write $U_0'(\mathfrak{N}') = U' \cap U_0(\mathfrak{N}')$. We consider the limit $\mathcal{V} = \varinjlim_n H^q_{n.ord}(Y^B(U' \cap U(p^n)), L(\kappa\varepsilon; W) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$, where $H^q_{n.ord} = eH^q$ for the idempotent $e = \lim_{n\to\infty} \mathbb{T}(p)^{n!}$. The module $\mathcal{V}$ is naturally a module over $\mathbf{G}(\mathfrak{N}')$ and hence over $W[[\Gamma_0]]$. Then in the same manner in [H89] Corollary 3.5 and Theorem 3.8, we can prove that for the Pontryagin dual $\mathbf{V}'$ of $\mathcal{V}$,

$$\mathbf{V}'/P\mathbf{V}' \cong H^q_{n.ord}(Y^B(U_0'(\mathfrak{N}_P)), L(\kappa(P)\varepsilon(P); W[\varepsilon_P]))$$

as Hecke modules and that $\mathbf{V}'$ is $W[[\Gamma_0]]$–free module of finite rank. We write V_P' for the Hecke module of the right-hand-side of the above formula. Then we define $\mathbf{h}' \subset \mathrm{End}_{W[[\Gamma_0]]}(\mathbf{V}')$ by the $W[[\Gamma_0]]$–subalgebra generated by $\mathbb{T}(y)$ for all integral ideles y. As proved under (unr) and $p > 3$ in [PAF] Corollaries 4.31–32 or [H02] Corollary 4.3 (where the assumption is $p > 2$ and N denotes the prime-to–p part of the present $\mathfrak{N}'$), $\mathbf{h}'$ is $W[[\Gamma_0]]$–algebra free of finite rank, whose rank is equal to $\mathrm{rank}_{W[\varepsilon_P]} h_P'$ for $h_P' = h^{n.ord}_{\kappa(P)}(U_0'(\mathfrak{N}\mathfrak{p}^{e(P)}), \varepsilon(P); W[\varepsilon_P])$. Since they have the same generators $\mathbb{T}(y)$'s, $\mathbf{h}'/P\mathbf{h}'$ surjects down to h_P'. By comparing their rank over $W[\varepsilon_P]$, we find $\mathbf{h}'/P\mathbf{h}' \cong h_P'$ canonically sending $\mathbb{T}(y)$ to $\mathbb{T}(y)$. Since R' is the direct summand of $h_{P_0}' \subset h_\kappa(\mathfrak{N}, \varepsilon; W)$, by Hensel's lemma (cf. [BCM] III.4.6), $\mathbf{h}'$ has a unique local ring $\mathbf{R}' \subset \mathbf{h}'$ with $\mathbf{R}'/P_0\mathbf{R}' \cong R'$. We put $\mathbf{V}'(\mathbf{R}') = \mathbf{R}'\mathbf{V}'$, which is $W[[\Gamma_0]]$–free module of finite rank. Since $\mathbf{V}'(\mathbf{R}')/P_0\mathbf{V}'(\mathbf{R}') \cong V'(R')$, which is a free of finite rank over $R' = \mathbf{R}'/P_0\mathbf{R}'$, we choose a lift $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ in $\mathbf{V}'$ of a base of $V'(R')$ over R'. Then the $\mathbf{R}'$–linear map $\pi : \mathbf{R}'^r \to \mathbf{V}'(\mathbf{R}')$ given by $(h_1, \ldots, h_r) \mapsto \sum_j h_j\mathbf{v}_j$ is surjective by Nakayama's lemma applied to $\mathbf{R}'$ and ideal P_0. By comparing the rank over $W[[\Gamma_0]]$, we find that π is an isomorphism. Thus $\mathbf{V}'(\mathbf{R}')$ is free of rank $r = 2^q$ over $\mathbf{R}'$.

We define R_P' by $R_P' = \mathbf{R}/P\mathbf{R} \subset h_P'$. Then $R_P' \cong R_P$ canonically, and $V_P'(R_P') \cong V_P(R_P)$ for $V_P = H^q_{n.ord}(U_0'(\mathfrak{N}_P), L(\kappa(P)\varepsilon(P); W[\varepsilon_P])$ in the same manner as in the proof of Theorem 6.1. This finishes the proof. □

6.2. Induced representations. We are going to verify the assumption of the freeness theorem: Theorem 6.1 for induced representations from CM fields.

We first recall a cusp form f on $GL_2(F_{\mathbb{A}})$ with complex multiplication by a CM field M. Let M/F be a CM field with integer ring R and choose a CM type Σ:

$$I_M = \mathrm{Hom}_{\mathrm{field}}(M, \overline{\mathbb{Q}}) = \Sigma \sqcup \Sigma c$$

for complex conjugation c. To assure the assumption (ord), we need to assume that the CM type Σ is p–ordinary, that is, the set Σ_p of p–adic places induced by $i_p \circ \sigma$ for $\sigma \in \Sigma$ is disjoint from $\Sigma_p c$ (its conjugate by the generator c of $\mathrm{Gal}(M/F)$). The existence of such an ordinary CM type implies that all prime factors of p in F split in M/F. For each $k \in \mathbb{Z}[I]$, we write $k\Sigma = \sum_{\sigma \in \Sigma} k_{\sigma|F}\sigma$.

We choose $\kappa_1 > \kappa_2$ with $\kappa_1 + \kappa_2 = [\kappa]I$ for an integer $[\kappa]$. We then choose a Hecke character λ of conductor $\mathfrak{C}\mathfrak{P}^e$ ($\mathfrak{C}$ prime to p) such that

$$\lambda((\alpha)) = \alpha^{\kappa_1\Sigma + c\kappa_2\Sigma} \ \text{ for } \alpha \in M^\times \text{ with } \alpha \equiv 1 \mod \mathfrak{C}\mathfrak{P}^e,$$

where $\mathfrak{P}^e = \prod_{\mathfrak{P} \in \Sigma_p} \left(\mathfrak{P}^{e(\mathfrak{P})}\mathfrak{P}^{ce(\mathfrak{P}^c)}\right)$ for $e = \sum_{\mathfrak{P} \in \Sigma_p \sqcup \Sigma_p c} e(\mathfrak{P})\mathfrak{P}$. We also decompose $\mathfrak{C} = \prod_{\mathfrak{L}} \mathfrak{L}^{e(\mathfrak{L})}$ for prime ideals $\mathfrak{L}$ of M. We extend λ to a p–adic idele character $\widehat{\lambda} : M_{\mathbb{A}}^\times/M^\times M_\infty^\times \to \overline{\mathbb{Q}}_p^\times$ so that $\widehat{\lambda}(a) = \lambda(aO)a_p^{-\kappa_1\Sigma - c\kappa_2\Sigma}$. By class field theory, we may regard $\widehat{\lambda}$ as a character of $\mathrm{Gal}(\overline{F}/M)$. Any character φ of $\mathrm{Gal}(\overline{F}/M)$ of the form $\widehat{\lambda}$ as above is called "of weight κ". For a prime ideal $\mathfrak{L}$ of M outside p, we write $\lambda_{\mathfrak{L}}$ for the restriction of $\widehat{\lambda}$ to $M_{\mathfrak{L}}^\times$. For $\mathfrak{P} \in \Sigma_p$, we define $\lambda_{\mathfrak{P}}(x) = \widehat{\lambda}(x)x^{\kappa_1\Sigma}$ for $x \in M_{\mathfrak{P}}^\times$ and $\lambda_{\mathfrak{P}^c}(x) = \widehat{\lambda}(x)x^{c\kappa_2\Sigma}$ for $x \in M_{\mathfrak{P}^c}^\times$. Then $\lambda_{\mathfrak{L}}$ for all prime ideals $\mathfrak{L}$ is a continuous character of $M_{\mathfrak{L}}^\times$ with values in $\overline{\mathbb{Q}}$ whose restriction to $R_{\mathfrak{L}}^\times$ is of finite order. By the condition $\kappa_1 > \kappa_2$, $\widehat{\lambda}$ cannot be of the form $\widehat{\lambda} = \phi \circ N_{M/F}$ for an idele character $\phi : F_{\mathbb{A}}^\times/F^\times F_{\infty+}^\times \to \overline{\mathbb{Q}}_p^\times$.

We define a function $F_{\mathbb{A}}^\times \ni y \mapsto \mathbf{a}_p(y, \theta(\lambda))$ supported by integral ideles by

$$\text{(6.2)} \qquad \mathbf{a}_p(y, \theta(\lambda)) = \sum_{x \in M_{\mathbb{A}}^\times, xx^c = y, x_{\Sigma_p} = 1} \widehat{\lambda}(x) \ \text{ if } y \text{ is integral.}$$

where x runs over elements in $M_{\mathbb{A}(\infty)}^\times/(\widehat{R}^{(p\mathfrak{C}\mathfrak{C}^c)})^\times$ satisfying the following three conditions: (i) xR is an integral ideal of M, (ii) $N_{M/F}(x) = y$ and (iii) $x_{\mathfrak{Q}} = 1$ for primes $\mathfrak{Q}$ in Σ_p and $\mathfrak{Q}|\mathfrak{C}$. The q–expansion determined by the coefficients $\mathbf{a}_p(y, \theta(\lambda))$ gives a unique element $\theta(\lambda) \in S_\kappa(\mathfrak{N}', \varepsilon'_\lambda; \overline{\mathbb{Q}})$ ([HT1] Theorem 6.1), where $\mathfrak{N}' = N_{M/F}(\mathfrak{C}\mathfrak{P}^e)d(M/F)$ for the discriminant $d(M/F)$ of M/F and ε'_λ is a suitable "Neben" character.

We decompose $\mathfrak{C} = \mathfrak{F}\mathfrak{F}^c\mathfrak{I}$ so that $\mathfrak{F}\mathfrak{F}_c$ is a product of split primes and $\mathfrak{I}$ for the product of inert or ramified primes, $\mathfrak{F} + \mathfrak{F}_c = R$ and $\mathfrak{F} \subset \mathfrak{F}_c^c$. We put $\mathfrak{f} = \mathfrak{F} \cap F$ and $\mathfrak{i} = \mathfrak{I} \cap F$. Assuming that λ^- has split conductor, we describe the Neben character ε_λ of the minimal form $f(\lambda)$ in the automorphic representation $\pi(\lambda)$ generated by $\theta(\lambda)$. The character ε_λ is possibly different from ε'_λ and is given as follows:

(1) For $\mathfrak{l}|\mathfrak{f}$, we identify $T_0(O_\mathfrak{l}) = O_\mathfrak{l}^\times \times O_\mathfrak{l}^\times$ with $R_{\mathfrak{L}^c}^\times \times R_\mathfrak{L}^\times$ with this order for the prime ideal $\mathfrak{L}|(\mathfrak{l}R \cap \mathfrak{F})$. We define $\varepsilon_{\lambda,\mathfrak{l}}$ by the restriction of $\lambda_{\mathfrak{L}^c} \times \lambda_\mathfrak{L}$ to $T_0(O_\mathfrak{l})$.

(2) For $\mathfrak{p}|p$, identify $T_0(O_\mathfrak{p})$ with $R_{\mathfrak{P}^c}^\times \times R_\mathfrak{P}^\times$ for $\mathfrak{P}|\mathfrak{p}$ in Σ_p, we define $\varepsilon_{\lambda,\mathfrak{p}}$ by the restriction of $\lambda_{\mathfrak{P}^c} \times \lambda_\mathfrak{P}$ to $T_0(O_\mathfrak{p})$.

(3) For $\mathfrak{l}|\mathfrak{i}d(M/F)$, we choose a character $\phi_\mathfrak{l} : F_\mathfrak{l}^\times \to \mathbb{C}^\times$ such that $\lambda_\mathfrak{L} = \phi_\mathfrak{l} \circ N_{M_\mathfrak{L}/F_\mathfrak{l}}$ (this is possible because λ^- has split conductor). Then we define $\varepsilon_{\lambda,1,\mathfrak{l}}(a) = \phi_\mathfrak{l}$ and $\varepsilon_{\lambda,2,\mathfrak{l}}(d) = \left(\frac{M_\mathfrak{L}/F_\mathfrak{l}}{d}\right)\lambda_\mathfrak{L}(d)$, where $\mathfrak{L}$ is the prime factor of $\mathfrak{l}$ in M and $\left(\frac{M_\mathfrak{L}/F_\mathfrak{l}}{d}\right)$ is the quadratic residue symbol for $M_\mathfrak{L}/F_\mathfrak{l}$.

(4) The central character $\varepsilon_{\lambda+}$ is given by the product of the restriction of λ to $F_\mathbb{A}^\times$ and the quadratic character $\left(\frac{M/F}{}\right)$ of the CM field M/F.

We now give an explicit description of $f(\lambda)$ without assuming that λ^- has split conductor. Let Ξ_{pr} be the set of prime factors $\mathfrak{l}$ of $\mathfrak{N}' = d(M/F)N_{M/F}(\mathfrak{C}\mathfrak{P}^e)$ where $\pi_\mathfrak{l}$ is principal. If λ^- has split conductor, Ξ_{pr} is the full set of prime factors of $\mathfrak{N}'$. Otherwise, $\mathfrak{l} \in \Xi_{pr}$ if and only if either $\mathfrak{l}|\mathfrak{f}$ or $\mathfrak{l}|\mathfrak{i}$ and

$$\lambda_\mathfrak{L}(x) = \phi_\mathfrak{l}(xx^c) \text{ for a character } \phi_\mathfrak{l} : F_\mathfrak{l}^\times \to \mathbb{C}^\times. \tag{6.3}$$

For $\mathfrak{l} \in \Xi_{pr}$, taking a prime $\mathfrak{L}|\mathfrak{l}$ in M, we have

$$\pi_\mathfrak{l}(\lambda) \cong \begin{cases} \pi(\lambda_{\mathfrak{L}^c}, \lambda_\mathfrak{L}) & \text{if } \mathfrak{l}|\mathfrak{f} \text{ and } \mathfrak{L}|\mathfrak{F}, \\ \pi(\phi_\mathfrak{l}, \left(\frac{M_\mathfrak{L}/F_\mathfrak{l}}{}\right)\phi_\mathfrak{l}) & \text{if } \mathfrak{l}|\mathfrak{i}. \end{cases} \tag{6.4}$$

We split $\mathfrak{N}'$ into a product $\mathfrak{N}_1\mathfrak{N}_2$ of co-prime ideals so that $\mathfrak{N}_1$ is made up of primes in Ξ_{pr}. Writing $\pi_\mathfrak{l}(\lambda) = \pi(\eta_\mathfrak{l}, \eta'_\mathfrak{l})$ for characters $\eta_\mathfrak{l}, \eta'_\mathfrak{l} : F_\mathfrak{l}^\times \to \mathbb{C}^\times$, we write $C_\mathfrak{l}$ for the conductor of $\eta_\mathfrak{l}^{-1}\eta'_\mathfrak{l}$. Define the minimal level of $\pi(\lambda)$ by

$$\mathfrak{N}(\lambda) = \mathfrak{N}_2 \prod_{\mathfrak{l} \in \Xi_{pr}} C_\mathfrak{l}.$$

We write $\Xi = \{\mathfrak{L}|\mathfrak{L} \supset \mathfrak{F}\mathfrak{P}^\Sigma, \mathfrak{L} \supset \mathfrak{N}(\lambda)\}$ for primes $\mathfrak{L}$ of M and define

$$\mathbf{a}_p(y, f(\lambda)) = \begin{cases} \sum_{xx^c=y, x_\Xi=1} \widehat{\lambda}(x)x_p^{(\kappa_1-\kappa_2)\Sigma} & \text{if } y \text{ is integral,} \\ 0 & \text{otherwise,} \end{cases} \tag{6.5}$$

where x runs over $(\widehat{R} \cap M^\times_{\mathbb{A}^{(\infty)}}/(R^{(\Xi)})^\times$ with $x_\mathfrak{L} = 1$ for $\mathfrak{L} \in \Xi$. The value $\widehat{\lambda}(x)$ is well defined modulo $(R^{(\Xi)})^\times$ as long as $x_\Xi = 1$ for the following reason: For primes $\mathfrak{l}|\mathfrak{N}(\lambda)$ non-split in M/F, by the condition $xx^c = y$, x is determined up to a unit u with $uu^c = 1$. Since $\lambda_\mathfrak{L}(u) = \phi_\mathfrak{l}(uu^c) = 1$, the value $\lambda_\mathfrak{L}(x_\mathfrak{L})$ is well defined. For $\mathfrak{L} \in \Xi$, by imposing $x_\mathfrak{L} = 1$, the condition $xx^c = y$ implies $x_{\mathfrak{L}^c} = y_\mathfrak{l}$; so, the value $\lambda_\mathfrak{L}(x_\mathfrak{l})$ is again well defined. As for a split prime $\mathfrak{l} \nmid \mathfrak{N}(\lambda)$ but $\mathfrak{l}|N_{M/F}(\mathfrak{C})$, we have $\lambda_\mathfrak{L}|_{O_\mathfrak{l}^\times} = \lambda_{\mathfrak{L}^c}|_{O_\mathfrak{l}^\times}$, so $\lambda_\mathfrak{L}(u_\mathfrak{L})\lambda_{\mathfrak{L}^c}(u_{\mathfrak{L}^c}) = 1$ because $uu^c = 1$ implies $u_\mathfrak{L} = u_{\mathfrak{L}^c}^{-1}$ identifying $R_\mathfrak{L}$ and $R_{\mathfrak{L}^c}$ with $O_\mathfrak{l}$. As for $\mathfrak{p}|p$

with $\mathfrak{p} \nmid \mathfrak{N}(\lambda)$, if $(uu^c) = 1$, we have

$$\widehat{\lambda}(u)u^{(\kappa_1-\kappa_2)\Sigma} = u^{-\kappa_1\Sigma-c\kappa_2\Sigma+(\kappa_1-\kappa_2)\Sigma} = (uu^c)^{-\kappa_2} = 1.$$

So again, $\widehat{\lambda}(x)x_p^{(\kappa_1-\kappa_2)\Sigma}$ is well-defined modulo such local units.

For a principal series representation $\pi(\eta', \eta)$ of $GL_2(F_\mathfrak{l})$, if $\eta|_{O_\mathfrak{l}^\times} = \eta'|_{O_\mathfrak{l}^\times}$, we have $\pi(\eta', \eta) \cong \eta \otimes \pi(\eta^{-1}\eta', 1)$ and $\pi(\eta^{-1}\eta', 1)$ is spherical; thus we have a unique spherical vector $v \neq 0$ in $\pi(\eta^{-1}\eta', 1)$ with $v|T(\mathfrak{l}) = (1+\eta^{-1}\eta'(\varpi_\mathfrak{l}))v$. The corresponding vector $v' = v \otimes \eta$ in $\pi(\eta', \eta)$ has minimal level fixed by $SL_2(O_\mathfrak{l})$ with $v'|T(y) = (\eta(y)+\eta'(y))v'$. If the conductor $C_\mathfrak{l}$ of $\eta^{-1}\eta'$ is non-trivial, again by the same argument, we find $v' \neq 0$ in $\pi_\mathfrak{l}(\lambda)$ such that $v'|T(y) = \eta(y)v'$ and $v'|u = \varepsilon(u)v'$ $(u \in U_0(C_\mathfrak{l})_\mathfrak{l})$, where $\varepsilon(u) = \eta(\det(u))(\eta^{-1}\eta'(a))$ for $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in U_0(C_\mathfrak{l})_\mathfrak{l}$. This shows that $f(\lambda)$ is a classical modular form in $M_\kappa(\mathfrak{N}(\lambda), \varepsilon_\lambda; \overline{\mathbb{Q}})$ if λ^- has split conductor. The form $f(\lambda)$ is a common eigenform of Hecke operators $\mathbb{T}(y)$. The p–adic Galois representation ρ_λ associated to $f(\lambda)$ is the induced representation $\mathrm{Ind}_M^F \widehat{\lambda}$, regarding $\widehat{\lambda}$ as a character of $\mathrm{Gal}(\overline{F}/M)$ by class field theory. By regularity: $\kappa_1 > \kappa_2$, $\widehat{\lambda}(c\sigma c^{-1}) \neq \widehat{\lambda}(\sigma)$ for $\sigma \in \mathrm{Gal}(\overline{F}/M)$, ρ_λ is absolutely irreducible by Mackey's theorem, and$f(\lambda)$ is a cusp form.

We take the coefficient ring W to be free of finite rank over $\mathbb{Z}_p$. Assuming that λ^- has split conductor ($\Leftrightarrow \pi(\lambda)$ is principal at every finite place), we shall study when $f(\lambda)$ satisfies the conditions (H1-7) of Theorem 6.1. We take a character φ of $\mathrm{Gal}(\overline{F}/M)$ of order prime to p such that $\widehat{\lambda}\varphi^{-1} \equiv 1 \mod \mathfrak{m}_W$ and define $\psi = \varphi^-$. Suppose that λ and φ coincides on $R_\mathfrak{L}^\times$ if $\mathfrak{L} \nmid p$. Then the conditions (2) and (3) on ψ in the introduction are an interpretation of principality of $\pi(\lambda)$ at every finite place. To interpret the four conditions (1-4) on ψ in the introduction in terms of φ, let $G(\mathfrak{C}) = M_\mathbb{A}^\times / \overline{M^\times U_M(\mathfrak{C})^{(p)} M_\infty^\times}$, where

$$U_M(\mathfrak{C})^{(p)} = \left\{ x \in \widehat{R}^\times | x_p = 1,\ x \equiv 1 \mod \mathfrak{C}\widehat{R} \right\}.$$

The first conditions (1) on ψ can be stated in terms of φ as follows:

(h1) *φ has order prime to p with exact conductor $\mathfrak{C}\mathfrak{P}^e$ for $\mathfrak{C}$ prime to p.*

Thus φ factors through the maximal prime-to-p quotient of $G(\mathfrak{C})$ which can be regarded canonically as a subgroup of $G(\mathfrak{C})$, because $G(\mathfrak{C})$ is almost p–profinite. The conditions (2-4) in the introduction imply the following three assertions:

(h2) *For all prime factors $\mathfrak{L}|\mathfrak{I}$, $\varphi_\mathfrak{L} = \phi_\mathfrak{l} \circ N_{M/F}$ for a character $\phi_\mathfrak{l} : F_\mathfrak{l}^\times \to W^\times$.*

(h3) *$\varphi_\mathfrak{P} \neq \varphi_{\mathfrak{P}^c}$ for all $\mathfrak{P} \in \Sigma_p$.*

(h4) *Over $\mathrm{Gal}(\overline{F}/M[\sqrt{p^*}])$, we have $\varphi_c \neq \varphi$, where $\varphi_c(\sigma) = \varphi(c\sigma c^{-1})$.*

We write $G_{tor}(\mathfrak{C})$ for the maximal torsion subgroup of $G(\mathfrak{C})$.

Theorem 6.3. *Assume* (6.1) *and the four conditions* (h1-4). *Let $\lambda_k : G(\mathfrak{C}) \to \overline{\mathbb{Q}}_p^\times$ be an arithmetic Galoischaracter of weight $k_1\Sigma + ck_2\Sigma$ ($k_j \in \mathbb{Z}[I]$) such that $k_1 > k_2$ and $\lambda_k|_{G_{tor}(\mathfrak{C})} = \varphi$. Then for the local ring R of $h_k(\mathfrak{N}(\lambda_k), \varepsilon_{\lambda_k}; W[\lambda_k])$ corresponding to $f(\lambda_k)$, the R–component $V(R)$ of*

$V = H^q(Y_0^B(\mathfrak{N}(\lambda_k)), L(k\varepsilon_{\lambda_k}; W[\lambda_k]))$ is R–free of rank 2^q, where $W[\lambda_k]$ is the complete discrete valuation ring inside $\overline{\mathbb{Q}}_p$ generated by the values of λ_k over W and $q = |I_B| \leq 1$.

Proof. We take a sufficiently large κ with $\kappa_1 > \kappa_2$ and $\kappa_1 + \kappa_2 = [\kappa]I$ for $0 \leq [\kappa] \in \mathbb{Z}$ so that $\zeta^{\kappa_1\Sigma + c\kappa_2\Sigma} = 1$ for all $\zeta \in R^\times$ and $\kappa \equiv 0 \mod (Q-1)\mathbb{Z}[I]$ for $Q = |\mathbb{F}|$. Then we can find a Hecke character λ with the following properties:

(1) *We have $\lambda((\alpha)) = \alpha^{\kappa_1\Sigma + c\kappa_2\Sigma}\varphi((\alpha))$ for all $\alpha \in M^\times$ prime to $\mathfrak{C}\mathfrak{P}^e$;*
(2) *$\lambda \equiv \varphi \mod \mathfrak{m}_W$.*

We are going to show for $f(\lambda)$ the assumptions (H1-7) except for (H4) of Theorem 6.1. Thus if (H4) is not applicable to $\mathrm{Ind}_M^F \widehat{\lambda}$, we get the result for $f(\lambda_k)$ by Corollary 6.2, because $f(\lambda)$ is a member of the p–adic family of modular forms determined by $f(\lambda_k)$. Otherwise, we modify the choice of λ.

We verify condition (H1-3) and (H5-7) one by one. We always have a character λ_1 of conductor 1 with $\lambda_1((\alpha)) = \alpha^{\kappa_1\Sigma + c\kappa_2\Sigma}$ for all $\alpha \in M^\times$ and $\lambda_1 \equiv 1 \mod \mathfrak{m}_W$ by our choice of κ; so, $\lambda/\lambda_1 \equiv \varphi \mod \mathfrak{m}_W$. We may assume that $\lambda/\lambda_1 = \varphi$.

- By the above choice of λ_1, we have $\det \rho_{\lambda_1} = \mathcal{N}^{[\kappa]}\left(\frac{M/F}{}\right)$ and $\det \rho_\lambda = \mathcal{N}^{[\kappa]}\widetilde{\varphi}\left(\frac{M/F}{}\right)$, where $\widetilde{\varphi}$ is the Galois character corresponding to the pull back of φ as a Hecke character of $M_{\mathbb{A}}^\times$ to $F_{\mathbb{A}}^\times$. Then χ in (H1) is given by $\widetilde{\varphi}\left(\frac{M/F}{}\right)$, which has order prime to p because $p > 2$. This shows (H1).
- By (h2), we have for $\mathfrak{l}|\mathfrak{N}(\lambda)p$,
$$\rho_\lambda|_{D_\mathfrak{l}} \cong \begin{cases} \begin{pmatrix} \widetilde{\lambda} & 0 \\ 0 & \widetilde{\lambda}_c \end{pmatrix} & \text{if } \mathfrak{l} = \mathfrak{L}\overline{\mathfrak{L}}\ (\mathfrak{L} \neq \overline{\mathfrak{L}}) \text{ in } M, \\ \begin{pmatrix} \widetilde{\lambda}_\mathfrak{l} & 0 \\ 0 & \widetilde{\lambda}_\mathfrak{l}\left(\frac{M/F}{}\right) \end{pmatrix} & \text{if } \mathfrak{l} \text{ is inert or ramified in } M/F. \end{cases}$$
We can choose $\widehat{\lambda}_c$ to corresponds to $\widehat{\lambda}_{\mathfrak{P}^c}$ for $\mathfrak{P} \in \Sigma_p$ with $\mathfrak{P}|\mathfrak{l}$ if $\mathfrak{l}|p$. Then by construction (or the definition of κ_2), we have $\delta_\mathfrak{l} = \widehat{\lambda}_{\mathfrak{P}^c}$. This shows (H2).
- Since λ_1 is of conductor 1, we find that $\widehat{\lambda}|_{I_\mathfrak{l}} = \varphi|_{I_\mathfrak{l}}$, which is of order prime to p. This shows (H3).
- Since $\widehat{\lambda} \equiv \varphi \mod \mathfrak{m}_W$, (h3) implies that $\overline{\delta}_\mathfrak{p} \neq \overline{\varepsilon}_\mathfrak{p}$; so, (H5) follows from (h3).
- The condition (H6) follows from the definition of $\mathfrak{N}(\lambda)$ and (h1), because $C(\overline{\varepsilon}_\mathfrak{l}\overline{\delta}_\mathfrak{l}^{-1})$ is equal to $C(\varepsilon_\mathfrak{l}\delta_\mathfrak{l}^{-1})$ by (H3) already verified. By our definition of $\mathfrak{N}(\lambda)$, its $\mathfrak{l}$ part coincides with $C(\varepsilon_\mathfrak{l}\delta_\mathfrak{l}^{-1})$.
- The condition (H7) follows from (h4) by Mackey's theorem.

Thus as long as $\widehat{\lambda} \not\equiv \widehat{\lambda}_c\mathcal{N} \mod \mathfrak{m}_W$ on $I_\mathfrak{p}$ for every $\mathfrak{p}|p$, we have verified the theorem.

Now assume that

$$P = \left\{ \mathfrak{p} | p \middle| \widehat{\lambda} \equiv \widehat{\lambda}_c \mathcal{N} \mod \mathfrak{m}_W \text{ on } I_{\mathfrak{p}} \right\}$$

is non-empty. Let $\overline{R^\times}$ (resp. $\overline{O^\times}$) be the p–adic closure of $R^\times$ (resp. $O^\times$) in $R_p^\times$ for $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Since M cannot have p–th root of unity (by ordinarity of Σ and unramifiedness of p in $F/\mathbb{Q}$), $[R^\times : O^\times]$ is prime to p; so, $\overline{R^\times}/\overline{O^\times}$ has order prime to p. We consider the character $x \mapsto x^\Sigma$ of $R_p^\times \to W^\times$, which has values in a complete valuation subring A of W unramified and finite over $\mathbb{Z}_p$. Let $A_p^\times$ be the maximal p–profinite subgroup of $A^\times$, which is canonically a direct factor of $A^\times$, because A is unramified over $\mathbb{Z}_p$. Let $x \mapsto \langle x \rangle$ be the projection of $x \in A^\times$ to $A_p^\times$. Thus $\langle x \rangle \equiv 1 \mod \mathfrak{m}_W$ for all $x \in A^\times$ and $\langle \zeta \rangle = 1$ for all roots of unity ζ in A. Thus $x \mapsto \langle x^\Sigma \rangle$ is a character of $R_p^\times/\overline{R^\times}$, which is a subgroup of finite index of $G(1)$. We can extend this character to a character $\widehat{\chi}$ of $G(1)$ so that $\widehat{\chi} \equiv 1 \mod \mathfrak{m}_W$ on $G(1)$. This is possible for the following reason: We first extend the character to a character $\chi' : G(1) \to W^\times$, which is always possible, replacing W by its finite extension if necessary. Then we take a Teichmüller lift ε of the reduction (χ' mod $\mathfrak{m}_W$). Then $\widehat{\chi} = \varepsilon^{-1}\chi'$ gives the desired extension. By our construction, $\widehat{\chi}$ is the p–adic avatar of an arithmetic Hecke character χ whose infinity type is Σ.

We now take the Teichmüller lift $\widehat{\lambda}_0$ of ($\widehat{\lambda} \mod \mathfrak{m}_W$), which is a p–adic avatar of a finite order character $\lambda_0 : G(\mathfrak{C}) \to W^\times$. Then $\lambda' = \lambda_0\chi$ is of infinite type Σ and satisfies $\lambda' \equiv \lambda \equiv \varphi \mod \mathfrak{m}_W$. For $x \in R_p$, we write $\omega(x) = \lim_{n\to\infty} x^{[R:pR]^n} \in R_p$ for $x \in R_p$. Since p is unramified in $M/\mathbb{Q}$, the Teichmüller lift of ($x^k \mod \mathfrak{m}_W$) for $k \in \mathbb{Z}[\Sigma \cup \Sigma c]$ is given by $\omega(x)^k$ (in other words, the operations k and ω commute). Thus, at the place $\mathfrak{p} \in P$, by the above process of construction, $\lambda'^-(x_{\mathfrak{p}}) = \mathcal{N}^{-1}(x_{\mathfrak{p}})$ for $x_{\mathfrak{p}} \in R_{\mathfrak{P}} \cap F_{\mathfrak{P}}^\times$ ($\mathfrak{P} \in \Sigma_p$ with $\mathfrak{P}|\mathfrak{p}$), and the level $\mathfrak{N}(\lambda')$ of $f(\lambda')$ is prime to all $\mathfrak{p} \in P$. Thus $f(\lambda')$ has weight $(I, 0)$ and its Galois representation satisfies (H4). Then the theorem follows from Corollary 6.2, since $f(\lambda_k)$ comes from the same local ring of the universal nearly ordinary Hecke algebra **h** as the local ring of the p–adic family of Hecke eigenforms determined by $f(\lambda)$ or $f(\lambda')$. □

For our later use, we shall compute the q–expansion of classical modular forms associated to $f(\lambda)$. Pick $y \in F_{\mathbb{A}}^\times$ with $y_p = y_\infty = 1$. Then by the definition of $\widehat{\lambda}$ and (6.5), we get the following formula of the complex Fourier coefficients:

$$a(\xi y d, f(\lambda)) = \sum_{xx^c = \xi y d, x_\Xi = 1} \lambda(xR),$$

where $xR = F \cap x\widehat{R}$ and x runs over $(\widehat{R} \cap M_{\mathbb{A}^{(\infty)}}^\times)/R^{(\Xi)}$ for Ξ as in (6.5). This shows that for $f_{\mathrm{diag}[y,1]}$ in (S2),

$$f_{\mathrm{diag}[y,1]}(\tau) = N(\mathfrak{y})^{-1} \sum_{\mathfrak{A}; \mathfrak{A}\mathfrak{A}^c \sim \mathfrak{y}\mathfrak{d}} \lambda(\mathfrak{A})\alpha^{-\kappa_2}\theta(\lambda; \mathfrak{A}),$$

where $\mathfrak{A}$ runs over a complete representative set for ideal classes of M with $\mathfrak{A}\mathfrak{A}^c = \alpha\mathfrak{y}\mathfrak{d}$ ($\mathfrak{y} = y\widehat{O} \cap F$) for a totally positive $\alpha \in F$ and

$$\theta(\lambda;\mathfrak{A}) = \sum_{\xi \in \mathfrak{A}^{-1}/\mu(M)} \lambda(\xi^{(\infty\Xi)})(\xi\xi^c)^{-\kappa_2} q^{\alpha\xi\xi^c}. \tag{6.6}$$

Here we regard λ as an idele character $\lambda : M_{\mathbb{A}}^\times/M^\times$ by putting

$$\lambda(x) = \lambda(xR)x_\infty^{-\kappa_1\Sigma - c\kappa_2\Sigma},$$

and ξ runs over elements in $\mathfrak{A}^{-1}$ such that $\xi\mathfrak{A}$ is outside Ξ for Ξ as in (6.5). As a locally constant function on $\widehat{\mathfrak{A}}^{-1}$, the p–component of $\phi_1' : \xi \mapsto \lambda(\xi^{(\Xi)})$ is given by λ_p^{-1} restricted to $\mathfrak{A}_p^{-1}$ by the following reason: ϕ_1' is the characteristic function of $\mathfrak{A}_{\mathfrak{l}}^{-1}$ for $\mathfrak{l}$ outside the conductor $C(\lambda)$, and taking $\xi \in \mathfrak{A}^{-1}$ with $\xi \equiv 1 \mod C^{(p)}(\lambda)$, we see that $\phi_1'(\xi) = \lambda(\xi^{(\Xi)}) = \lambda(\xi^{(p)}) = \lambda(\xi_p)^{-1}$.

The modular form $\theta(\lambda;\mathfrak{A})$ is of weight $\kappa\varepsilon$ on

$$\Gamma_0(\mathfrak{N}(\lambda);\mathfrak{y}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(F) \middle| a, d \in O,\ b \in \mathfrak{y},\ c \in \mathfrak{N}(\lambda)\mathfrak{y}^{-1} \right\}.$$

6.3. Self-duality. Let $L^*(\kappa\varepsilon;W)$ be the dual lattice of $L(\kappa;W)$ under the pairing $[\ ,\ ]$ introduced in Subsection 5.3. Then by definition, $L^*(\kappa\varepsilon;W) \subset L(\kappa\varepsilon;W)$ and the quotient $L(\kappa\varepsilon;W)/L^*(\kappa\varepsilon;W)$ is spanned by $X^{n-j}Y^j$ for $0 < j < n$.

Since

$$U_0(\mathfrak{N}p)_p \operatorname{diag}[p,1] U_0(\mathfrak{N}p)_p = \bigsqcup_{u \mod pO_p} \left(\begin{smallmatrix} p & u \\ 0 & 1 \end{smallmatrix}\right) U_0(\mathfrak{N}p)_p,$$

the action of $\left(\begin{smallmatrix} p & u \\ 0 & 1 \end{smallmatrix}\right)$ on $L(\kappa\varepsilon;W)/L^*(\kappa\varepsilon;W)$ (even after dividing by p^{κ_2}) is nilpotent. Thus the projector $e = \lim_{n\to\infty} \mathbb{T}(p)$ kills the cohomology group:

$$H^r_*(Y, L(\kappa\varepsilon;W)/L^*(\kappa\varepsilon;W)) \quad (Y = Y_0^B(\mathfrak{N}))$$

for any $r \geq 0$, and hence by cohomology sequence, we get a canonical isomorphism for $Y = Y_0^B(\mathfrak{N})$:

$$H^r_{*,n.ord}(Y, L^*(\kappa\varepsilon;W)) \cong H^r_{*,n.ord}(Y, L(\kappa\varepsilon;W)), \tag{6.7}$$

where H^r_* is either compactly supported or usual cohomology group. We define the action of Hecke operators $\mathbb{T}(y)$ and $\langle\mathfrak{l}\rangle$ on $H^r_*(Y, L^*(\kappa^*\varepsilon^*;W))$ via the adjoint action under $[,\ ]$ of the semi-group $\Delta_0(\mathfrak{N})$. Then the operator is integral if either $p|\mathfrak{N}$ or $[\kappa] \leq 1 \Leftrightarrow [\kappa] \geq 0$. Thus in the same way, we get

$$H^r_{*,n.ord}(Y, L(\kappa^*\varepsilon^*;W)) \cong H^r_{*,n.ord}(Y, L^*(\kappa^*\varepsilon^*;W)). \tag{6.8}$$

As we have seen in [H88a] Theorem 10.1, $H^r_*(Y, L(\kappa\varepsilon;W) \otimes (\mathbb{Q}_p/\mathbb{Z}_p))$ is p–divisible if $|I_B| \leq 1$. Then by looking into the cohomology sequence attached to the short exact sequence:

$$0 \to L(\kappa\varepsilon;W) \to L(\kappa\varepsilon;W \otimes \mathbb{Q}_p) \to L(\kappa\varepsilon;W) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to 0,$$

$H^r_*(Y, L(\kappa\varepsilon; W))$ is free of finite rank over W, and we get a perfect pairing:

$$(\ ,\ )_W : H^q_{n.ord}(Y, L(\kappa\varepsilon; W)) \times H^q_{c,n.ord}(Y, L(\kappa^*\varepsilon^*; W)) \to W$$

of W–free modules. For the moment, assume that $F \neq \mathbb{Q}$. Then $Y^B(U)$ is compact; so, $H^q_{cusp,n.ord} = H^q_{n.ord} = H^q_{c,n.ord}$, and we have the perfect duality pairing

$$(6.9) \quad (\ ,\ )_W : H^q_{cusp,n.ord}(Y, L(\kappa\varepsilon; W)) \times H^q_{cusp,n.ord}(Y, L(\kappa^*\varepsilon^*; W)) \longrightarrow W$$

As already verified in [H88b] Theorem 3.1 for $F = \mathbb{Q}$, the assertion (6.9) holds even for $F = \mathbb{Q}$; so, we do not need to assume $F \neq \mathbb{Q}$ anymore. We thus have

Corollary 6.4. *Under the assumptions and notations of* Corollary 6.2*, the map* $(v, w) \mapsto f(v \otimes w)$ *induces a surjective linear map:* $V(R_P) \otimes_{R_P} V'(R_P) \twoheadrightarrow S(R_P)$ *for all* $P \in \mathcal{A}(\mathbb{I})$*, where* $S = S_{\kappa(P)}(\mathfrak{N}, \varepsilon(P); W[\varepsilon_P])$*,* $V = H^q(Y, L(\kappa(P)\varepsilon(P); W[\varepsilon_P]))$*,* $V' = H^q(Y, L(\kappa(P)^*\varepsilon(P)^*; W[\varepsilon_P]))$*. If* $q = |I_B| = 0$*,* f *is an isomorphism:* $V(R_P) \otimes_{R_P} V'(R_P) \cong S(R_P)$*.*

7. Proof of the theorem

We shall prove the theorem in the introduction under the assumptions (h1-4) on φ, which are equivalent to the assumptions (1-4) in the introduction once we have chosen φ with $\psi = \varphi^-$. We first recall integrality results due to Shimura [ACM] Section 32 and Katz [K] II on the values of modular forms and then prepare preliminary results on integral decomposition of quaternionic quadratic spaces. After that, we prove the theorem in the case where the degree $[F : \mathbb{Q}]$ is even. The odd degree case will be reduced to the even degree case.

7.1. Integrality of values of modular forms. By the approximation theorem,

$$GL_2(F)\backslash GL_2(F^{(\infty)}_{\mathbb{A}})/U_0(\mathfrak{N}) \cong F^\times\backslash F^\times_{\mathbb{A}^{(\infty)}}/\det(U_0(\mathfrak{N})) \cong Cl_F \quad \text{via } y \mapsto \det(y)$$

for the class group Cl_F of F. From this, $f \in S_\kappa(\mathfrak{N}, \varepsilon; W)$ is determined by the q–expansions $\{f(y)\}_y$. Writing $\mathfrak{y} = y\widehat{O} \cap F$ for the ideal corresponding to the idele y and setting $\widetilde{y} = \left(\begin{smallmatrix} y & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $f(y)$ is the q–expansion at the Tate AVRM $\mathrm{Tate}_{\mathfrak{y}^*,O}(q)$ (in [K] 1.1) of the classical modular form $f_{\widetilde{y}}$ (of (S2) in Subsection 5.1) of weight $k = \kappa_1 - \kappa_2 + I$ on the following congruence subgroup:

$$(7.1) \qquad \Gamma_0(\mathfrak{N}; \mathfrak{y}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(F) \middle| a, d \in O,\ b \in \mathfrak{y},\ c \in \mathfrak{y}^{-1}\mathfrak{N} \right\}.$$

Here $\mathfrak{y}^* = \mathfrak{y}^{-1}\mathfrak{d}^{-1}$ for the absolute different $\mathfrak{d}$ of F.

A classical modular form with q–expansion coefficients in W on a slightly smaller Γ_1–type congruence subgroup:

$$(7.2) \qquad \Gamma(\mathfrak{N}; \mathfrak{y}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{N}; \mathfrak{y}) \middle| a \equiv d \equiv 1 \mod \mathfrak{N} \right\}$$

has a moduli theoretic interpretation, which we recall in the following paragraph. We write $S_k(\Gamma(\mathfrak{N}; \mathfrak{y}); A)$ for the space of the classical cusp forms on $\Gamma(\mathfrak{N}; \mathfrak{y})$ of weight k with q–expansion coefficients in A.

Let A be a valuation ring with residual characteristic p. An abelian scheme $X_{/A'}$ over an A–algebra A' is called an abelian variety with real multiplication by O (AVRM) if it has an embedding: $O \hookrightarrow \mathrm{End}(X_{/A'})$ of algebras such that $H^0(X,\Omega_{X/O}) = (O \otimes_{\mathbb{Z}} A')\omega$ for a nowhere vanishing differential ω. Here we have used the unramifiedness of F at p (otherwise, we need to formulate this condition as $H^0(X,\Omega_{X/O}) = (\mathfrak{d}^{-1} \otimes_{\mathbb{Z}} A')\omega)$. Each Hilbert modular form $f \in S_k(\Gamma(\mathfrak{N};\mathfrak{y});A)$ can be regarded as a function of quintuples: (X,λ,i,ω,A') made up of an A–algebra A', an AVRM X over A', a polarization λ whose polarization ideal is given by $\mathfrak{y}^*$, an embedding $i : \mu_{\mathfrak{N}} \hookrightarrow X$ of group schemes over A' and a differential ω as above (see, for more details of AVRM's, [K] 1.0 and [PAF] Section 4.1). Here $\mu_{\mathfrak{N}}$ is the group scheme made up of $\mathfrak{N}$–torsion points of $\mathbb{G}_m \otimes \mathfrak{d}^{-1}$, that is, $\mu_{\mathfrak{N}}(A) = \{\zeta \in \mathbb{G}_m \otimes \mathfrak{d}^{-1}(A) | \mathfrak{N}\zeta = 0\}$, regarding $\mathbb{G}_m \otimes \mathfrak{d}^{-1}(A)$ as an additive group. Every ingredient of the quintuple has to be defined over A'. As a function of $(X,\lambda,i,\omega)_{/A'}$, f satisfies the following conditions (see [HMI] 4.2.7):

(M1) $f(X',\lambda',i',\omega') = \rho(f(X,\lambda,i,\omega))$ if $\rho : A' \to C$ is an A–algebra homomorphism and $(X',\lambda',i',\omega')_{/C} \cong (X,\lambda,i,\omega)\times_{A',\rho}C$. Here "$\cong$" implies: $\phi : X \times_A C \cong X'_{/C}$ as AVRM's, ${}^t\phi \circ \lambda' \circ \phi = \lambda \times_{A'} C$, $\phi \circ i \equiv i'$ and $\phi^*\omega' = \omega$.

(M2) f vanishes at all cusps, that is, the q–expansion of f at every Tate quintuple vanishes at $q = 0$.

(M3) $f(X,\lambda,i,\alpha\omega) = \alpha^{-k}f(X,\lambda,i,\omega)$ for $\alpha \in (A' \otimes_{\mathbb{Z}} O)^\times$.

The "Neben" character $\varepsilon : U_0(\mathfrak{N}) \to \overline{\mathbb{Q}}^\times$ restricted to $U_0^1(\mathfrak{N}) = U_0(\mathfrak{N}) \cap SL_2(\widehat{O})$ factors through $U_0^1(\mathfrak{N})/U^1(\mathfrak{N})$ for $U^1(\mathfrak{N}) = U(\mathfrak{N}) \cap SL_2(\widehat{O})$ (the conductor of ε^- is $\mathfrak{N}$), because $\varepsilon(u) = \varepsilon_1(\det(u))\varepsilon^-(d)$ for $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Thus to evaluate $f \in S_\kappa(\mathfrak{N},\varepsilon;A)$ at an AVRM X of CM type, we only need to specify $\mu_{\mathfrak{N}} \hookrightarrow X$.

Let M/F be the CM quadratic extension in the introduction. Recall the decomposition: $\mathfrak{C} = \mathfrak{F}\mathfrak{F}_c\mathfrak{I}$ of the conductor of the Hecke character λ such that $\mathfrak{F} + \mathfrak{F}_c = R$ with $\mathfrak{F} \subset \mathfrak{F}_c^c$ and $\mathfrak{I}$ is made up of primes non-split in M/F. By (h2) (for $\varphi = \lambda$), the prime factors of $\mathfrak{N}(\lambda)$ are either split or ramified over F. If $\mathfrak{l}|\mathfrak{N}(\lambda)$ and $\mathfrak{l} = \mathfrak{L}\overline{\mathfrak{L}}$ (with $\mathfrak{L} \neq \overline{\mathfrak{L}}$) in M, we may choose $\mathfrak{L}$ so that $\mathfrak{L} \supset \mathfrak{F}$. The exponent of $\mathfrak{l}$ in $\mathfrak{N}(\lambda)$ is less than or equal to that of $\mathfrak{L}$ in $\mathfrak{F}$. Thus to evaluate $f(\lambda)$ at a CM point, we need to specify the level structure for the level $d(M/F)\mathfrak{f}$ ($\mathfrak{f} = \mathfrak{F} \cap F$). Actually we later need the level structure at other primes non-split in M/F; so, we first specify level structure for split primes and then extend the definition to non-split primes. We shall do this first for an abelian variety of CM type Σ with multiplication by R. Hereafter $\mathfrak{F}$ is an integral ideal of R with $\mathfrak{F} + \mathfrak{F}^c = R$ and prime to p (because we need to be more careful for primes dividing p).

Let $\overline{W}$ be as in the introduction. Define $\mathcal{W} = i_p^{-1}(\overline{W}) \subset \overline{\mathbb{Q}}$, which is a valuation ring unramified over $\mathbb{Z}_{(p)}$ with algebraically closed residue field $\overline{\mathbb{F}}$.

We consider $X(R)_{/\mathbb{C}}$ to be the algebraization of the complex torus $\mathbb{C}^{\Sigma}/R^{\Sigma}$, where $R^{\Sigma} = \{(a^{\sigma})_{\sigma\in\Sigma}|a \in R\}$ and $\mathbb{C}^{\Sigma} = R^{\Sigma} \otimes_{\mathbb{Z}} \mathbb{R}$. Since $X(R)$ has complex multiplication, it can be defined over $\overline{\mathbb{Q}}$ and hence over a number field (see [ACM] 12.4). By the main theorem of complex multiplication (see [ACM] 18.6), $X(R)$ and its ℓ–divisible group for any prime ℓ outside p are actually defined over an infinite extension K of $\mathbb{Q}$ unramified at p. By the criterion of good reduction by unramifiedness of ℓ–power torsion points (see [ST]), we find a model $X(R)_{/\mathcal{W}}$ of $X(R)_{/K}$.

By choosing $\delta \in M$ with $\mathrm{Im}(\sigma(\delta)) > 0$ for $\sigma \in \Sigma$, we have a polarization pairing $(x, y) \mapsto \mathrm{Tr}_{M/\mathbb{Q}}(\delta x c(y))$. This pairing identifies $R \wedge_O R$ with $\mathfrak{y}$ for a suitable choice of a fractional ideal $\mathfrak{y} \subset F$ (prime to p) and induces a $\mathfrak{y}^*$–polarization $\lambda = \lambda(R)$. Thus we have the CM-triple $(X(R), \lambda(R), i(R), \omega(R))_{/\mathcal{W}}$, choosing $\omega(R)$ so that $H^0(X(R), \Omega_{X(R)/\mathcal{W}}) = (O \otimes_{\mathbb{Z}} \mathcal{W})\omega(R)$.

Since $\overline{W}$ has algebraically closed residue field, for any integer m prime to p, we have $X(R)[m] = \{x \in X(R)(\overline{W})|mx = 0\} \cong (\mathbb{Z}/m\mathbb{Z})^{[M:\mathbb{Q}]}$ and $\mu_m \cong \mathbb{Z}/m\mathbb{Z}$ as group schemes over $\overline{W}$. Thus we define the level $\mathfrak{f}$–structure to be

$$\mu_{\mathfrak{f}} \cong O/\mathfrak{f} \cong X(R)[\mathfrak{F}] = \{x \in X(R)(\overline{W})|\mathfrak{F}x = 0\}.$$

Since the Frobenius map of $\overline{\mathbb{F}}_p$ acts by multiplication by p (times a unit) on $\Omega_{X(R)/\overline{W}}$, the p–divisible group $X(R)[\mathfrak{P}^{\infty}]_{/\mathcal{W}}$ for $\mathfrak{P} \in \Sigma_p$ is connected. Since the residue field of $\mathcal{W}$ is algebraically closed, we see that $X(R)[\mathfrak{P}^e] \cong \mu_{\mathfrak{P}^e}$ over $\mathcal{W}$ (for $e = (e(\mathfrak{P}))_{\mathfrak{P}\in\Sigma_p}$), which gives rise to the level $\mathfrak{p}^e$–structure we need.

Since $R \wedge R \cong \mathfrak{y}$, we can choose a base w_1 and w_2 of R so that $R = Ow_1 + \mathfrak{y}w_2$. For any integral ideal $\mathfrak{q}$ prime to p, we choose a generator $\varpi_{\mathfrak{q}}$ of $\mathfrak{q}O_{\mathfrak{q}}$. Fixing an isomorphism $O/\mathfrak{q} \cong \mathfrak{y}/\mathfrak{q}$, we embed $O/\mathfrak{q} \cong \mathfrak{y}/\mathfrak{q}/\mathfrak{y} \hookrightarrow \mathfrak{q}^{-1}R_{\mathfrak{q}}/R_{\mathfrak{q}} \cong X(R)[\mathfrak{q}]$ by sending x to $\varpi_{\mathfrak{q}}^{-1}xw_2 \in M_{\mathfrak{q}}/R_{\mathfrak{q}}$, which gives the level $\mathfrak{q}$–structure on $X(R)$. We choose the base $w = (w_1, w_2)$ so that the level $\mathfrak{p}^e\mathfrak{f}$–structure we have chosen coincides with the one for $\mathfrak{q}$ if $\mathfrak{p}^e\mathfrak{f} + \mathfrak{q}$ is non-trivial. We may always choose w so that $w_0 = w_1/w_2 \in \mathfrak{H}^I$. Therefore choosing the base (w_1, w_2) is almost equivalent to the choice of a point $w_0 \in \mathfrak{H}^I$ modulo $\Gamma(\mathfrak{N}, \mathfrak{y})$ for $\mathfrak{N} = \mathfrak{q} \cap \mathfrak{f}\mathfrak{p}^e$. We write the level structure as $i(R) : \mu_{\mathfrak{N}} \hookrightarrow X(R)[\mathfrak{N}]$.

The above definition of the quadruple $x(R) = (X(R), \Lambda(R), i(R), \omega(R))_{/\mathcal{W}}$ can be generalized to ideals of an O–order of R. Let $\mathfrak{m}$ be an integral ideal of F prime to $p\mathfrak{f}$. Let $R' = O + \mathfrak{m}R$ be the O–order of M of conductor $\mathfrak{m}$. We take a proper fractional ideal $\mathfrak{A}$ of R' prime to $p\mathfrak{f}\mathfrak{q}d(M/F)$. A fractional R'–ideal $\mathfrak{A}$ is called *R'–proper* if $\{x \in M|x\mathfrak{A} \subset \mathfrak{A}\} = R'$. The polarization pairing on R (so on M) induces the polarization $\Lambda(\mathfrak{A})$ on $\mathfrak{A}$. We identify $\mathfrak{A} \wedge \mathfrak{A}$ with a fractional ideal $\mathfrak{y}(\mathfrak{A})$ of F under this pairing. It is easy to verify $\mathfrak{y}(\mathfrak{A}) = \mathfrak{y}(R)\mathfrak{m}N_{M/F}(\mathfrak{A})$. Then we can choose a base w of $\mathfrak{A}$ so that $\mathfrak{A} = Ow_1 + \mathfrak{y}(\mathfrak{A})w_2$ and $w_0(\mathfrak{A}) = w_1/w_2 \in \mathfrak{H}^I$. This choice w gives rise to the level structure $i(\mathfrak{A}) : \mu_{\mathfrak{N}} \hookrightarrow X(\mathfrak{A})[\mathfrak{N}]$. We can always find an étale constant subgroup $C \cong O/\mathfrak{c}$ ($\mathfrak{c}$ prime to $\mathfrak{f}\mathfrak{q}d(M/F)p$) in $X(R)$ such that the étale quotient $X(\mathfrak{A}) = X(R)/C$ over $\mathcal{W}$ (e.g. [GME] 1.8.3) gives a model over $\mathcal{W}$ of $\mathbb{C}^\Sigma/\mathfrak{A}^\Sigma$. Since $\mathfrak{c}$ is prime to $p\mathfrak{f}$, the level structure $i(R)$ and the differential $\omega(R)$ induce a unique level structure and a unique differential $\omega(\mathfrak{A})$ on $X(\mathfrak{A})$. We make a choice w so that the two level structures (one coming from $i(R)$ and another from the base w) coincide at primes where the two are well defined. Thus we have a unique point $w_0(\mathfrak{A}) \in \mathfrak{H}^I/\Gamma_1(\mathfrak{N},\mathfrak{y})$. Having w is equivalent to having the quadruple $x(\mathfrak{A}) = (X(\mathfrak{A}), \Lambda(\mathfrak{A}), i(\mathfrak{A}), \omega(\mathfrak{A}))$ over $\mathbb{C}$.

Supposing that $f \in S_k(\Gamma(\mathfrak{N};\mathfrak{y});\mathcal{W})$ (and regarding f as a complex modular form), we may interpret the value $f(x(\mathfrak{A}))$ in terms of evaluation at a CM point $w_0(\mathfrak{A}) \in \mathfrak{H}^I$. For each $z = (z_1, z_2)$ with $z_0 := \frac{z_1}{z_2} \in \mathfrak{H}^I$, we consider the lattice $L_z = L_z^{\mathfrak{y}} = 2\pi i(Oz_1 + \mathfrak{y}z_2) \subset F_{\mathbb{C}} = F \otimes_{\mathbb{Q}} \mathbb{C}$. We define a pairing $\langle\ ,\ \rangle : F_{\mathbb{C}} \times F_{\mathbb{C}} \to \mathbb{R}$ by $\langle 2\pi i(az_1+bz_2), 2\pi i(cz_1+dz_2)\rangle = ad-bc$, which induces a $\mathfrak{y}^*$–polarization $\lambda_z = \lambda_z^{\mathfrak{y}}$ on the complex torus $X_z = X_z^{\mathfrak{y}} = F_{\mathbb{C}}/L_z$. Thus we can algebraize X_z to an abelian variety $X_{z/\mathbb{C}}$. We have a canonical level $\mathfrak{N}$–structure $i_z : (\mathfrak{d}^{-1} \otimes O/\mathfrak{N}) \cong 2\pi i(\mathfrak{y}z_2 \otimes O/\mathfrak{N}) \subset X_z(\mathbb{C})$ as long as $\mathfrak{y}$ is prime to $\mathfrak{N}$. Then the analytic value of f at z is given by

$$z_2^{-k} f((z_0,1)) = f(z) = f(x_z^{\mathfrak{y}}) \text{ for } x_z^{\mathfrak{y}} = (X_z, \lambda_z, i_z, du), \tag{7.3}$$

where u is the variable $(u_\sigma)_{\sigma\in I}$ with $u_\sigma \in \mathbb{C}$ identifying $F_{\mathbb{C}}$ with $\mathbb{C}^I$ as $\mathbb{C}$–algebras.

Defining the canonical period $\Omega \in F_{\mathbb{C}}^\times = (\mathbb{C}^\times)^\Sigma$ by

$$\omega(R) = \Omega du \tag{7.4}$$

and choosing $\mathfrak{y}$ so that $R = (2\pi i)^{-1} L_{z_0}^{\mathfrak{y}}$, we find $x(\mathfrak{A}) \cong x_z^{\mathfrak{y}(\mathfrak{A})}$ and

$$f(x(\mathfrak{A})) = \frac{(2\pi i)^k f(z)}{\Omega^k} \in \mathcal{W} \text{ up to units in } \mathcal{W}, \tag{7.5}$$

because $\omega(\mathfrak{A})/\omega(R) \in (O \otimes_{\mathbb{Z}} \mathcal{W})^\times$ (see [ACM] Section 32 and [K] II). Here writing $\Omega = (\Omega_\sigma) \in \mathbb{C}^\Sigma$, $\Omega^k = \prod_{\sigma\in\Sigma} \Omega_\sigma^{k_\sigma}$.

Since $\mathcal{W}$–integral modular forms $f(z,w)$ of weight (k,k) for the product of congruence subgroups: $\Gamma(\mathfrak{N};\mathfrak{y}) \times \Gamma(\mathfrak{N}';\mathfrak{y}')$ classify the pairs of test objects: $(x_z^{\mathfrak{y}}, x_w^{\mathfrak{y}'})$, the same formula is valid (by the same proof given in [K]): up to units in $\mathcal{W}$,

$$f(x(\mathfrak{A}), x(\mathfrak{B})) = \frac{(2\pi i)^{2k} f(z,w)}{\Omega^{2k}}. \tag{7.6}$$

7.2. Error terms of integral decomposition. Let B be a quaternion algebra over F. Let M/F be a CM field with integer ring R. We are going to compute error terms of O–integral decomposition of an O–lattice of B as an integral quadratic space into a direct sum of two O–lattices of M with its norm form.

We fix a maximal order O_B of B. For an embedding $i : R \hookrightarrow B$ of O–algebras, since i is an embedding of O–algebras, we have $\mathrm{Tr}(i(a)) = \mathrm{Tr}_{M/F}(a)$ for the reduced trace Tr of B and $i(a)i(a)^\iota = N_{M/F}(a) = aa^c$. This shows $i(a^c) = i(a)^\iota$ for the main involution ι of B.

Let L be an O–lattice in B. We consider the two orders:

$$O^l_L = \{x \in B | xL \subset L\} \text{ and } O^r_L = \{x \in B | Lx \subset L\}. \tag{7.7}$$

We suppose to have two embedding $l : R \hookrightarrow B$ and $r : R \hookrightarrow B$. Thus L becomes an $R_l \otimes_O R_r$–module by $(a \otimes b)\ell = l(a)\ell r(b)$, where $R_l = l^{-1}(l(R) \cap O^l_L)$ and $R_r = r^{-1}(r(R) \cap O^r_L)$. Since $K^m \otimes K^n \cong M_{m\times n}(K)$, we find that $M_m \otimes_K M_n(K) \cong M_{mn}(K)$ as K–algebras. By extending scalars to M, we find $B \otimes_F M \cong M_2(M)$, and the above argument applied to the extended algebra $M_2(M)$ shows that the embedding $l \otimes r : R_l \otimes_O R_r \hookrightarrow \mathrm{End}_O(L)$ is injective. Therefore B is a free $M \otimes_F M$–module of rank 1. When we regard B as an M–vector space, we agree to use right multiplication by $\alpha \in M$ given by $\alpha b = b \cdot r(\alpha)$. Therefore $M \otimes_F M$ is identified with $M \oplus M$ by $a \otimes b \mapsto (ab, a^c b)$ for the generator c of $\mathrm{Gal}(M/F)$. Then we define $L^1 = (1, 0)L$ and $L^2 = (0, 1)L$ for the idempotents $(1, 0), (0, 1) \in M \oplus M$. Since $L^M = L^1 \oplus L^2 \supset L$, we can define $L_j = L^j \cap L$. Then $L_M = L_1 \oplus L_2 \subset L$. Since $(1, 0)B$ is the eigenspace of $M \oplus M$ killed by the right factor M, we have

$$L_2 = \left\{x \in L \middle| S(L_1, x) = 0\right\},$$

because multiplication by units in $(M \otimes_F M)^\times$ preserves the inner product $S(x, y) = \mathrm{Tr}(xy^\iota)$ up to scalar similitude. By S, we have the orthogonal projection π_1 of B to ML_1 and π_2 to ML_2. Then we may have defined $L^M = \pi_1(L) \oplus \pi_2(L)$. Indeed, π_1 (resp. π_2) is given by the multiplication by $(1, 0)$ (resp. $(0, 1) \in M \otimes_F M$). We want to determine primes dividing the index $[L^M : L_M]$. Here is the result:

Lemma 7.1. *Let $d(R_l/O)$ (resp. $d(R_r/O)$) be the relative discriminant of R_l/O (resp. of R_r/O). Then we have $d(R_l/O)d(R_r/O)L^M \subset L_M$.*

Proof. The process constructing L^M and L_M can be done at each localization $B_\mathfrak{p}$ for primes $\mathfrak{p}$ of O. Then $L_{i,\mathfrak{p}} = L_\mathfrak{p} \cap M_\mathfrak{p} L_i$ and $\pi_j(L_\mathfrak{p}) = \pi_j(L)_\mathfrak{p}$. If a prime $\mathfrak{p}$ of O is unramified in R_r and R_l, we have $R_{l,\mathfrak{p}} \otimes_{O_\mathfrak{p}} R_{r,\mathfrak{p}} \cong R_\mathfrak{p} \oplus R_\mathfrak{p}$, and hence $L^M_\mathfrak{p} = L_{M,\mathfrak{p}}$ by definition. More generally, by the definition of the discriminant, we have

$$d(R_l/O)d(R_r/O)(R \oplus R) \subset R_l \otimes R_r \subset M \otimes_F M.$$

This shows the desired assertion. □

For a prime $\mathfrak{l}$ outside the discriminant of B/F, identifying $B_\mathfrak{l}$ with $M_2(F_\mathfrak{l})$, we define the Eichler order of level $\mathfrak{l}^m$ by

$$\widehat{O}_0(\mathfrak{l}^m)_\mathfrak{l} = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(F_\mathfrak{l}) \middle| c \in \mathfrak{l}^m O_\mathfrak{l}\right\}.$$

Here $\widehat{O}_0(\mathfrak{l}^0)_{\mathfrak{l}}$ is the fixed maximal order of $B_{\mathfrak{l}}$. We then put for ideals $\mathfrak{N}$ outside the discriminant of B/F, $\widehat{O}_0(\mathfrak{N}) = \prod_{\mathfrak{l}} \widehat{O}_0(\mathfrak{l}^{e(\mathfrak{l})})$, where $\mathfrak{N} = \prod_{\mathfrak{l}} \mathfrak{l}^{e(\mathfrak{l})}$ is the prime decomposition of $\mathfrak{N}$ (for $\mathfrak{l} \nmid \mathfrak{N}$, we agree to put $e(\mathfrak{l}) = 0$).

We identify B_p with $M_2(F_p)$ so that r and l both bring $(x,y) \in M_p = M_{\Sigma_p} \times M_{\Sigma_p c}$ onto $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$ in $M_2(F_p)$. For $\mathfrak{l}|\mathfrak{f} = \mathfrak{F} \cap O$, we take the factor $\mathfrak{L}|\mathfrak{l}$ so that $\mathfrak{L}|\mathfrak{F}$, and we identify $B_{\mathfrak{l}}$ with $M_2(F_{\mathfrak{l}})$ bringing $(x,y) \in M_{\mathfrak{l}} = M_{\mathfrak{L}} \times M_{\overline{\mathfrak{L}}}$ to $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$ in $M_2(F_{\mathfrak{l}})$. For $\mathfrak{l}|D(M/F)$, we embed $M_{\mathfrak{l}}$ by $r = l$ into the $O_{\mathfrak{l}}$–order of $M_2(F_{\mathfrak{l}})$ generated by the scalar in $O_{\mathfrak{l}}$ and $\Delta_0^B(\mathfrak{l})$, that is the Eichler order $\widehat{O}_0(D(M/F))_{\mathfrak{l}}$ of level $D(M/F)_{\mathfrak{l}}$.

Proposition 7.2. *Suppose the following three conditions:*

(a) *$p\mathfrak{N}$ is prime to $\mathfrak{D} = d(R_r/O)d(R_l/O)$;*

(b) *$L_{\mathfrak{f}p} = \widehat{O}_0(\mathfrak{f}\mathfrak{p}^e)_{\mathfrak{f}p} \subset B_{\mathfrak{f}p}$ for the conductor $\mathfrak{p}^e = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p})}$ of ε_2;*

(c) *$\varepsilon_{1,p}$ is trivial on $O_p^\times$ and $\kappa = (I, 0)$.*

Let $v \in L(\kappa\varepsilon; \overline{W}) = \overline{W}$ and $w \in L(\kappa^*\varepsilon^*; \overline{W}) = \overline{W}$. Then $\phi : L \to \overline{W}$ given by $\phi(\gamma) = [\gamma v, w]$ is a $\overline{W}$–integral linear combination of functions of the form $\phi_1 \otimes \phi_2$ for functions $\phi_j : L^j \to \overline{W}$ such that

(1) *$\phi_1(x) = \phi_{1,p}(x_p)\phi_1^{(p)}(x^{(p)})$ (resp. $\phi_2(x) = \phi_{2,p}(x_p)\phi_2^{(p)}(x^{(p)})$), where we embed $x \in M$ into $M_p \times M^{(p)}$ by $x \mapsto (x_p, x^{(p)})$ and for a $\mathbb{Z}$–module $X \subset B$, $X^{(p)} = X \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(p)}$ with $\widehat{\mathbb{Z}}^{(p)} = \prod_{\ell \nmid p} \mathbb{Z}_\ell$;*

(2) *$\phi_{2,p}\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) = \varepsilon_2(d)$ if $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) \in O_p^2$ and vanishes outside $O_p \times O_p^\times \subset O_p^2 = L_p^2$;*

(3) *$\phi_{1,p}$ is the characteristic function of $L_p^1 \cong O_p \times \mathfrak{p}^e O_p$;*

(4) *$\phi_j^{(p)}$ ($j = 1, 2$) factors through the finite quotient $L^j/\mathfrak{f}\mathfrak{D}L^j$ of $L^{j,(p)}$;*

(5) *the function ϕ_j is supported on L^j and has values in $\overline{W}$.*

Proof. We regard ϕ as a function of $B_{\mathbb{A}}^{(\infty)} = B_p \times B_{\mathbb{A}}^{(p\infty)}$ supported on $\widehat{L}$ so that $\phi(b) = \phi_p(b_p)\phi^{(p)}(b^{(p)})$ for $\phi_p = \phi|_{B_p}$ and $\phi^{(p)} = \phi|_{B_{\mathbb{A}}^{(p\infty)}}$. We identify B_p with

$$M_2(F_p) = M_p \oplus M_p = \begin{pmatrix} R_{\Sigma_p c} & R_{\Sigma_p c} \\ R_{\Sigma_p} & R_{\Sigma_p} \end{pmatrix}.$$

Then $\phi_p\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \varepsilon_1(a)\varepsilon_2(d)[v, w]$ if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \widehat{O}_0(\mathfrak{p}^e)_p$. This shows the desired assertion for ϕ_p.

As for the component outside p, we only need to prove that the characteristic function $\chi_{L^{(p)}}$ of $L^{(p)}$ is a finite $\overline{W}$–linear combination of tensor products of $\overline{W}$–integral locally constant functions. Note that any additive character $L^M/L_M \to \overline{W}^\times$ is a tensor product of $\overline{W}$–integral valued additive characters of $L^M/L_M = L^{M,(p)}/L_M^{(p)}$, because $[L^M : L]$ is a product of primes dividing the discriminant $\mathfrak{D}$ by the proposition. We then have $\chi_L = [L^M : L]^{-1} \sum_\psi \psi$, where ψ running through all additive characters of $L^{M,(p)}/L^{(p)}$. Note that $\psi = \psi_1 \otimes \psi_2$ with locally constant additive characters of $\psi_j : L^j \to \overline{W}^\times$.

Thus we may take $\phi_1(x_p, x^{(p)}) = \phi_{1,p}(x_p)\psi_1(x^{(p)})\varepsilon_2^{(p)}(x^{c(p)})$ and $\phi_2(y_p, y^{(p)}) = \phi_{2,p}(y_p)\psi_1(y^{(p)})\varepsilon_1^{(p)}(y^{(p)})$ for $(x, y) \in L^1 \oplus L^2$. Since ψ_j (resp. $\varepsilon_j^{(p)}$) factors through $L^j/\mathfrak{D}L^j$ by Lemma 7.1 (resp. $L^j/\mathfrak{f}L^j$ by definition), we conclude that $\phi_j^{(p)}$ factors through $L^j/\mathfrak{f}\mathfrak{D}L^j$. □

Let $B = M_2(F)$. We choose two fractional ideals $\mathfrak{B}_1$ and $\mathfrak{B}_2$ of M. Then we decompose $\mathfrak{A} = Oz_1 + \mathfrak{a}z_2$ and $\mathfrak{B} = Ow_1 + \mathfrak{b}w_2$ with $z_0 = z_1/z_2 \in \mathfrak{H}^I$ and $w_0 = w_1/w_2 \in \mathfrak{H}^I$. The regular representation l of R on $\mathfrak{B}_1$ given by $l(\alpha)\left(\begin{smallmatrix} z_0 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} z_0\alpha \\ \alpha \end{smallmatrix}\right)$ gives an embedding of R into

$$O_L^l = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \middle| a, d \in O,\ b \in \mathfrak{a},\ c \in \mathfrak{a}^{-1} \right\}.$$

Similarly we define an embedding $r : R \hookrightarrow O_L^r$ replacing z_0 by w_0, where

$$O_L^r = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \middle| a, d \in O,\ b \in \mathfrak{b},\ c \in \mathfrak{b}^{-1} \right\}.$$

We consider the tensor product: $\mathfrak{B}_1 \otimes_O \mathfrak{B}_2$ and $L = l(\mathfrak{B}_1)v \cdot r(\mathfrak{B}_2) \subset M_2(F)$ for a suitable $v \in M_2(F)$.

We want to determine the factors of L_M and L^M. Since L^1 is the projection of L to the first factor M of $M \otimes_F M = M \oplus M$, writing the projection to the first factor as $(a \otimes b) \mapsto a^c b$ (so the projection to the second factor is given by $(a \otimes b) \mapsto a^c b^c$), we have $L^1 \cong \mathfrak{B}_1^c\mathfrak{B}_2$ and $L^2 \cong \mathfrak{B}_1^c\mathfrak{B}_2^c$.

Since $R \otimes_O R$ can be identified with

$$\left\{(a, b) \in R \oplus R \middle| a \equiv b \mod \mathfrak{d}(M/F)\right\}$$

inside $R \oplus R \subset M \otimes_F M$ for the relative different $\mathfrak{d}(M/F)$ for M/F, we see that $L_1 \cong \mathfrak{B}_1^c\mathfrak{B}_2\mathfrak{d}(M/F)$ and $L_2 \cong \mathfrak{B}_1^c\mathfrak{B}_2^c\mathfrak{d}(M/F)$.

Remark 7.1. We analyze the choice of v locally at primes $\mathfrak{p}|p$ of F when $\mathfrak{B}_{j,\mathfrak{p}} = R_\mathfrak{p}$ for $j = 1, 2$. Since the prime ideal $\mathfrak{p}$ is split into $\mathfrak{P}\mathfrak{P}^c$ with $\mathfrak{P} \in \Sigma_p$ in M, by choosing the base (e_1, e_2) for $e_1 = (1, 0), e_2 = (0, 1)$ of $R_\mathfrak{p} = R_{\mathfrak{P}^c} \oplus R_\mathfrak{P}$ over $O_\mathfrak{p}$, we may assume that $l(\alpha) = r(\alpha) = \left(\begin{smallmatrix} \alpha^c & 0 \\ 0 & \alpha \end{smallmatrix}\right)$. Then we choose v to be $b = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. By computation, we have

$$l(\alpha)b \cdot r(\beta^c) = \left(\begin{smallmatrix} \alpha^c & 0 \\ 0 & \alpha \end{smallmatrix}\right) b \begin{pmatrix} \beta & 0 \\ 0 & \beta^c \end{pmatrix} = \begin{pmatrix} \alpha^c\beta & \alpha^c\beta^c \\ \alpha\beta & \alpha\beta^c \end{pmatrix}.$$

This shows that $l(R_\mathfrak{p})b \cdot r(R_\mathfrak{p}) = M_2(O_\mathfrak{p})$, and regarding $M_2(O_\mathfrak{p})$ as an $R_\mathfrak{p}$–module via $\alpha x = l(\alpha)x$, we find

$$M_2(O_\mathfrak{p}) = \begin{pmatrix} R_{\mathfrak{P}^c} & R_{\mathfrak{P}^c} \\ R_\mathfrak{P} & R_\mathfrak{P} \end{pmatrix}.$$

Take $O_\mathfrak{p}$ basis $w = (w_1, w_2)$ and $z = (z_1, z_2)$ of $R_\mathfrak{p}$ in M so that $w \equiv z \equiv (e_1, e_2)$ mod $\mathfrak{p}^m$ for $m \geq e(\mathfrak{p})$ for $e(\mathfrak{p})$ as in Proposition 7.2.

We define $p(z, w) = z_2 w_2 p(z_0, w_0)$ and $[u; z, w] = S(u, p(z, w))$ (the homogeneous form of $[u; z_0, w_0]$). Then we find $[b; z, w] = (z_1 - z_2)(w_2 - w_1)$ and that $[b; z, w]$ is a $\mathfrak{p}$–adic unit.

7.3. Proof. We first suppose that $[F:\mathbb{Q}]$ is even. Then we have a definite quaternion algebra $B_{/F}$ with $d(B/F)=1$ and $I_B=\emptyset$. We write $G_{/\mathbb{Q}}$ for the algebraic group associated to $B^\times$.

We fix a maximal order O_B and identify $\widehat{O}_B$ with $M_2(\widehat{O})$ once and for all. Thus $\widehat{O}_0(\mathfrak{N})\subset\widehat{O}_B$ is an open compact subring. We have $U_0^B(\mathfrak{N})=\widehat{O}_0(\mathfrak{N})^\times$. We fix complete representative sets $\{a_1,\dots,a_h\}$ for $G(\mathbb{Q})\backslash G(\mathbb{A})/U_0^B(\mathfrak{N})G(\mathbb{R})F_{\mathbb{A}}^\times$ with $a_{i,\mathfrak{N}p}=a_\infty=1$ and $Z\subset(F_{\mathbb{A}}^\times)^{(\mathfrak{N}p\infty)}$ for $Cl_F=F_{\mathbb{A}}^\times/F^\times\widehat{O}^\times F_\infty^\times$. We consider

$$\text{(7.8)}\quad \Delta_{ijz}(\mathfrak{N})=a_i^{-\iota}z\cdot\Delta_0^B(\mathfrak{N})a_j^\iota\cap B, O_{ijz}(\mathfrak{N})=a_i^{-\iota}z\cdot\widehat{O}_0(\mathfrak{N})a_j^\iota\cap B\ (z\in Z)$$
$$\text{and}\ \ \Gamma_0^i(\mathfrak{N})=G^1(\mathbb{Q})\cap a_iU_0^B(\mathfrak{N})a_i^{-1}G(\mathbb{R}),$$

where $G^1(A)=\{g\in G(A)|gg^\iota=1\}$. Thus $\Delta_{ijz}(\mathfrak{N})\subset O_{ijz}(\mathfrak{N})$. Note here that $\{a_iz|z\in Z\}_{i=1,\dots,h}$ gives a complete representative set for $G(\mathbb{Q})\backslash G(\mathbb{A})/U_0^B(\mathfrak{N})G(\mathbb{R})$.

Let $\phi\in H^0(Y_0^B(\mathfrak{N}),L(\kappa\varepsilon;\overline{W}))$; so, we may regard $\phi:G(\mathbb{A})\to L(\kappa\varepsilon;\overline{W})$ with $\phi(\gamma xu)=u^\iota\phi(x)$ for $u\in U_0^B(\mathfrak{N})F_{\mathbb{A}}^\times G(\mathbb{R})F_{\mathbb{A}}^\times$ and $\gamma\in G(\mathbb{Q})$. Similarly, we choose $\phi^*\in H^0(Y_0^B(\mathfrak{N}),L(\kappa^*\varepsilon^*;\overline{W}))$. Then

$$(\phi,\phi^*)_{\overline{W}}=\sum_{i=1}^h[\phi(a_i),\phi^*(a_i)].$$

Pick $y\in F_{\mathbb{A}}^\times$ with $y_p=y_\infty=1$. Supposing ξyd is integral, we consider $\mathbb{T}(\xi yd)$ for $0\ll\xi\in F$. By (unr), we have $d_p=1$. We choose a decomposition

$$U_0^B(\mathfrak{N})\left(\begin{smallmatrix}\xi yd&0\\0&1\end{smallmatrix}\right)U_0^B(\mathfrak{N})=\bigsqcup_{\varpi}\varpi U_0^B(\mathfrak{N}).$$

Here we can choose ϖ so that $\varpi\varpi^\iota=\xi yd$, because

$$U\backslash U\left(\begin{smallmatrix}y&0\\0&1\end{smallmatrix}\right)U/U=U_0^B(\mathfrak{N})\backslash U_0^B(\mathfrak{N})\left(\begin{smallmatrix}y&0\\0&1\end{smallmatrix}\right)U_0^B(\mathfrak{N})/U_0^B(\mathfrak{N})$$

writing $U=\{u\in U_0^B(\mathfrak{N})|uu^\iota=1\}$. Thus $\varpi_p\varpi_p^\iota=\xi$. Then

$$\phi|\mathbb{T}(\xi yd)(x)=\xi^{-\kappa_2}\sum_{\varpi}\varpi_{p\mathfrak{N}}\phi(x\varpi^{-\iota}).$$

Since $a_i\varpi^{-\iota}\in\sqcup_{j,z}G(\mathbb{Q})a_jz\cdot U_0^B(\mathfrak{N})G(\mathbb{R})$, we can write $a_i\varpi^{-\iota}=\gamma_ia_ju_iz$ for $\gamma_i^{-\iota}\in\Delta_{ijz}(\mathfrak{N})$ and $u_i\in U_0^B(\mathfrak{N})G(\mathbb{R})$. Thus we have, writing $\mathfrak{a}_i=N_{B/F}(a_i)\widehat{O}\cap F$ and $\mathfrak{y}=y\widehat{O}\cap F$, $\mathfrak{a}_j\mathfrak{y}\mathfrak{d}\mathfrak{z}^2\xi=N(\gamma_i^{-1})\mathfrak{a}_i\ \mathfrak{z}=z\widehat{O}\cap F$; in other words, $\mathfrak{y}^{-1}\mathfrak{d}^{-1}\mathfrak{a}_i\mathfrak{a}_j^{-1}\mathfrak{z}^{-2}$ is generated by a totally positive element $\alpha_{ijz}\in F$ prime to $p\mathfrak{N}$. Thus we have

$$\xi=\alpha_{ijz}\gamma_i^{-1}\gamma_i^{-\iota}\ \text{ up to totally positive units.}$$

Then we see, up to totally positive units,

$$\phi|\mathbb{T}(\xi yd)(a_i)=\xi^{-\kappa_2}\sum_{\varpi}\varpi_{p\mathfrak{N}}\phi(a_i\varpi^{-\iota})=\alpha_{ijz}^{-\kappa_2}\sum_{\gamma_i}N_{B/F}(\gamma_i)^{\kappa_2}\gamma_i^{-\iota}\phi(a_j).$$

Here, extending $\varepsilon : U_0(\mathfrak{N}) \to \overline{\mathbb{Q}}^\times$ to $\varepsilon : U_0(\mathfrak{N})F_{\mathbb{A}}^\times \to \overline{\mathbb{Q}}_p^\times$ by the p–adic avatar $\widehat{\varepsilon}_+ : F_{\mathbb{A}}^\times/F^\times \to \overline{\mathbb{Q}}_p^\times$ of the central character ε_+, we have

$$N_{B/F}(\gamma_i)^{\kappa_2}\gamma_i^{-\iota}\phi(a_j) = \varepsilon(\gamma_i^{-\iota})\phi(a_j)\left(\sigma(\gamma_i^{-1})\left(\begin{smallmatrix} X_\sigma \\ Y_\sigma \end{smallmatrix}\right)\right),$$

which is p–integral if $\phi(a_j)$ is in $L(\kappa\varepsilon; \overline{W})$.

Since B is totally definite ($|I_B| \leq 1$ and $|I_B| \equiv [F : \mathbb{Q}] \mod 2 \Rightarrow I_B = \emptyset$), $\overline{\Gamma}_0^i(\mathfrak{N}) = \Gamma_0^i(\mathfrak{N})/O^\times$ is a finite group. We then put $e_i = |\overline{\Gamma}_0^i(\mathfrak{N})|$. Defining

$$\Theta_{ijz}(v, w) = \frac{1}{e_i e_j} \sum_{\gamma \in \Delta_{ijz}(\mathfrak{N}) \cap Supp(\varepsilon)} N_{B/F}(\gamma)^{-\kappa_2}[\gamma v, w] q^{\alpha_{ijz}\gamma\gamma^\iota}$$

for $v \in H^0(\Gamma_0^j(\mathfrak{N}), L(\kappa\varepsilon; \overline{W}))$ and $w \in H^0(\Gamma_0^i(\mathfrak{N}), L(\kappa^*\varepsilon^*; \overline{W}))$ (and rewriting $\gamma_i^{-\iota}$ as γ), we find for $y \in F_{\mathbb{A}}^\times$ with $y_p = 1$

$$f(\phi \otimes \phi^*)(y) = N(y)^{-1} \sum_{i,j,z; \mathfrak{a}_i \mathfrak{a}_j^{-1} \mathfrak{z}^{-2} \sim \mathfrak{y}\mathfrak{d}} \alpha_{ijz}^{-\kappa_2} \Theta_{ijz}(\phi(a_j), \phi^*(a_i)), \tag{7.9}$$

where $\mathfrak{a} \sim \mathfrak{b}$ indicates that the two ideals belong to the same strict class in F. Here Θ_{ijz} is a theta series of the O–lattice $\Delta_{ijz}(\mathfrak{N})$ and is a Hilbert modular form of weight $\kappa\varepsilon$ on $\Gamma_0(\mathfrak{N}; \mathfrak{y})$ for $\mathfrak{y} = F \cap y\widehat{O}$. Since the pairing: $[\ ,\ ]$ is p–integral valued on $L(\kappa\varepsilon; \overline{W}) \times L(\kappa^*\varepsilon^*; \overline{W})$ and α_{ijz} is prime to $p\mathfrak{N}$, the theta series has p–integral Fourier coefficients (except possibly for the constant term). The constant term does not show up if $\phi \in H^0_{n.ord}(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W)) \subset H^0_{cusp}(Y_0^B(\mathfrak{N}), L(\kappa\varepsilon; W))$. Thus restricting ϕ to the ordinary part, $f(\phi \otimes \phi^*)$ has to be cuspidal (cf. [H88a] Theorem 6.2) and hence, the constant term vanishes. We may forget about the integrality problem stemming from the denominator: $e_i e_j$.

We choose an ideal $\mathfrak{A}$ of M with $N_{M/F}(\mathfrak{A}) \sim \mathfrak{y}$. We choose $\alpha \gg 0$ with $\mathfrak{y}^{-1}\mathfrak{d}^{-1}N_{M/F}(\mathfrak{A}) = (\alpha)$. Then we consider the theta series defined in (6.6):

$$\theta(\lambda; \mathfrak{A}) = \sum_{\gamma \in \mathfrak{A}^{-1}} \lambda(\gamma)(\gamma\gamma^c)^{-\kappa_2} q^{\alpha\gamma\gamma^c}$$

for a Hecke character λ of conductor $\mathfrak{C}$ with $\lambda(\alpha) = \alpha^{\kappa_1\Sigma + \kappa_2\Sigma c}$ if $\alpha \equiv 1 \mod \mathfrak{C}$. Strictly speaking, we need to divide the above series by $|\mu(M)|$ (see (6.6)), but $|\mu(M)|$ is prime to p by the unramifiedness of p in $M/\mathbb{Q}$. So we forget about $|\mu(M)|$. Here we have freedom of choosing $\mathfrak{A}$ in its ideal class (by changing $\alpha \gg 0$ suitably).

We define the reversed Petersson inner product $(f, g) = \langle g, f \rangle = \overline{\langle f, g \rangle}$ to make it linear with respect to the right variable g. By the variable change $z \mapsto -\overline{z}$, we have

$$(f, g) = \langle f_c, g_c \rangle \quad \text{for } f_c(z) = \overline{f(-\overline{z})}. \tag{7.10}$$

Unless the following condition is met:

$$\text{(7.11)} \qquad \kappa = (I, 0) \text{ and } (\lambda^-)^*(\mathfrak{P}^c) \equiv 1 \mod \mathfrak{m}_W \text{ for some } \mathfrak{P} \in \Sigma_p,$$

we have proven in [H05d] Proposition 5.6 the following equality up to units in $\overline{W}$:

$$\text{(MT)} \qquad L_p(\widehat{\lambda^-}) = \frac{(2\pi i)^{2(\kappa_1-\kappa_2)} W_p(\lambda^-)(f(\lambda), f(\lambda))_{\mathfrak{N}}}{\Omega^{2(\kappa_1-\kappa_2)}} \in \overline{W},$$

where $W_p(\lambda) = \prod_{\mathfrak{P}\in\Sigma_p} W(\lambda_{\mathfrak{P}})$ and

$$W(\lambda_{\mathfrak{P}}) = N(\mathfrak{P}^{-e(\mathfrak{P})})\lambda(\varpi_{\mathfrak{P}}^{-e(\mathfrak{P})}) \sum_{u\in(R/\mathfrak{P}^{e(\mathfrak{P})})^\times} \lambda_{\mathfrak{P}}(u)\mathbf{e}_M\left(\frac{u}{\varpi_{\mathfrak{P}}^{e(\mathfrak{P})}}\right)$$

if $e(\mathfrak{P}) > 0$ and $W(\lambda_{\mathfrak{P}}) = 1$ otherwise. We would like to show (choosing λ in the p–adic analytic family so that (7.11) does not hold)

$$\text{(GL)} \qquad \frac{(2\pi i)^{2(\kappa_1-\kappa_2)} W_p(\lambda^-)(\theta(\lambda;\mathfrak{A}), \Theta_{ijz}(\phi(a_j), \phi^*(a_j)))_\Gamma}{\Omega^{2(\kappa_1-\kappa_2)}} \in \overline{W}$$

for $\Gamma = \Gamma_0(\mathfrak{N}(\lambda);\mathfrak{y})$ and the optimal CM period Ω defined in (7.4), as long as $\phi \in V(R)$ and $\phi^* \in V^*(R)$ for $R = R_P$ as in Corollary 6.4 for P associated to λ.

We write $O_i(\mathfrak{N})$ for $O_{iiz}(\mathfrak{N})$ with $z = 1$. We choose an embedding $i_0 : M \hookrightarrow B$. We may then realize B as

$$B = \left\{\left(\begin{smallmatrix} a^c & b^c \\ b\eta & a \end{smallmatrix}\right) \middle| a, b \in M\right\}$$

with O_B containing $\left(\begin{smallmatrix} a^c & b^c \\ b\eta & a \end{smallmatrix}\right)$ if $a, b \in R$. We define $i_1(a) = \left(\begin{smallmatrix} a^c & 0 \\ 0 & a \end{smallmatrix}\right) \in B$. For primes $\mathfrak{l}$ split in M/F, we assume that our identification $B_{\mathfrak{l}} \cong M_2(F_{\mathfrak{l}})$ is induced by completing $\mathfrak{L}$–adically the above expression of B choosing one prime factor $\mathfrak{L}|\mathfrak{l}$ in M. Taking $a_1 = 1$, we find that $i_1(R) \subset O_1(\mathfrak{N})$ if $\mathfrak{N}$ is made of primes split in M/F. Suppose now that $\mathfrak{N}$ contains primes non-split in M/F. For a given finite set S of primes, we can conjugate the embedding i_1 by a norm 1 element $u_{\mathfrak{l}}$ ($\mathfrak{l} \in S$) so that $ui_1u^{-1}(R_S) \subset O_1(\mathfrak{N})_S$ ($O_1(\mathfrak{N})_S = O_1(\mathfrak{N}) \otimes_O O_S$ for the localization $O_S = \prod_{\mathfrak{l}\in S} O_{\mathfrak{l}}$). By the strong approximation theorem, choosing one prime $\mathfrak{q}$ of F, we can write $u = \gamma u'$ with $\gamma \in G(\mathbb{Q})$ and $u' \in U_0^B(\mathfrak{N})B_{\mathfrak{q}}^\times$. Thus changing i_1 by $\gamma i_1 \gamma^{-1}$, we may assume that for any given $\mathfrak{N}$ that $i_1(R_1) \subset O_1(\mathfrak{N})$ for an O–order $R_1 \subset R$ of $\mathfrak{q}$–power conductor. We identify $M_{\mathbb{A}}^\times$ with the image in $G(\mathbb{A})$ under i_1.

If $d(M/F) \neq 1$, we find $b_1, \ldots, b_j$ in $M_{\mathbb{A}}^\times$ so that $N_{M/F}(b_j)$ gives a complete representative set for $F^\times\backslash F_{\mathbb{A}}^\times/\widehat{O}^\times(F_{\mathbb{A}}^\times)^2$. By the reduced norm map: $N_{B/F} : G(\mathbb{A}) \to F_{\mathbb{A}+}^\times$, we have a surjection:

$$G(\mathbb{Q})\backslash G(\mathbb{A})/U_0^B(\mathfrak{N})G(\mathbb{R})F_{\mathbb{A}}^\times \twoheadrightarrow F_+^\times\backslash F_{\mathbb{A}+}^\times/\widehat{O}^\times(F_{\mathbb{A}}^\times)^2.$$

Thus we can choose $\{a_i = b_j s_k\} = \{b_j\} \times \{s_k\}$ so that $N_{B/F}(s_k) = 1$. Then again by the strong approximation theorem, we can write $s_k = \gamma_k u_k$ with $u_k \in U_0^B(\mathfrak{N})B_{\mathfrak{q}}^\times$ and $\gamma_k \in G(\mathbb{Q})$. Since b_j commutes with $i_1(R_1)$, conjugation by b_j does not alter i_1. Then defining $i_j : M \to B$ by $\gamma_k i_1 \gamma_k^{-1}$ and putting R_j to be the inverse image under i_j of $i_j(M) \cap O_j(\mathfrak{N})$, we find that R_j is an O–order of M of $\mathfrak{q}$–power conductor.

Suppose now that $d(M/F) = 1$. In this case, the image of $M_{\mathbb{A}}^{\times}$ in the class group $F_+^{\times}\backslash F_{\mathbb{A}+}^{\times}/\widehat{O}^{\times}F_{\infty+}^{\times}$ under the norm map is of index two; so, we need to add one more element $b' \in G(F_{\mathfrak{q}})$ with $N_{M/F}(b)$ generating $\mathfrak{q}O_{\mathfrak{q}}$, choosing the prime $\mathfrak{q}$ to be inert in M/F. Then the representatives a_i can be chosen as $b_j s_k$ or $b_j b' s_k$ for $s_k \in SL_2(F_{\mathfrak{q}})$ and $b_j \in M_{\mathbb{A}}^{\times}$. Thus, by the same argument as above, we find again an O–order R_j of $\mathfrak{q}$–power conductor and an embedding $i_j : R_j \hookrightarrow O_j(\mathfrak{N})$. We have now proven:

Lemma 7.3. *Let the notation be as above. By choosing a prime ideal $\mathfrak{q}$ of F outside any given finite set of primes, we can embed the order $O + \mathfrak{q}^m R \subset M$ of $\mathfrak{q}$–power conductor into $O_j(\mathfrak{N})$ for all $j = 1, 2, \ldots, h$, if the conductor $\mathfrak{q}^m$ is sufficiently deep.*

We write R_j for $O_j(\mathfrak{N}) \cap R$. By the above lemma, we assume that R_j is of conductor $\mathfrak{q}^{m(j)}$. We choose later $\mathfrak{q}$ in a way optimal to our proof. We regard $L_{ijz} = O_{ijz}(\mathfrak{N})$ as $R_i \otimes_O R_j$ module by i_1: $(\alpha,\beta)b = \alpha b \beta$. Since $M \otimes_F M = M \oplus M$, writing 1_r (resp. 1_l) the idempotent of left and right factors, we split $O_{ijz}(\mathfrak{N}) \subset L_{ijz}^M = 1_r L_{ijz} \oplus 1_l L_{ijz}$. The index $[L_{ijz}^M : L_{ijz}]$ is a product of a power of $\mathfrak{q}$ and primes ramifying in M/F, which we can choose to be prime to p. Then as studied in Subsection 7.2, we can write Θ_{ijz} of level $\mathfrak{N}$ as a p–integral linear combination of $\theta(\phi_1)\theta(\phi_2)$ of theta series of $L_{ijz}^r = 1_r L_{ijz}$ and $L_{ijz}^l = 1_l L_{ijz}$, respectively. The functions ϕ_k $(k = 1, 2)$ can be chosen to be p–integral.

We now bound the level of $\theta(\phi_k)$. To make the argument simple, first assume that $i_1(R) \subset O_1(\mathfrak{N})$, $a_i = b_{i'}$ and $a_j = b_{j'}$, and we choose that $b_{i'}$ so that $b_{i',\mathfrak{l}} = 1$ for all primes $\mathfrak{l}|\mathfrak{N}p \cdot d(M/F)\mathfrak{q}$. Note that $b_{i'}z \cdot O_0(\mathfrak{N})b_{j'}^{-1} = \mathfrak{z}\mathfrak{b}_{i'} \otimes \mathfrak{b}_{j'}^{-1}$ as $R \otimes_O R$–modules for $\mathfrak{b}_{i'} = (b_{i'}\widehat{R} \cap M)$, we find from the discussion at the end of the previous section that $L_{ijz}^1 = \mathfrak{z}\mathfrak{b}_{i'}^c\mathfrak{b}_{j'}^{-1}$ and $L_{ijz}^2 = \mathfrak{z}\mathfrak{b}_{i'}^c\mathfrak{b}_{j'}^{-c}$. Thus we find that $\mathfrak{y}\mathfrak{d} = \mathfrak{a}_i^{-1}\mathfrak{a}_j\mathfrak{z}^2 = N_{M/F}(L_{ijz}^1) = N_{M/F}L_{ijz}^2$.

As explained in the introduction, we take φ with $\psi = \varphi^-$. We may assume that the weight κ of $f(\varphi)$ is $(I, 0)$. We than take a weight κ member $f(\lambda)$ of the p–adic family (associated with φ: $\widehat{\lambda}|_{G_{tor}(\mathfrak{C})} = \varphi$) with complex multiplication by M. To avoid (7.11) ($\Leftrightarrow$ (MT)), we choose ε so that it is non-trivial at all $\mathfrak{p}|p$. Replacing φ by $\varphi\eta$ for a finite order character $\eta : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{W}^{\times}$ does not alter the anticyclotomic part φ^-. By a theorem of Chevalley ([Ch]), we can choose η so that $\eta_{\mathfrak{l}} = \lambda_{\mathfrak{l}}^{-1}$ on the inertia group at $\mathfrak{l}$ for every prime $\mathfrak{l}$ in any given finite set of prime ideals. Thus we may assume

$$\lambda \textit{ has conductor prime to } \Sigma_p\mathfrak{c}. \tag{7.12}$$

Write $\mathfrak{N} = \mathfrak{N}(\lambda)$. Under this assumption, $\kappa = \kappa^*$, $\varepsilon^* = \varepsilon^{-1}$ and $[v, w] = vw$ by identifying $L(\kappa\varepsilon; \overline{W}) = \overline{W}$ (on which $\Delta_0(\mathfrak{N})$ acts via multiplication by ε) and $L(\kappa^*\varepsilon^*; \overline{W}) = \overline{W}$. Then

$$[\gamma\phi(a_j), \phi^*(a_i)] = \varepsilon(\gamma_{\mathfrak{f}p})\phi(a_j)\phi^*(a_i).$$

Regarding the character $\varepsilon : \Delta_0^B(\mathfrak{N})_{\mathfrak{f}p} \to \overline{W}^\times$ as a function ε_{ijz} of $B \otimes_{\mathbb{Q}} \mathbb{A}^{(\infty)}$ supported on $\widehat{\Delta}_{ijz}(N) = a_i^\iota z \Delta_0^B(\mathfrak{N}) a_j^{-\iota}$ by $\varepsilon_{ijz}(x) = \varepsilon(x_{\mathfrak{f}p})$ $(\widehat{\Delta}_{ijz}(N)_{\mathfrak{f}p} = \Delta_0^B(N)_{\mathfrak{f}p})$, the function $\chi_{ijz} : \gamma \mapsto \varepsilon(\gamma)[\gamma\phi(a_j), \phi^*(a_i)]$ is the function ε_{ijz} multiplied by the p–integral constant: $\phi(a_j)\phi^*(a_i)$. Write down χ_{ijz} as a sum $\chi_{ijz} = \sum_{\phi_1,\phi_2} \phi_1 \otimes \phi_2$ for finitely many p–integral locally constant functions $\phi_1 : L^1_{ijz} \to \overline{W}$ and $\phi_2 : L^2_{ijz} \to \overline{W}$. By Proposition 7.2, $\phi_{2,p}(x_p) = \lambda_{\Sigma_p}(x_{\Sigma_p})$ on $R_{\Sigma_p c} \times R^\times_{\Sigma_p}$ and is supported by $(R_{\Sigma_p c} \times R^\times_{\Sigma_p}) \subset L^2_{ijz,p}$ (and $\phi_{1,p}$ is the characteristic function of $L^1_{ijz,p} = R_{\Sigma_p c} \times \mathfrak{p}^e R_{\Sigma_p}$).

By the proof of Proposition 7.2, we find that $\phi_k^{(p)}$ $(k = 1, 2)$ factors through $L^k_{ijz}/\mathfrak{d}(M/F)\mathfrak{f}L^k_{ijz}$. Thus $\theta(\phi_k)$ is at least automorphic with respect to the congruence subgroup $\Gamma_0(\mathfrak{N}(\lambda); \mathfrak{y}) \cap \Gamma(d(M/F)^2; \mathfrak{y})$, where

$$\Gamma(\mathfrak{N}; \mathfrak{y}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \Gamma_0(\mathfrak{N}; \mathfrak{y}) \middle| a \equiv d \equiv 1 \mod \mathfrak{N} \right\}.$$

This follows from the fact that ϕ_k as above is a linear combination of p–integral functions χ of the lattice $(\mathfrak{z}\mathfrak{b}^c_{j'}, \mathfrak{b}^{-1}_{i'})$ modulo $(\mathfrak{z}\mathfrak{b}^c_{j'}, \mathfrak{b}^{-1}_{i'}\mathfrak{d}(M/F))$ for a sufficiently large m and the fact that $\theta(\chi) = \sum_{\xi \in M} \chi(\xi) q^{\alpha_{ijz}\xi\xi^c}$ has the level as described above.

More generally, when $a_i = b_{i'}s$ and $a_j = b_{j'}s'$ for s or s' with norm 1 in $B^\times_{\mathfrak{q}}$, R_i and R_j could have conductor a power of $\mathfrak{q}$; so, the same argument yields that $\theta(\phi_k)$ is on $\Gamma = \Gamma_0(\mathfrak{N}(\lambda); \mathfrak{y}) \cap \Gamma(d(M/F)^2\mathfrak{q}^m; \mathfrak{y})$ for a sufficiently large m.

As seen in (6.6), the $\mathfrak{y}$–component of $f(\lambda)$ is given by a p–integral finite sum $|\mu(M)|^{-1} \sum_{\mathfrak{A}} \lambda(\mathfrak{A})\theta(\lambda; \mathfrak{A})$ of theta series of the form:

$$\theta(\lambda; \mathfrak{A}) = \sum_{\xi \in \mathfrak{A}^{-1}} \lambda(\xi^{(\Xi\infty)}) q^{\alpha\xi\xi^c},$$

where $\mathfrak{A}\mathfrak{A}^c = \alpha\mathfrak{y}\mathfrak{d}$ (with $\alpha \gg 0$ in F). Here the sum $\sum_{\mathfrak{A}} \lambda(\mathfrak{A})\theta(\lambda; \mathfrak{A})$ is over ideal classes of M whose norm isequivalent to $\mathfrak{y}\mathfrak{d}$. By choosing $v \in M_2(F)$ and $(z_0, w_0) \in \mathfrak{H}^I \times \mathfrak{H}^I$ as in Section 4, we identify $M_2(F)$ with $M \oplus M$. Then we choose $\mathcal{L} = \mathfrak{A}^{-1} \oplus L^2_{ijz}$ as an O–lattice of $M_2(F)$. Since we have freedom of changing $\mathfrak{A}$ in its ideal class, we may assume that the p–adic completion $\mathcal{L}_p = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is equal to $M_2(O_p)$ in $M_2(F_p) = B_p$, because $L^2_{ijz} = O_p \oplus O_p$. Then $\mathcal{L}^1 = \mathfrak{A}^{-1}$ and $\mathcal{L}^2 = L^2_{ijz}$. We take $\phi'_1 : \mathcal{L}^1 \to \overline{W}$ so that $\theta(\phi'_1) = \theta(\lambda; \mathfrak{A})$. Then $\phi'_1(\xi) = \lambda(\xi^{(\Xi\infty)})$ and $\phi'_{1,\Sigma_p} = \lambda^{-1}_{\Sigma_p}(\xi_{\Sigma_p})$, and $\phi'_{1,\Sigma_p c}$ is the characteristic function of $R_{\Sigma_p c}$.

We choose two ideals $\mathfrak{B}_1$ and $\mathfrak{B}_2$ of M and $v \in M_2(F)$ very close p–adically to $b = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in M_2(F_p)$ as in Remark 7.1 so that $L = l(\mathfrak{B}_1)v \cdot r(\mathfrak{B}_2) \subset \mathcal{L}$ with $\mathcal{L}/L$ killed by a power of $d(M/F)\mathfrak{q}$. Here we need to introduce another prime $\mathfrak{q}$, because $\mathcal{L}^2$ is stable only by an O–order in M of $\mathfrak{q}$–power conductor. We choose the base $\mathfrak{B}_1 = Oz_1 + \mathfrak{y}z_2$ and $\mathfrak{B}_2 = Ow_1 + \mathfrak{y}w_2$ again as in Remark 7.1. Let $z = (z_1, z_2)$ and $w = (w_1, w_2)$. Thus $z_0 = z_1/z_2$ and $w_0 = w_1/w_2$ are both in $\mathfrak{H}^I$. Thus we have from Theorem 4.1 and (7.10) that:

$$(\theta(\phi_1'), \theta(\phi_1)\theta(\phi_2))_\Gamma = \langle \theta(\phi_1')_c, \theta(\phi_1 \otimes \phi_2)_c \rangle_\Gamma = C\Psi(z, w)$$

for a constant $C \in \overline{W}^\times$ and a congruence subgroup

$$\Gamma = \Gamma_0(\mathfrak{N}(\lambda); \mathfrak{y}) \cap \Gamma(d(M/F)^2\mathfrak{q}^m; \mathfrak{y}) \quad (m \gg 0).$$

Here $\Psi(z, w)$ is the homogeneous version of the modular form:

$$\Psi(z_0, w_0) = \sum_{0 \ll \alpha \in \Gamma \backslash M_2(F)} \phi^{*(\infty)}(\epsilon\alpha)\mathbf{e}_F(\det(\alpha)z_0)\theta(\phi_1)|_1\alpha(w_0) \tag{7.13}$$

for the partial Fourier transform ϕ^* of $\phi = \overline{\phi}_1' \circ c \otimes \phi_2$, because $\theta(\phi)_c(z) = \overline{\theta(\phi)(-\overline{z})} = \theta(\overline{\phi \circ c})$. The constant C is prime to p (that is, $i_p(C) \in W^\times$) because of the following reason: Since Ψ is of weight (I, I), the homogeneous form is given by $z_2^I w_2^I \Psi(z, w) = \Psi(z_0, w_0)$. Since v is very close p–adically to b, we may assume that $v = b$. Then by Theorem 4.1 and $[b; z, w] = (z_1 - z_2)(w_2 - w_1)$, we have

$$\begin{aligned} C = z_2^I w_2^I \operatorname{Im}(z_0)^{-I} \operatorname{Im}(w_0)^{-I} [b; z_0, w_0]^I |[b; z_0, w_0]|^{2I} \\ = \frac{(z_1 - z_2)(w_2 - w_1)|(z_1 - z_2)(w_2 - w_1)|^2}{(z_1\overline{z}_2 - \overline{z}_1 z_2)(w_1\overline{w}_2 - \overline{w}_1 w_2)}, \end{aligned}$$

whose image under i_p is easily seen to be in $W^\times$ (by our choice of the base z and w as in Remark 7.1).

The local partial Fourier transform preserves p–integral Schwartz-Bruhat functions on $M_2(F_\mathfrak{l})$ as long as $\mathfrak{l} \nmid p$. Since $M_p = M_{\Sigma_p} \oplus M_{\Sigma_p c}$, we find

$$M_2(F_p) = M_p \oplus M_p = \left(\begin{smallmatrix} M_{\Sigma_p c} & M_{\Sigma_p c} \\ M_{\Sigma_p} & M_{\Sigma_p} \end{smallmatrix}\right).$$

The first column is the factor M_p carrying $\overline{\phi}_{1,p}' \circ c$. The function $\overline{\phi}_{1,p}' \circ c$ is supported on R_p. Since complex conjugation interchanges a and c (see Proposition 7.2), we see from (6.6) that $(\overline{\phi}_{1,p}' \circ c)\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) = \lambda_{\Sigma_p}(a)$ (because we have assumed that λ has conductor prime to Σ_p^c: (7.12)). Similarly, $\phi_{2,p}\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) = \lambda_{\Sigma_p}(d)$ for $b \in R_{\Sigma_p c}$ and $d \in R_{\Sigma_p}$. Thus $\phi_p(a, b)$ equals to $\chi(a, b)\lambda_{\Sigma_p}(a)$ for the characteristic function χ of $R_p = O_p^\times \times O_p$. The partial Fourier transform is with respect to the variables "$(a^{(p)}, b^{(p)})$" keeps p–integrality by the Fourier inversion formula. Thus we may concentrate on the p–component. Define for each $\mathfrak{P} \in \Sigma$, $\Phi_\lambda(x)$ to be equal to $\lambda_\mathfrak{P}(x)$ if $x \in R_\mathfrak{P}^\times$ and 0 outside $R_\mathfrak{P}^\times$. Then the Fourier transform of Φ_λ is given by $W(\lambda_\mathfrak{P})\lambda_\mathfrak{P}(\varpi_\mathfrak{P}^{e(\mathfrak{P})})\Phi_{\overline{\lambda}}(\varpi_\mathfrak{P}^{e(\mathfrak{P})}x)$ (see [BNT]

Proposition 13 in VII.7). Thus we need to prove $W(\lambda^-_{\mathfrak{P}})W(\lambda_{\mathfrak{P}})\lambda(\varpi_{\mathfrak{P}}^{e(\mathfrak{P})}) \in \overline{W}$. This can be done as follows: writing $e = e(\mathfrak{P})$ and $\varpi = \varpi_{\mathfrak{P}}$,

$$\begin{aligned} (7.14)\quad W(\lambda^-_{\mathfrak{P}})\lambda(\varpi^e)W(\lambda_{\mathfrak{P}}) &= N(\mathfrak{P}^{-2e})\lambda(\varpi^e)\lambda(\varpi^{-ce})G(\lambda_{\mathfrak{P}}^{-1})G(\lambda_{\mathfrak{P}}) \\ &= \lambda_{\mathfrak{P}}(-1)\lambda(\varpi^{-ce})\lambda(\varpi^e)N(\mathfrak{P}^{-e}), \end{aligned}$$

where $G(\chi) = \sum_{u\in R/\mathfrak{P}^e} \chi(u)\mathbf{e}_M(\frac{u}{\varpi^e})$ for the conductor $\mathfrak{P}^e$ of χ. Note here that the infinity type of λ is $-\Sigma$, and hence $\lambda(\varpi^e)$ is up to unit equal to $\varpi^{e\Sigma}$ which is equal to $N(\mathfrak{P}^e)$ up to units in $\overline{W}$. This shows the desired integrality.

Since the partial Fourier transform with respect to the character $\mathbf{e}_{\mathbb{A}}(ab' - ba')$ interchanges (a, b), the support of $\overline{\phi}^*_p$ is contained in

$$\begin{pmatrix} O_p & \varpi^{-e}O_p^\times \\ O_p & O_p \end{pmatrix} = \tau^{-1}\begin{pmatrix} O_p & O_p \\ \mathfrak{p}^e O_p & O_p^\times \end{pmatrix} \subset M_2(F_p),$$

where $\tau = \left(\begin{smallmatrix} 0 & -1 \\ \varpi^e & 0 \end{smallmatrix}\right)$.

The function $\phi_{1,p}$ is the characteristic function of $R_{\Sigma_p c} \times \mathfrak{p}^e R^\times_{\Sigma_p}$. Since τ normalizes $U_0(\mathfrak{p}^e)_p$, we can choose complete representative set $\mathcal{R}$ for

$$U_0(\mathfrak{p}^e)_p \backslash \left(\begin{pmatrix} O_p & O_p \\ \mathfrak{p}^e O_p & O_p^\times \end{pmatrix} \times GL_2(F_{\mathbb{A}^{(p\infty)}}) \right)$$

such that $\alpha \in \mathcal{R}$ can be written as $\tau^{-1}\beta$ with p–component β_p is upper triangular (e.g. [MFG] 3.1.6) with p–adic unit at the lower bottom corner. The Hecke operator UxU for $x \in \mathcal{R}$ preserves the p–integral structure of $S_\kappa(\Gamma; W)$ (the space of cusp forms on Γ with W–integral Fourier coefficients). This fact follows, for example, [H88a] Theorem 4.11, and actually, if $x \in GL_2(F)$ has upper triangular p–component with p–adic unit at the lower bottom corner, the action of $\theta \mapsto \theta|_1 x$ on modular forms preserves p–integrality since it is basically given by $\theta(z) \mapsto \theta(az)$ for totally positive a. Thus the action of β: $\theta(\phi_1)|_1\tau^{-1} \mapsto \theta(\phi_1)|_1\tau^{-1}\beta$ in (7.13) preserves the p–integrality (see Theorem 4.9 in [H88a]), and $\theta(\phi_1)|_1\tau^{-1}\beta$ has p–integral q–expansion with respect to the variable w if $\theta(\phi_1)|\tau^{-1}$ is p–integral. Thus we need to prove that $\theta(\phi)|_1\tau^{-1}$ has p–integral q–expansion coefficients, in order to show $\Psi(z, w)$ in (7.13) has p–integral q–expansion. Since $\theta(\phi)|\tau'$ for $\tau' = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is given by $\theta(\widehat{\phi}_1)$ for the Fourier transform $\widehat{\phi}_1$ of ϕ_1 regarding it as a function on $M_{\mathbb{A}}$. The p–integrality only depends on the p–part $\phi_{1,p}$ of ϕ_1. By computation, $\widehat{\phi}_{1,p}$ is $N(\mathfrak{p}^{-e})$ times the characteristic function of $R_{\Sigma_p c} \times \mathfrak{p}^{-e}R_{\Sigma_p}$. Taking ϖ^{-e} in O, we find that $\theta(\phi_1)|\tau^{-1}$ is equal to $\theta(\widehat{\phi}_1)|_1\left(\begin{smallmatrix} 1 & 0 \\ 0 & \varpi^{-e} \end{smallmatrix}\right)(w) = \varpi^e\theta(\widehat{\phi}_1)(\varpi^e w)$ up to a p–adic unit. Since $\varpi^e N(\mathfrak{p}^{-e})$ is a p–adic unit, we get the desired integrality.

By the q–expansion principle, we conclude from (7.6)

$$(7.15)\qquad \frac{(2\pi i)^{2\Sigma} W_p(\lambda^-)(\theta(\lambda; \mathfrak{A}), \theta(\phi_1)\theta(\phi_2))_\Gamma}{\Omega^{2\Sigma}} \in \overline{W}.$$

This shows

$$[\overline{\Gamma}_0(\mathfrak{N}(\lambda);\mathfrak{y}):\overline{\Gamma}]\frac{(2\pi i)^{2\Sigma}W_p(\lambda^-)(\theta(\lambda;\mathfrak{A}),\Theta_{ijz})_{\Gamma_0(\mathfrak{N}(\lambda);\mathfrak{y})}}{\Omega^{2\Sigma}}\in\overline{W}.$$

Write $(\theta(\lambda;\mathfrak{A}),f)_\Gamma$ for the inner product $(\theta(\lambda;\mathfrak{A}),f_\mathfrak{y})$ for the $\mathfrak{y}$–component $f_\mathfrak{y}$ of $f\in S_\kappa(\mathfrak{N},\varepsilon;W)$. Since any $f\in S_\kappa(\mathfrak{N}(\lambda),\varepsilon;\overline{W})$ is a $\overline{W}$–linear combination of Θ_{ijz} by Corollary 6.4, we conclude

$$[\overline{\Gamma}_0(\mathfrak{N}(\lambda);\mathfrak{y}):\overline{\Gamma}]\frac{(2\pi i)^{2\Sigma}W_p(\lambda^-)(\theta(\lambda;\mathfrak{A}),S_\kappa(\mathfrak{N}(\lambda),\varepsilon;\overline{W}))_{\Gamma_0(\mathfrak{N}(\lambda);\mathfrak{y})}}{\Omega^{2\Sigma}}\subset\overline{W}.$$

Since $[\overline{\Gamma}_0(\mathfrak{N}(\lambda);\mathfrak{y}):\overline{\Gamma}]$ is a factor of

$$N_{F/\mathbb{Q}}(\mathfrak{N}')^2\prod_{\mathfrak{l}|\mathfrak{N}'}\left(1-\frac{1}{N_{F/\mathbb{Q}}(\mathfrak{l})^2}\right)$$

for $\mathfrak{N}'=d(M/F)^2\mathfrak{q}^m$, if $p\nmid(N(\mathfrak{l})\pm 1)$ for all primes $\mathfrak{l}|d(M/F)\mathfrak{q}$, we get

$$\text{(7.16)}\qquad \frac{(2\pi i)^{2\Sigma}W_p(\lambda^-)(\theta(\lambda;\mathfrak{A}),S_\kappa(\mathfrak{N}(\lambda),\varepsilon;\overline{W}))_{\Gamma_0(\mathfrak{N}(\lambda);\mathfrak{y})}}{\Omega^{2\Sigma}}\subset\overline{W}.$$

We can choose $\mathfrak{q}$ (by unramifiedness of p in $F/\mathbb{Q}$ and $p\geq 5$) so that

$$p\nmid(N_{M/F}(\mathfrak{q})\pm 1).$$

Thus if $p\nmid(N_{M/F}(\mathfrak{l})\pm 1)$ for all primes $\mathfrak{l}|d(M/F)$, we conclude $H(\varphi)|\frac{h(M)}{h(F)}L^-(\varphi)$ as we explained in the introduction. Here $H(\varphi)$ is the congruence power series with respect to the nearly ordinary Hecke algebra $\mathbf{h}(\mathfrak{N}(\varphi),\varepsilon_\varphi;W)$ interpolating $h_\kappa^{n.ord}(\mathfrak{N}(\lambda),\varepsilon_\lambda;W)$ (for all $\kappa\varepsilon\in\mathcal{A}(\mathbb{I})$). Thus $H(\varphi)$ divides thecongruence power series H in [HT1] but could be smaller if $\mathfrak{C}\cap\mathfrak{C}^c$ contains non-trivial prime factor. In [HT1], we had an extra factor $\Delta(M/F;\mathfrak{C})$ which is equal to the product of the Euler factors of $L(s,\alpha)L(s,\varphi^{-1}\varphi_c)$ for primes outside p in $\mathfrak{C}\cap\mathfrak{C}^c$. This comes from the formula of the inner product of $\theta(\lambda)$ in [HT1] Theorem 7.1. After doing the same computation for $f(\lambda)$ of smaller level instead of $\theta(\lambda)$ and writing $k=\kappa_1-\kappa_2+I$ (see [H05d] (5.5)), we get the exact formula, if λ^- has split conductor:

$$\text{(7.17)}\quad (f(\lambda)^u,f(\lambda)^u)_{\mathfrak{N}(\lambda)} = D\cdot N_{F/\mathbb{Q}}(\mathfrak{N}(\lambda))2^{-2k+1}\pi^{-(k+I)}\Gamma_F(k+I)L(1,Ad(f(\lambda)))$$

under the terminology of [HT1] Section 7 without any error terms. Here $D=N(\mathfrak{d})$ is the discriminant of $F/\mathbb{Q}$.

Here is how to remove the condition: $p\nmid(N_{M/F}(\mathfrak{l})\pm 1)$ for primes $\mathfrak{l}$ in the discriminant $d(M/F)$. The idea is to make quadratic base-change (and then descent). As a target of the base-change, we can find a totally real quadratic extension F'/F unramified at p such that $d(M'/F')$ for the composite $M'=MF'$ does not contain prime factors as above. Then for M'/F', we get the assertion. We later choose F' more carefully so that we can effectively descend back to F again. Let χ be the character $\mathrm{Gal}(F'/F)\cong\{\pm 1\}$ restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$. Suppose that we find a character η of $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ of conductor

$\mathfrak{C}'$ such that $\eta^{c-1} = \chi$.

We can always assume that η is of order prime to p by taking the Teichmüller lift of ($\eta \mod \mathfrak{m}_{\overline{W}}$). Let Γ_M be as in the introduction and we consider the universal character $\widetilde{\varphi} : G(\mathfrak{C}) \to W[[\Gamma_M]]$ with branch character φ. Put Ψ : $\mathrm{Gal}(\overline{F}/F) \to GL_2(\mathbb{I})$ be the induced Galois representation $\mathrm{Ind}_M^F \widetilde{\varphi}$. Then we have

$$Ad(\Psi) \cong \alpha \oplus \mathrm{Ind}_M^F(\widetilde{\psi}) \ \text{ for } \alpha = \left(\frac{M/F}{}\right).$$

Thus

$$Ad(\Psi) \otimes \chi \cong \alpha\chi \oplus \mathrm{Ind}_M^F(\widetilde{\varphi\eta}^{-1}\widetilde{\varphi\eta}_c).$$

By Fujiwara's "$R = T$" theorem [Fu] (actually its $\mathbb{I}$–adic version: [HMI] Theorem 3.59), under the assumption (h1-4), the congruence power series $H(\varphi)$ gives the characteristic power series of the Selmer group

$$\mathrm{Sel}(Ad(\Psi)) = \mathrm{Hom}(Cl^-, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}} \mathbb{I} \oplus \mathrm{Sel}(\psi),$$

where $Cl^- = Cl_M/Cl_F$ for the class groups Cl_M (resp. Cl_F) of M (resp. F).

We need to argue more for the character $\varphi\eta$, because $\varphi\eta$ may not satisfy the condition (h2). We choose F' so that $F'_{\mathfrak{l}} = M_{\mathfrak{l}}$ for all $\mathfrak{l}|2pd(M/F)$ and F'/F ramifies outside $2d(M/F)$ only at primes which split in M/F. This is possible for the following reason: We take an element $\delta \in O$ so that $M = F[\sqrt{\delta}]$. Then we take a high power $\mathfrak{a} = (2pd(M/F))^m$ so that any element $u \in F$ with $u \equiv 1 \mod \mathfrak{a}$ is a square in $F_{\mathfrak{l}}$ for all $\mathfrak{l}|2pd(M/F)$. Then for the infinite set $\Xi = \{\varepsilon \in O | \varepsilon \equiv \delta \mod \mathfrak{a},\ \varepsilon \gg 0\}$, we can find an infinite set of primes $\mathfrak{q} = (\varepsilon\delta^{-1})$ which splits in M/F. Then we define $F' = F[\sqrt{\varepsilon}]$. By our choice, $(\varepsilon) = \mathfrak{q}(\delta)$, and hence if a prime outside $2d(M/F)$ ramifies in F'/F, it has to be $\mathfrak{q}$, which splits in M/F.

We shall show that for the above choice of F', $\varphi\eta$ satisfies (h2). In fact, suppose that $\mathfrak{l}$ remains prime in M/F. Then if $\eta_{\mathfrak{l}}^{c-1} = \chi_{\mathfrak{l}} \neq 1$, then $\chi_{\mathfrak{l}}$ has to ramify, and hence F'/F ramifies at $\mathfrak{l}$. By our choice of F', $\mathfrak{l}$ splits in M/F, a contradiction. If $\mathfrak{l}$ ramifies in M, $\chi_{\mathfrak{l}}$ restricted in $\mathrm{Gal}(\overline{M}_{\mathfrak{l}}/M_{\mathfrak{l}})$ is trivial because $F'_{\mathfrak{l}} = M_{\mathfrak{l}}$. This shows that $\varphi_{\mathfrak{l}}\eta_{\mathfrak{l}}$ is c–invariant, and hence by local class field theory, it is a pull-back of a character of $F_{\mathfrak{l}}^{\times}$ by the norm. Thus $\varphi\eta$ satisfies (h2), and the congruence power series $H(\varphi\eta)$ still gives the exact characteristic power series of $\mathrm{Sel}(Ad(\Psi'))$, where $\Psi' = \mathrm{Ind}_M^F \widetilde{\varphi\eta}$. This is the beauty of taking level $\mathfrak{N}(\varphi)$ (not the deeper level: $N_{M/F}(\mathfrak{C})d(M/F)$ taken in [HT1] and [HT2]). Writing the congruence power series for $\widehat{\varphi} = \varphi \circ N_{M'/M}$ as $H(\widehat{\varphi})$, by the base change (cf. [H00] Proposition 2.4), we have (by $p > 2$),

$$\mathrm{Sel}(Ad(\mathrm{Ind}_{M'}^{F'} \widehat{\varphi})) = \mathrm{Sel}(Ad(\Psi)) \oplus \mathrm{Sel}(Ad(\Psi) \otimes \chi),$$

which implies

$$H(\widehat{\varphi}) = H(\varphi)H(\varphi\eta)\frac{h(M'')}{h(M)},$$

where M'' is the third (and unique) CM quadratic extension of F inside $M' = MF'$.

If $\chi = \eta^{1-c}$ for a Hecke character η of M, $\chi\psi$ is again anti-cyclotomic. We have shown in [H05d] Corollary 5.5:

$$(h(M)/h(F))L^-(\psi)|H(\varphi) \text{ and } (h(M)/h(F))L^-(\psi\eta)|H(\varphi\eta),$$

which is enough to conclude the equality for each (by Nakayama's lemma):

$$(h(M)/h(F))L^-(\psi) = H(\varphi) \text{ and } (h(M)/h(F))L^-(\psi\eta) = H(\varphi\eta)$$

from $(h(M')/h(F'))L^-(\widehat{\psi}) = H(\widehat{\varphi})$ we have already proven.

We now prove the anticyclotomy of χ: $\chi = \eta^{c-1}$. Let $\chi : M_{\mathbb{A}}^\times/M^\times \to \{\pm 1\}$ be the quadratic idele character corresponding to M'/M. We want to have a finite order Hecke character $\eta : M_{\mathbb{A}}^\times \to \mu_{\mathfrak{N}}$ such that $\eta^{c-1} = \chi$, where $\eta^c(x) = \eta(c(x))$ for $x \in M_{\mathbb{A}}^\times$.

Let k be a number field. By class field theory, any continuous character of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ can be regarded as a continuous idele character: $C_k = k_{\mathbb{A}}^\times/k^\times \to \mathbb{T}$, where

$$\mathbb{T} = \left\{z \in \mathbb{C}\big||z| = 1\right\}.$$

A given continuous character of C_k is of finite order if and only if it is trivial on the identity component of the infinite part $k_\infty^\times$ of $k_{\mathbb{A}}^\times$ (cf. [MFG] Proposition 2.2). By Artin reciprocity, any continuous character of C_k trivial on the identity component of $k_\infty^\times \subset k_{\mathbb{A}}^\times$ can be viewed as a (finite order) character of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ canonically.

Looking at the exact sequence:

$$1 \to M^\times \to M_{\mathbb{A}}^\times \to C_M \to 1,$$

by Hilbert's theorem 90 applied to $M^\times$ and $\mathrm{Gal}(M/F) = \langle c \rangle$, we find

$$H^0(\mathrm{Gal}(M/F), C_M) = C_F,$$

and the kernel of $c-1 : x \mapsto x^{c-1}$ is given by C_F. A character $\phi : C_M \to \mathbb{T}$ is of the form $\phi = \eta^{c-1}$ if and only if ϕ is trivial on C_F. Since $\mathrm{Gal}(M'/F) \cong (\mathbb{Z}/2\mathbb{Z})^2$, we find a quadratic character α of C_F such that $\chi = \alpha \circ N_{M/F}$. This shows that $\chi(x) = \alpha(xx^c) = \alpha(x^2) = 1$ for $x \in C_F$. Thus we can write $\chi = \eta^{c-1}$ for a character $\eta : C_M \to \mathbb{T}$.

To have η factor through the Galois group of the maximal abelian extension of M, we need to show that η can be chosen so that its restriction to $M_\infty^\times$ is trivial. Since $\chi = \eta^{c-1}$ is trivial on $M_\infty^\times$, η is trivial on $(M_\infty^\times)^{c-1} = \mathrm{Ker}(N_{M/F} : M_\infty^\times \to F_\infty^\times)$. Thus $\eta|_{M_\infty^\times}$ factors through $N_{M/F} : M_\infty^\times \to F_{\infty+}^\times$. Replacing η by $\eta(\xi \circ N_{M/F})$ for a Hecke character ξ of F, we may assume that η is trivial on $M_\infty^\times$. This finishes the proof for even degree field.

We now assume that F has odd degree. The above trick of taking totally real quadratic extensions F'/F reduces the proof to the even degree case of M'/F'; so, we get the theorem. □

As we have seen that $\psi = \varphi^-$ if and only if ψ is trivial on C_F. If ψ is anticyclotomic, then $\psi(x^c) = \psi(x^{-1})$ ($\Leftrightarrow \psi = 1$ on $N_{M/F}(M_{\mathbb{A}}^{\times})$). Thus $\psi|_{C_F}$ is either the character of M/F or trivial. Since ψ is a Hecke character of $M_{\mathbb{A}}^{\times}$ of finite order, its infinity type is trivial; so, ψ has to be trivial on C_F. This shows

(7.18) If ψ is anticyclotomic, then $\psi = \varphi^-$ for a Hecke character φ of M.

We leave the reader to show that we can take φ to be of finite order (see [HMI] Lemma 5.31).

References

Books

[AAF] G. Shimura, *Arithmeticity in the Theory of Automorphic Forms*, Mathematical Surveys and Monographs 82, AMS, 2000

[ACM] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998

[BAL] N. Bourbaki, *Algèbre*, Hermann, Paris, 1947-59

[BCM] N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961–83

[BNT] A. Weil, *Basic Number Theory*, Springer, 1974

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, 2000, World Scientific Publishing Co., Singapore (a list of errata downloadable at `www.math.ucla.edu/~hida`)

[HMI] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, Oxford University Press, 2006 (a list of errata downloadable at `www.math.ucla.edu/~hida`)

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press and Iwanami Shoten, 1971, Princeton-Tokyo

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST 26, Cambridge University Press, Cambridge, 1993

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge studies in advanced mathematics 69, Cambridge University Press, Cambridge, 2000 (a list of errata downloadable at `www.math.ucla.edu/~hida`)

[PAF] H. Hida, *p–Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics. Springer, New York, 2004 (a list of errata downloadable at `www.math.ucla.edu/~hida`)

Articles

[Ch] C. Chevalley, Deux théorèmes d'arithmétiue, J. Math. Soc. Japan 3 (1951), 35–44

[CW] J. Coates and A. Wiles, Kummer's criterion for Hurwitz numbers. Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), pp. 9–23. Japan Soc. Promotion Sci., Tokyo, 1977

[CW1] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), 223–251

[Fu] K. Fujiwara, Deformation rings and Hecke algebras in totally real case, preprint, 1999 (arXiv.math.NT/0602606)

[H81] H. Hida, On abelian varieties with complex multiplication as factors of the jacobians of Shimura curves, Amer. J. Math. 103 (1981), 727–776

[H86] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. scient. Éc. Norm. Sup. 4-th series 19 (1986), 231–273

[H88a] H. Hida, On p-adic Hecke algebras for GL_2 over totally real fields, Ann. of Math. 128 (1988), 295–384

[H88b] H. Hida, Modules of congruence of Hecke algebras and L-functions associated with cusp forms, Amer. J. Math. 110 (1988), 323–382

[H89] H. Hida, On nearly ordinary Hecke algebras for $GL(2)$ over totally real fields, Advanced Studies in Pure Math. 17 (1989), 139–169

[H91] H. Hida, On p–adic L–functions of $GL(2) \times GL(2)$ over totally real fields, Ann. l'institut Fourier 41 (1991), 311–391

[H94] H. Hida, On the critical values of L–functions of $GL(2)$ and $GL(2) \times GL(2)$, Duke Math. J. 74 (1994), 431–529

[H96] H. Hida, On the search of genuine p–adic modular L–functions for $GL(n)$, Mémoire SMF 67, 1996 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H99] H. Hida, Non-critical values of adjoint L–functions for $SL(2)$, Proc. Symp. Pure Math. 66 Part 1 (1999), 123–175 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H00] H. Hida, Adjoint Selmer group as Iwasawa modules, Israel J. Math. 120 (2000), 361–427 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H02] H. Hida, Control theorems for coherent sheaves on Shimura varieties of PEL–type, Journal of the Inst. of Math. Jussieu, 2002 1, 1–76 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H04] H. Hida, Non-vanishing modulo p of Hecke L–values, in: "*Geometric Aspects of Dwork's Theory, II*" (edited by Alan Adolphson, Francesco Baldassarri, Pierre Berthelot, Nicholas Katz, and Francois Loeser), Walter de Gruyter, 2004, pp. 735–784 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H05a] H. Hida, p–Adic automorphic forms on reductive groups, Astérisque 298 (2005), 147–254 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H05b] H. Hida, The integral basis problem of Eichler, IMRN 34 (2005) 2101–2122 (downloadable at `www.math.ucla.edu/~hida`)

[H05c] H. Hida, The Iwasawa μ–invariant of p–adic Hecke L–functions, preprint, 2004 (preprint downloadable at `www.math.ucla.edu/~hida`)

[H05d] H. Hida, Non-vanishing modulo p of Hecke L–values and application, to appear in the Proceedings of the Durham symposium, 2004 (preprint downloadable at `www.math.ucla.edu/~hida`)

[HT1] H. Hida and J. Tilouine, Anticyclotomic Katz p–adic L–functions and congruence modules, Ann. Sci. Ec. Norm. Sup. 4-th series 26 (1993), 189–259

[HT2] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fields, Inventiones Math. 117 (1994), 89–147

[MT] B. Mazur and J. Tilouine, Représentations Galoisiennes, différentielles de Kähler et "conjectures principales", Publ. IHES 71 (1990), 65–103

[K] N. M. Katz, p-adic L-functions for CM fields, Inventiones Math. 49 (1978), 199–297

[O] M. Ohta, Congruence modules related to Eisenstein series, Ann. Éc. Norm. Sup. 4-th series 36 (2003), 225–269

[R] K. Rubin, On the main conjecture of Iwasawa theory for imaginary quadratic fields. Invent. Math. 93 (1988), 701–713

[R1] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Inventiones Math. 103 (1991), 25–68

[ST] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. 88 (1968), 452–517

[Sh1] G. Shimura, The arithmetic of certain zeta functions and automorphic forms on orthogonal groups, Ann. of Math. 111 (1980), 313–375

[Sh2] G. Shimura, On certain zeta functions attached to two Hilbert modular forms: I. The case of Hecke characters, II. The case of automorphic forms on a quaternion algebra, I: Ann. of Math. 114 (1981), 127–164; II: ibid. 569–607

[TW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke modules, Ann. of Math. 141 (1995), 553–572

[Ti] J. Tilouine, Sur la conjecture principale anticyclotomique, Duke. Math. J. 59 (1989), 629–673

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. 141 (1995), 443–551

Haruzo Hida
Department of Mathematics
UCLA
Los Angeles CA 90095-1555
USA
hida@math.ucla.edu

Optimal Levels for Modular Mod 2 Representations over Totally Real Fields

Frazer Jarvis

Received: August 30, 2005
Revised: January 26, 2006

Abstract. In this paper, we study the level lowering problem for mod 2 representations of the absolute Galois group of a totally real field F. In the case $F = \mathbb{Q}$, this was done by Buzzard; here, we generalise some of Buzzard's results to higher weight and arbitrary totally real fields, using Rajaei's generalisation of Ribet's theorem and previous work of Fujiwara and the author.

2000 Mathematics Subject Classification: 11F33, 11F41, 11G18, 14G35
Keywords and Phrases: Hilbert modular forms, totally real fields, Galois representations

The main theorem of this paper is the following result, which reduces level lowering for the prime $\ell = 2$ for totally real fields to a multiplicity one hypothesis, thus showing that multiplicity one is the only obstruction to level lowering in characteristic 2.

Theorem 0.1 *Let* F *be a totally real number field. Let*

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

be a continuous irreducible representation such that $\overline{\rho}$ is not induced from a character of $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}(i))$. *Let $\mathfrak{n}(\overline{\rho})$ denote the Artin conductor away from 2 of $\overline{\rho}$. Suppose that there is some Hilbert cuspidal eigenform of arithmetic weight k and level $U_1(\mathfrak{n})$ that gives rise to $\overline{\rho}$, where $(2, \mathfrak{n}) = 1$. Suppose also that $\overline{\rho}$ satisfies a certain multiplicity one hypothesis (see Definition 6.1). Then there is a Hilbert cuspidal eigenform of weight k and level $U_1(\mathfrak{n}(\overline{\rho}))$ that gives rise to $\overline{\rho}$.*

We note that it is part of the hypothesis that $\overline{\rho}$ occurs at some level prime to 2. This will not be true in general, but it makes for a comparatively clean statement, and the reader will easily be able to extend the statement if needed. The question of possible level structures at 2 is more naturally considered in the context of optimising the weight, we shall not address this problem here; this is the subject of work in progress with Kevin Buzzard and Fred Diamond. We remark (as Fujiwara [11] also explains) that the methods in this paper show that if ℓ is odd, the same result holds for characteristic ℓ representations without the multiplicity one hypothesis. We have:

Theorem 0.2 *Let ℓ be an odd prime. Let*

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

be a continuous irreducible representation. If $[\mathrm{F}(\mu_\ell) : \mathrm{F}] = 2$, suppose that $\overline{\rho}$ is not induced from a character of $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}(\mu_\ell))$. Let $\mathfrak{n}(\overline{\rho})$ denote the Artin conductor away from ℓ of $\overline{\rho}$. Suppose that there is some Hilbert cuspidal eigenform of arithmetic weight k and level $U_1(\mathfrak{n}\mathfrak{p}^r)$ that gives rise to $\overline{\rho}$. If $r > v_\mathfrak{p}(\mathfrak{n}(\overline{\rho}))$, then there is a Hilbert cuspidal eigenform of weight k and level $U_1(\mathfrak{n}\mathfrak{p}^{r-1})$ that gives rise to $\overline{\rho}$.

This result has no multiplicity one hypothesis, and also allows us to lower the level if ℓ and $\mathfrak{n}$ are not coprime, so as to lower the level by all primes not dividing the characteristic. We recall that Fujiwara's work remains unpublished, but alternative references are available for all but his version of Mazur's Principle when $[\mathrm{F} : \mathbb{Q}]$ is even. In particular, when $[\mathrm{F} : \mathbb{Q}]$ is odd, this theorem does not depend on Fujiwara's unpublished work.

We will concentrate on the case $\ell = 2$, as Theorem 0.2 is an easy corollary of previous results of Fujiwara ([11]) and Rajaei ([18]). However, the case $\ell = 2$ requires additional work, and combines Rajaei's results with ideas of Buzzard ([3]), which in turn are based on work of Ribet, for the case $\mathrm{F} = \mathbb{Q}$.

1 Notation

Our notation completely follows [15], and we summarise it next. Throughout this paper, F will denote a totally real number field of degree d over $\mathbb{Q}$. Let $I = \{\tau_1, \ldots, \tau_d\}$ denote the set of embeddings $\mathrm{F} \hookrightarrow \mathbb{R}$. If $\mathfrak{p}$ is a prime of F, then we will denote the local ring at $\mathfrak{p}$ by $\mathcal{O}_\mathfrak{p}$ and its residue field by $\kappa_\mathfrak{p}$. We will be considering continuous semisimple representations

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2),$$

and we study such representations which are associated to Hilbert modular forms.

The *weight* of a Hilbert modular form will be a d-tuple of integers, $k \in \mathbb{Z}^I$, so that there is one component for each infinite place of F.

Definition 1.1 We say that k is *arithmetic* if $k_\tau \geq 2$ for all $\tau \in I$, and further, if all k_τ have the same parity.

Throughout this paper, weights will always be supposed arithmetic.
Given a weight k, we define a d-tuple $v \in \mathbb{Z}^I_{\geq 0}$ so that $k + 2v$ is *parallel* (i.e., $k_\tau + 2v_\tau$ is independent of τ), and some $v_\tau = 0$. We also write $t = (1, \ldots, 1)$, so that $k + 2v$ is a multiple of t. The transformation law for Hilbert modular forms is normalised by choosing a vector $w = k + v - \alpha.t$ for some integer α, and we choose $\alpha = 1$ (as in [12]). If $x \in \mathbb{Z}^I$ is parallel, we write $x = [x]t$ so $[x] \in \mathbb{Z}$.
If G denotes the algebraic group $\mathrm{Res}_{\mathrm{F}/\mathbb{Q}}(\mathrm{GL}_2)$ with centre Z, then the *level* of a Hilbert modular form is an open compact subgroup U of $G(\mathbb{A}^\infty)$, where $\mathbb{A}^\infty$ denotes the finite adeles of $\mathbb{Q}$. In this paper, we will only ever consider subgroups U of the form $U = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$, where $U_{\mathfrak{p}}$ is an open compact subgroup of $\mathrm{GL}_2(\mathrm{F}_{\mathfrak{p}})$. The (finite-dimensional complex) vector space of Hilbert cusp forms of weight k and level U will be denoted $S_k(U)$ (see [12], (2.3), for the precise definition of this space, where it is denoted $S_{k,w,I}(U;\mathbb{C})$; in [15], it is denoted $S_{k,w}(U)$).
Suppose B is a quaternion algebra over F and let $S(B)$ denote the set of finite places ramifying in B. If S is any finite set of finite places of F containing $S(B)$, we define the Hecke algebra $\mathbb{T}^{S,B}$ as the $\mathbb{Z}$-algebra generated by all the Hecke operators $T_{\mathfrak{q}}$ with $\mathfrak{q} \notin S(B)$, and the operators $S_{\mathfrak{q}}$ for $\mathfrak{q} \notin S$. If U is as above, and S contains all finite places at which $U_{\mathfrak{q}}$ is not maximal compact, then $\mathbb{T}^{S,B}$ acts on $S_k(U)$ through a quotient which we denote $\mathbb{T}^{S,B}_k(U)$. If $B = \mathrm{GL}_2$, we will omit it from the notation. If S consists precisely of $S(B)$ together with the places $\mathfrak{q}$ such that $U_{\mathfrak{q}}$ is not maximal compact in $(\mathcal{O}_B \otimes \mathcal{O}_{\mathfrak{q}})^\times \cong \mathrm{GL}_2(\mathcal{O}_{\mathfrak{q}})$, then we will omit it from the notation.

2 Preliminaries

Carayol ([5]) and Taylor ([19]) have proven that to any Hilbert cuspidal eigenform, one may attach a compatible system of global Galois representations compatible with the local Langlands correspondence. For a statement, see [19] or [15].
This result leads us to examine analogues of the Serre conjectures for Galois representations over totally real fields.

Definition 2.1 Given an irreducible modulo ℓ representation,

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell),$$

we say that $\overline{\rho}$ is *modular of level U and weight k* if there exists a Hilbert cuspidal eigenform $f \in S_k(U)$ and a prime $\lambda | \ell$ of $\mathcal{O}_f$ (the ring of integers of the number field generated by the Hecke eigenvalues) such that $\overline{\rho}$ is isomorphic to the reduction of $\rho_{f,\lambda}$ mod λ. As we will primarily be interested in the case $U = U_1(\mathfrak{n})$, we will simply say that $\overline{\rho}$ is *modular of level* $\mathfrak{n}$ if it is modular of level $U_1(\mathfrak{n})$.

(Note that we only consider here Hilbert modular forms coming from characteristic zero, and do not think about mod ℓ forms in the sense of Katz.)
In general, a modular $\overline{\rho}$ may have many different weights and levels, even when we insist that f is a newform (i.e., does not occur at a lower level). We are interested in this paper in the smallest possible levels that may arise.
We define an "optimal" level as in [15]. Given $\overline{\rho}$, define

$$\mathfrak{n}(\overline{\rho}) = \text{the Artin conductor (away from } \ell\text{) of } \overline{\rho}.$$

Note that $\mathfrak{n}(\overline{\rho})$ is prime to ℓ. It is not true that if $\overline{\rho}$ is modular, then it is modular of level $\mathfrak{n}(\overline{\rho})$ (one can see that one cannot always remove primes dividing the characteristic simply by looking at det $\overline{\rho}$). To get a clean statement, however, we will be assuming that our representation is modular at a level prime to ℓ, and try to remove primes not dividing the characteristic. The reader will be able to adapt the statement to more general situations if required.
Let $\mathfrak{p} \nmid \ell$ be prime. For any ℓ-adic character χ of $D_{\mathfrak{p}}$, the decomposition group at $\mathfrak{p}$, let $\overline{\chi}$ denote the reduction modulo ℓ, and let $a(\chi)$ denote the $\mathfrak{p}$-adic valuation of the conductor. In [15], one finds the following generalisation of a result of Carayol ([6]) and Livné ([17]).

Theorem 2.2 *Suppose π is an automorphic representation of $\mathrm{GL}_{2/\mathrm{F}}$ giving rise to $\overline{\rho}$. If π has conductor $\mathfrak{n}$, write $n_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{n})$. Write $\overline{n}_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{n}(\overline{\rho}))$. Then one always has $\overline{n}_{\mathfrak{p}} \leq n_{\mathfrak{p}}$ (so $\mathfrak{n}(\overline{\rho})|\mathfrak{n}$), and one has equality except possibly in the following cases:*

1. *$\pi_{\mathfrak{p}}$ is special, associated to a character χ of $\mathrm{F}_{\mathfrak{p}}^{\times}$ which is unramified.*

2. *$\pi_{\mathfrak{p}}$ is special, associated to a character χ of $\mathrm{F}_{\mathfrak{p}}^{\times}$ which degenerates, in that $a(\chi) = 1$ and $a(\overline{\chi}) = 0$.*

3. *$\pi_{\mathfrak{p}}$ is principal series, associated to two characters χ and ψ of $\mathrm{F}_{\mathfrak{p}}^{\times}$, with at least one of the characters degenerating.*

4. *$\pi_{\mathfrak{p}}$ is a supercuspidal Weil representation, associated to a character of $\Omega^{\times}$ which degenerates, where Ω is the unramified quadratic extension of $\mathrm{F}_{\mathfrak{p}}$.*

For a character of $\mathrm{F}_{\mathfrak{p}}^{\times}$ to degenerate, we require that $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \pmod{\ell}$, and for a character of $\Omega^{\times}$ to degenerate, we require that $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{p}) \equiv -1 \pmod{\ell}$.

Conjecture 2.3 Suppose that $\overline{\rho}$ is modular of weight k and level $U_1(\mathfrak{n})$ with $(\mathfrak{n}, \ell) = 1$. If $v_{\mathfrak{p}}(\mathfrak{n}) > v_{\mathfrak{p}}(\mathfrak{n}(\overline{\rho}))$ and $\mathfrak{p} \nmid \ell$, then it is modular of weight k and level $U_1(\mathfrak{n}/\mathfrak{p})$.

As usual, the method is to remove one prime at a time from the level. The theorem above classifies the primes which may occur.

Remark 2.4 We first remark that cases (2)–(4) of the classification above (Theorem 2.2) will be treated with the existing methods, once we have a good notion of auxiliary prime. Indeed, [15] treats cases (2) and (4), and [11] also treats (3) (as well as doing (2) and (4) independently). One readily verifies that all proofs continue to hold in the case of mod 2 representations, as long as auxiliary primes are available. We will explain later that Buzzard's construction of auxiliary primes generalises to the totally real case.

Remark 2.5 We also point out for later use that the proof of "Mazur's Principle" (the case $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{p}) \not\equiv 1 \pmod{\ell}$ of case (1)) given in [14] for $[\mathrm{F} : \mathbb{Q}]$ odd, and [11] for $[\mathrm{F} : \mathbb{Q}]$ even, is valid more generally when $\overline{\rho}(\mathsf{Frob}_\mathfrak{p})$ is not a scalar (see [14], Corollary 18.8, and [11], end of §5). As the ratio of the diagonal entries of $\overline{\rho}(\mathsf{Frob}_\mathfrak{p})$ is equal to $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{p})$, this is implied by the congruence condition; however, we will later need the stronger version—after all, the congruence condition will never be satisfied when $\ell = 2$. The condition that ℓ be odd was imposed in [14] and [11] only in order that auxiliary primes should exist; as in the previous remark, our generalisation of Buzzard's construction of auxiliary primes then implies some cases of Mazur's Principle even when $\ell = 2$.

3 Characters and Carayol's Lemma

One of the crucial technical tricks used in the theory of level lowering is a result known as Carayol's Lemma (after [6]). The version we want to use was proven in [15].

Roughly, Carayol's Lemma allows us to show that if a mod ℓ representation $\overline{\rho}$ is modular, associated to some modular form with character ϕ, then given any character $\psi \equiv \phi \pmod{\ell}$, there is some modular form with character ψ which gives rise to the given mod ℓ representation. In other words, whether or not there is a modular form of given character giving rise to $\overline{\rho}$ depends only on the character modulo ℓ.

In [15], we proved the following (for additional notation, as well as a more general statement, see [15]):

Theorem 3.1 (Carayol's Lemma) *Let ℓ be an odd prime. Suppose that S is a finite set of places of* F *containing all infinite places of* F*. Let k be arithmetic, and let U and U' be S-subgroups with U' normal in U. Suppose r (resp. χ) is an irreducible representation (resp. a character with ℓ-power order) of $U/U'(U \cap Z(\mathbb{Q}))$. Let $\overline{\theta} : \mathbb{T}_k^S(U, r) \longrightarrow \overline{\mathbb{F}}_\ell$ be a homomorphism for which $\overline{\rho} = \overline{\rho}_{\overline{\theta}}$ is irreducible. If $[\mathrm{F}(\mu_\ell) : \mathrm{F}] = 2$, suppose that $\overline{\rho}$ is not induced from a character of the kernel of the mod ℓ cyclotomic character. Then there exists a homomorphism $\overline{\theta}' : \mathbb{T}_k^S(U, r \otimes \chi) \longrightarrow \overline{\mathbb{F}}_\ell$ such that the two maps $\mathbb{T}^S \longrightarrow \overline{\mathbb{F}}_\ell$ induced by $\overline{\theta}$ and $\overline{\theta}'$ coincide.*

The additional hypothesis when $[\mathrm{F}(\mu_\ell) : \mathrm{F}] = 2$ was not explicitly stated in [15], as it was a running hypothesis throughout the paper. (The author apologises if this has caused any confusion.) This hypothesis on ℓ, as well as the stipulation that ℓ be odd, was only invoked to allow us to introduce an auxiliary prime (see next section) so that U—and therefore U'—may be assumed *sufficiently small* in the sense of Carayol ([4], 1.4.1.1, 1.4.1.2). However, as a corollary of the proof, we can omit this hypothesis, and still deduce the same result (even for $\ell = 2$), so long as U is sufficiently small.

Corollary 3.2 *Suppose the notation and hypotheses are as above, except that we replace the hypotheses on ℓ by the hypothesis that U is sufficiently small. Then Carayol's Lemma is again true.*

4 Auxiliary primes

A crucial trick that we will use is to alter the level by making it sufficiently small, and then return to the original level. This trick originated in [8] and [9] and easily generalises to totally real fields; the case of mod 2 representations was treated in [3].

Let G be a finite group. Suppose that

$$\overline{\rho} : G \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

is an irreducible continuous representation and let

$$\chi : G \longrightarrow \{\pm 1\}$$

be a surjective character.

In our applications, $\overline{\rho}$ will be the given Galois representation. We will let χ be the mod 4 cyclotomic character giving the action of $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})$ on the fourth roots of unity. As F is totally real, its absolute Galois group contains complex conjugation elements, so this mod 4 cyclotomic character is non-trivial, and hence maps surjectively onto $\{\pm 1\}$. As $\overline{\rho}$ is continuous, it factors through a finite group; we let G be a finite group through which $\overline{\rho} \oplus \chi$ factors.

We say that $g \in G$ is *special* if $\mathrm{tr}\,\overline{\rho}(g) = 0$.

We will need the following lemma.

Lemma 4.1 *Suppose that $\overline{\rho}$ is not induced from a character of $\ker \chi$. Then there exists $g \in G$ which is not in $\ker \chi$ and which is not special.*

Proof. See [3]. □

When χ is the mod 4 cyclotomic character, its kernel is precisely $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}(i))$.

We now apply this lemma to construct "auxiliary" primes. From the lemma, we see that if

$$\overline{\rho} : G \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

is an irreducible mod 2 representation, then there exists an element $g \in G$ such that $\chi(g) = -1$ and $\mathrm{tr}\,\overline{\rho}(g) \neq 0$. If χ is the mod 4 cyclotomic character, and $g \in G$ is the image of $\mathsf{Frob}_{\mathfrak{q}}$, then $\chi(g) = -1$ is equivalent to $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{q}) \equiv 3 \pmod 4$.

Lemma 4.2 *Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_{\mathrm{F}}$ with $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{q}) \equiv 3$ (mod 4). Suppose that E is a finite extension of $\mathbb{Q}_2$ and that*

$$\psi : (\mathcal{O}_{\mathrm{F}}/\mathfrak{q})^{\times} \longrightarrow \mathcal{O}_E^{\times}$$

is a character with trivial reduction. If $\psi(-1) = 1$, then ψ is trivial.

Proof. As ψ has trivial reduction, it is valued in $\ker(\mathcal{O}_E^{\times} \longrightarrow k_E^{\times})$, where k_E denotes the residue field of $\mathcal{O}_E$. It is easy to see (using Hensel's lemma, for example) that the only torsion in this kernel is killed by a power of 2. But

$$|(\mathcal{O}_{\mathrm{F}}/\mathfrak{q})^{\times}| = N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{q}) - 1 \equiv 2 \text{ (mod 4)}.$$

It follows that ψ is valued in $\{\pm 1\}$. If also $\psi(-1) = 1$, then the 2-torsion of $(\mathcal{O}_{\mathrm{F}}/\mathfrak{q})^{\times}$ is killed by ψ, so ψ must be trivial. □

The following result generalises Corollary 2.6 of [3] to totally real fields.

Theorem 4.3 *Suppose that $\overline{\rho}$ is an irreducible continuous mod 2 representation not induced from a character of $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}(i))$. Then there exists a prime $\mathfrak{r}$ with the property that if $\overline{\rho}$ is associated to a cuspidal eigenform f of weight k and level $U_1(\mathfrak{n}) \cap U_1^1(\mathfrak{r})$ for some $\mathfrak{n}$ prime to $\mathfrak{r}$, then there is a cuspidal eigenform g of weight k and level $U_1(\mathfrak{n})$ which also gives rise to $\overline{\rho}$.*

Proof. For this, we apply Carayol's Lemma and the lemmas above. Let G be a finite group through which $\overline{\rho} \oplus \chi$ factors. By the hypotheses above on $\overline{\rho}$, we can find an element $g \in G$ which is neither in $\ker \chi$, nor is special. Let $\mathfrak{r}$ be any prime such that $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{r}) > 4^d$ which is unramified for $\overline{\rho}$ such that $\mathsf{Frob}_{\mathfrak{r}}$ maps to g. Then

- $\chi(\mathsf{Frob}_{\mathfrak{r}}) = -1$, i.e., $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{r}) \equiv 3$ (mod 4), and
- $\mathrm{tr}\,\overline{\rho}(\mathsf{Frob}_{\mathfrak{r}}) \neq 0$.

As $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{r}) > 4^d$, the group $U_1^1(\mathfrak{r})$ is sufficiently small ([14], §12) so that we may apply Corollary 3.2. We may regard f as an eigenform on $U_0(\mathfrak{n}\mathfrak{r})$ with character $\chi = \chi_{\mathfrak{n}}\chi_{\mathfrak{r}}$ of the abelian group $U_0(\mathfrak{n})/U_1(\mathfrak{n}) \times U_0(\mathfrak{r})/U_1^1(\mathfrak{r})$. We apply Corollary 3.2 with $U = U_0(\mathfrak{n}) \cap U_1^1(\mathfrak{r})$ and $U' = U_1(\mathfrak{n}) \cap U_1^1(\mathfrak{r})$ to see that there is a cuspidal eigenform f' on $U_1(\mathfrak{n}) \cap U_1^1(\mathfrak{r})$ with character $\chi' = \chi'_{\mathfrak{n}}\chi'_{\mathfrak{r}}$ which is congruent to f and such that $\chi'_{\mathfrak{n}}(-1) = (-1)^{[k+2v]}$.

However, one knows that $\chi'(-1) = (-1)^{[k+2v]}$, so that $\chi'_{\mathfrak{r}}(-1) = 1$. As $\overline{\rho}$ is unramified at $\mathfrak{r}$, the reduction of $\chi'_{\mathfrak{r}}$ is trivial. By Lemma 4.2, $\chi'_{\mathfrak{r}}$ itself is trivial. It follows that f' is actually a cuspidal eigenform on $U_1(\mathfrak{n}) \cap U_0(\mathfrak{r})$. This implies that the component at $\mathfrak{r}$ of the automorphic representation corresponding to f' is either unramified principal series or is special unramified. The latter is ruled out as then we would have $\mathrm{tr}\,\overline{\rho}(\mathsf{Frob}_{\mathfrak{r}}) = 0$. Thus f' is old at $\mathfrak{r}$, and we may choose an eigenform g for level $U_1(\mathfrak{n})$ with the same Hecke eigenvalues as those for f' except possibly at $\mathfrak{r}$. The result follows. □

5 Shimura curves

In this section, we summarise results (in §5.2) of [14] on integral models and their reductions in characteristic p of Shimura curves whose level structure involves primes dividing p, but where such primes do not ramify in the quaternion algebra, and the relevant results (in §5.3) of Boutot-Zink ([2]) and Varshavsky ([20], [21]) on integral models and their reductions in characteristic p of Shimura curves whose level structure does not involve primes dividing p, but where such primes do ramify in the quaternion algebra. These results also appear in [18]; this section is as much to fix notation as it is to remind the reader of previous results.

5.1 Formalism of vanishing cycles

Here we summarise the theory of vanishing cycles from SGA 7, XIII, XV. For a beautiful introduction to the theory, see also [18].

Let V be a mixed characteristic henselian discrete valuation ring with fraction field K and residue field k of characteristic p. If $\mathcal{C}$ is a proper generically smooth curve over $S = \operatorname{spec} V$ with semistable reduction, and $\mathcal{F}$ is a constructible sheaf on $\mathcal{C}$ with torsion prime to p, then we have the following exact sequence:

$$\begin{aligned} 0 \longrightarrow H^1(\mathcal{C}\otimes\overline{k},\mathcal{F}) \longrightarrow H^1(\mathcal{C}\otimes\overline{K},\mathcal{F}) \xrightarrow{\beta} H^1(\mathcal{C}\otimes\overline{k},R\Phi\mathcal{F}) \\ \longrightarrow H^2(\mathcal{C}\otimes\overline{k},\mathcal{F}) \longrightarrow H^2(\mathcal{C}\otimes\overline{K},\mathcal{F}) \longrightarrow 0 \end{aligned}$$

where $R\Phi\mathcal{F}$ is a complex of sheaves supported on the singular points Σ of the special fibre, and $R^i\Phi\mathcal{F} \neq 0$ only when $i = 1$. In particular,

$$H^1(\mathcal{C}\otimes\overline{k},R\Phi\mathcal{F}) = \bigoplus_{x\in\Sigma}(R^1\Phi\mathcal{F})_x.$$

Furthermore, we have a complete understanding of the sheaf $R^1\Phi\mathcal{F}$ coming from the Picard-Lefschetz formula. We define

$$X(\mathcal{C},\mathcal{F}) = \operatorname{im}(\beta)(1)$$

where the (1) denotes the Tate twist.

The cohomology $H^1(\mathcal{C}\otimes\overline{K},\mathcal{F})$ may be computed by means of another complex $R\Psi\mathcal{F}$ of sheaves on $\mathcal{C}\otimes\overline{k}$.

There is a trace pairing in this situation; Illusie ([13]) has explained that this induces a second exact sequence, dual to the first:

$$\begin{aligned} 0 \longrightarrow H^0(\widehat{\mathcal{C}\otimes\overline{k}},R\Psi\mathcal{F}) \longrightarrow H^0(\widehat{\mathcal{C}\otimes\overline{k}},\mathcal{F}) \longrightarrow \bigoplus_{x\in\Sigma} H^1_x(\mathcal{C}\otimes\overline{k},R\Psi\mathcal{F}) \\ \xrightarrow{\beta'} H^1(\mathcal{C}\otimes\overline{K},\mathcal{F}) \longrightarrow H^1(\mathcal{C}\otimes\overline{k},\mathcal{F}) \longrightarrow 0, \end{aligned}$$

where $\widehat{\mathcal{C}\otimes\overline{k}}$ denotes the normalisation of the special fibre of $\mathcal{C}$. We set

$$\widehat{X}(\mathcal{C},\mathcal{F}) = \mathrm{im}(\beta').$$

Rajaei ([18], prop.1) points out that $\widehat{X}(\mathcal{C},\mathcal{F})$ actually lies inside $H^1(\mathcal{C}\otimes\overline{k},\mathcal{F})$, regarded a subspace of $H^1(\mathcal{C}\otimes\overline{K},\mathcal{F})$ by the first exact sequence. The first exact sequence is called the *specialisation exact sequence* and the second is called the *cospecialisation exact sequence.*
Deligne defines a *variation map*

$$\mathrm{Var}(\sigma)_x : (R^1\Phi\mathcal{F})_x \longrightarrow H^1_x(\mathcal{C}\otimes\overline{k},\mathcal{F})$$

for $\sigma \in I_K$, the inertia group of $\mathrm{Gal}(\overline{K}/K)$. The action of $\sigma \in I_K$ on both exact sequences may be expressed using this map; for example, the action of σ on $H^1(\mathcal{C}\otimes\overline{K},\mathcal{F})$ is given by $\mathrm{id} + (\beta' \circ \bigoplus_{x\in\Sigma}\mathrm{Var}(\sigma)_x \circ \beta)$. From the form of the variation map, one may define a canonical *monodromy logarithm*

$$N_x : (R^1\Phi\mathcal{F})_x(1) \longrightarrow H^1_x(\mathcal{C}\otimes\overline{k},\mathcal{F}).$$

Rajaei explains that this monodromy map induces an injective map $\lambda : X(\mathcal{C},\mathcal{F}) \longrightarrow \widehat{X}(\mathcal{C},\mathcal{F})$; we write $\Phi(\mathcal{C},\mathcal{F}) = \mathrm{coker}\,\lambda$, and call it the *component group* (by analogy with Jacobians).
We end this survey with an alternative, more concrete, description of $\widehat{X}(\mathcal{C},\mathcal{F})$. Let

$$r : \widehat{\mathcal{C}\otimes\overline{k}} \longrightarrow \mathcal{C}\otimes\overline{k}$$

denote the normalisation map. Then we define the sheaf $\mathcal{G}$ by

$$0 \longrightarrow \mathcal{F} \longrightarrow r_*r^*\mathcal{F} \longrightarrow \mathcal{G} \longrightarrow 0;$$

as in [14], §17, or [18], §1.3, we may also write

$$\widehat{X}(\mathcal{C},\mathcal{F}) = \mathrm{im}(H^0(\mathcal{C}\otimes\overline{k},\mathcal{G}) \longrightarrow H^1(\mathcal{C}\otimes\overline{k},\mathcal{F})).$$

5.2 Integral models of Shimura curves: the split case

Next, we fix a quaternion algebra B over F, and suppose that $\mathfrak{p}$ is a finite prime of F at which B is split. We will suppose that B is split at the infinite place τ_1 and ramified at the other infinite places of F. At each split place v, we fix an isomorphism $B(\mathrm{F}_v) \cong M_2(\mathrm{F}_v)$, and if v is a finite place, we even fix $B(\mathcal{O}_v) \cong M_2(\mathcal{O}_v)$. We regard F as a subfield of $\mathbb{C}$ via τ_1. In the usual way, we let $G = \mathrm{Res}_{\mathrm{F}/\mathbb{Q}}(B^\times)$, and if U is an open compact subgroup of $G(\mathbb{A}^\infty)$, we may form a Shimura curve M_U, defined over F, whose complex points are

$$G(\mathbb{Q})\backslash G(\mathbb{A}^\infty) \times X/U,$$

where $X = \mathfrak{h}^\pm = \mathbb{C} - \mathbb{R}$ is two copies of the upper-half complex plane.

Now we suppose that $U = U_0(\mathfrak{p}) \times H$, as in [14]. Thus U, the level, has a component $U_0(\mathfrak{p}) \subset \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$ at $\mathfrak{p}$, and a level $H \subset \prod_{v \neq \mathfrak{p}}(B \times \mathrm{F}_v)^\times$ away from $\mathfrak{p}$. Write $\Gamma = \prod_{v \neq \mathfrak{p}}(B \times \mathrm{F}_v)^\times$. Here,

$$U_0(\mathfrak{p}) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \middle| c \in \mathfrak{p} \right\},$$

using the above identification. We suppose that H is sufficiently small in the sense of Carayol ([4], 1.4.1.1 and 1.4.1.2). When the level structure at $\mathfrak{p}$ is maximal compact, then Carayol ([4]) proved that the Shimura curve has an integral model $\mathbf{M}_{0,H}$ over $\operatorname{spec} \mathcal{O}_{(\mathfrak{p})}$ with good reduction (i.e., is proper and smooth).

Then in [14], we proved the following:

Theorem 5.1 *1. If H is sufficiently small (as above), then there exists a regular model $\mathbf{M}_{U_0(\mathfrak{p}),H}$ over $\operatorname{spec} \mathcal{O}_{(\mathfrak{p})}$ of M_U.*

2. The special fibre $\mathbf{M}_{U_0(\mathfrak{p}),H} \times \overline{\kappa}_{\mathfrak{p}}$ looks like two copies of $\mathbf{M}_{0,H} \times \overline{\kappa}_{\mathfrak{p}}$ intersecting transversely above a finite set of points Σ_H.

The set of points Σ_H are the *supersingular points* of $\mathbf{M}_{0,H} \times \overline{\kappa}_{\mathfrak{p}}$, and we use the same notation Σ_H for the points which lie above them in $\mathbf{M}_{U_0(\mathfrak{p}),H} \times \overline{\kappa}_{\mathfrak{p}}$, the singular points of the special fibre. Carayol ([4], §11) describes Σ_H as follows: Let $\overline{B}(\mathfrak{p})$ denote the quaternion algebra got from B by changing the invariants at $\mathfrak{p}$ and at τ_1 (so it is now ramified at both these places, and is totally definite). We write $\overline{B} = \overline{B}(\mathfrak{p})$. Let $\overline{G}$ denote the algebraic group $\mathrm{Res}_{\mathrm{F}/\mathbb{Q}}\overline{B}^\times$, and fix, for all places $v \neq \mathfrak{p}, \tau_1$, an isomorphism between $B \otimes \mathrm{F}_v$ and $\overline{B} \otimes \mathrm{F}_v$. Then $\overline{G}(\mathbb{A}^\infty)$ may be identified with $\Gamma \times \overline{B}_{\mathfrak{p}}^\times$. By [4], 11.2(3), there is a bijection

$$\begin{array}{rcl} \Sigma_H & \cong & \overline{G}(\mathbb{Q}) \backslash \overline{G}(\mathbb{A}^\infty)/H \times \mathcal{O}_{\overline{B}_{\mathfrak{p}}}^\times \\ & \cong & \overline{G}(\mathbb{Q}) \backslash \Gamma \times \mathrm{F}_{\mathfrak{p}}^\times / H \times \mathcal{O}_{\mathfrak{p}}^\times \end{array}$$

where the second isomorphism is induced by the reduced norm $\overline{B}_{\mathfrak{p}}^\times \longrightarrow \mathrm{F}_{\mathfrak{p}}^\times$.

5.3 Integral models of Shimura curves: the ramified case

Again, we consider a quaternion algebra B over F, and again suppose that B is split at the infinite place τ_1 and ramified at the other infinite places of F. This time, however, we suppose that $\mathfrak{p}$ is a finite prime of F at which B is ramified. Fix isomorphisms at split places in the same way as in the previous subsection. Again, if U is an open compact subgroup of $G(\mathbb{A}^\infty)$, we may form a Shimura curve M_U, defined over F.

Now we suppose that the level structure may be written $U = K_{\mathfrak{p}} \times H$, where $K_{\mathfrak{p}} = \mathcal{O}_{B,\mathfrak{p}}^\times$. In this case (and more generally), the integral models were studied by Boutot-Zink ([2]) and by Varshavsky ([20], [21]). Their methods generalise the case $\mathrm{F} = \mathbb{Q}$ due to Drinfeld and Čerednik respectively. As in the case $\mathrm{F} = \mathbb{Q}$, the results of Boutot and Zink apply for more general level structures. Again, the main result depends on defining another quaternion algebra $\overline{B}(\mathfrak{p})$, whose invariants are the same as B, except with the invariants at $\mathfrak{p}$ and τ_1 changed. So $\overline{B} = \overline{B}(\mathfrak{p})$ is now split at $\mathfrak{p}$, and is totally definite. We define the algebraic group $\overline{G}$ in the usual way, and fix isomorphisms between B and $\overline{B}$ everywhere except at $\mathfrak{p}$ and at τ_1.

Let $\overline{H}$ denote the subgroup of $(\overline{B} \otimes \mathbb{A}_{\mathrm{F}}^{\infty,\mathfrak{p}})^\times$ corresponding to H under the isomorphism

$$(\overline{B} \otimes \mathbb{A}_{\mathrm{F}}^{\infty,\mathfrak{p}})^\times \xrightarrow{\sim} (B \otimes \mathbb{A}_{\mathrm{F}}^{\infty,\mathfrak{p}})^\times.$$

Theorem 5.2 *1. In the above sitution, the Shimura curve M_U has an integral model $\mathbf{M}_U$ defined over* $\operatorname{spec}\mathcal{O}_{(\mathfrak{p})}$*, and the completion of this model along its special fibre is isomorphic as a formal $\mathcal{O}_\mathfrak{p}$-scheme (and the isomorphism is $G(\mathbb{A}^{\infty,\mathfrak{p}})$-equivariant) to*

$$\mathrm{GL}_2(\mathrm{F}_\mathfrak{p})\backslash(\mathfrak{h}_\mathfrak{p} \times_{\mathrm{Spf}\,\mathcal{O}_\mathfrak{p}} \mathrm{Spf}\,\mathcal{O}_\mathfrak{p}^{\mathrm{unr}}) \times X_H,$$

where X_H denotes the finite set $\overline{H}\backslash\overline{G}(\mathbb{A}^\infty)/\overline{G}(\mathbb{Q})$ and $\mathfrak{h}_\mathfrak{p}$ is Mumford's $\mathfrak{p}$-adic upper half-plane.

2. In particular, the dual graph associated to the special fibre of $\mathbf{M}_U$ is $\mathrm{GL}_2(\mathrm{F}_\mathfrak{p})^+\backslash(\Delta \times X_H)$, where Δ denotes the Bruhat-Tits building of $\mathrm{SL}_2(\mathrm{F}_\mathfrak{p})$; here, $\mathrm{GL}_2(\mathrm{F}_\mathfrak{p})^+$ denotes the set of elements of $\mathrm{GL}_2(\mathrm{F}_\mathfrak{p})$ with even $\mathfrak{p}$-adic valuation.

6 Ribet's theorem

As already remarked, the existence of auxiliary primes and Carayol's Lemma proves that one may lower the level for characteristic 2 representations in Cases (2)–(4) of Theorem 2.2 in the same way as [15] or [11] does for odd characteristic representations. To finish the proof of Theorem 0.1, it remains to verify Case (1). For odd characteristic, this is done in [18], except for certain cases where $[\mathrm{F} : \mathbb{Q}]$ is even. In this section, we deal with the case of characteristic 2 representations, also indicating how to deal with all cases when $[\mathrm{F} : \mathbb{Q}]$ is even. This analysis is also valid for odd characteristic, and thus completes the proof of level lowering for primes not dividing the characteristic in this case also.

The proof synthesizes the techniques of Buzzard ([3]) with the work of Rajaei ([18]) to find a version of Ribet's theorem for $\ell = 2$ applicable for totally real fields. Most of the hard work has been done in these two sources, and we refer to them for certain details.

Our target is to prove Theorem 0.1. For simplicity, we shall first describe the case where $[\mathrm{F} : \mathbb{Q}]$ is odd, and will later indicate how to adapt the argument to the even degree case.

We therefore fix a modular mod 2 Galois representation

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

which is continuous, irreducible and not induced from a character of $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}(i))$. Part of the hypotheses of the statement is that $\overline{\rho}$ is associated to some modular form of level prime to 2. If D denotes the quaternion algebra over F ramified at exactly all infinite places of F except τ_1, then the Jacquet-Langlands correspondence provides examples of automorphic representations on D of conductor prime to 2 and of some weight whose mod 2 Galois representation are isomorphic to $\overline{\rho}$.

Fix isomorphisms between D and GL_2 at split places in the usual way. If π is such an automorphic representation, with a fixed vector under $U \subset \mathrm{GL}_2(\mathbb{A}_{\mathrm{F}}^{\infty})$ and of weight k, then π corresponds to a maximal ideal m in the Hecke algebra $\mathbb{T} = \mathbb{T}_k^D(U)$ defined in §1. The level structure U gives a Shimura curve M_U as in §5.2, and Carayol ([5], §2) defines a sheaf $\mathcal{F}_k^D$ on M_U corresponding to the weight k.

Definition 6.1 We say that $\overline{\rho}$ satisfies *multiplicity one at weight k* if for all such maximal ideals m coming from automorphic representations of conductor prime to 2 and weight k, we have

$$\dim_{\mathbb{T}/\mathsf{m}}(H^1(M_U \otimes_{\mathrm{F}} \overline{\mathrm{F}}, \mathcal{F}_k^D) \otimes \mathbb{T}/\mathsf{m}) = 1.$$

Although we expect multiplicity one to hold often (after all, Fujiwara [10] has shown that at least in the ordinary case the minimal Hecke algebra is a complete intersection), Kilford ([16]) has shown that it sometimes fails for $\mathrm{F} = \mathbb{Q}$ when $\ell = 2$.

Having defined the notion of multiplicity one, we now turn to the proof of Theorem 0.1. By Remark 2.4, it suffices to consider Case (1) of Theorem 2.2, i.e., the special unramified case. Thus we suppose that $\overline{\rho}$ is modular of some weight k and some level $U_1(\mathfrak{n}) \cap U_0(\mathfrak{p})$. Here, $\mathfrak{n}$ is coprime to 2, and $\mathfrak{p} \nmid 2\mathfrak{n}$. We must prove the following result.

Theorem 6.2 *Let* $f \in S_k(U_1(\mathfrak{n}) \cap U_0(\mathfrak{p}))$ *be a Hilbert cuspidal eigenform, where* $(\mathfrak{n}, 2) = 1$ *and* $\mathfrak{p} \nmid 2\mathfrak{n}$ *is a prime ideal. Suppose that the mod 2 representation associated to* f,

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2),$$

1. *is absolutely irreducible and unramified at* $\mathfrak{p}$,
2. *is not induced from a character of* $\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}(i))$,
3. *satisfies multiplicity one at weight* k.

Then there is a Hilbert cuspidal eigenform $g \in S_k(U_1(\mathfrak{n}))$ *that gives rise to* $\overline{\rho}$.

In order to apply geometric arguments, we first add some auxiliary level structure with the aid of Theorem 4.3. This theorem guarantees the existence of infinitely many primes $\mathfrak{r}_0 \nmid 2\mathfrak{n}\mathfrak{p}$ such that $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{r}_0) > 4^d$ and such that $\mathfrak{r}_0$ is an example of a prime such that Theorem 4.3 holds. We may then add auxiliary level $U_1^1(\mathfrak{r}_0)$-structure, and we showed in [14], §12, that this is sufficiently small so that integral models exist for Shimura curves with this level structure. We may thus use geometric arguments when this auxiliary level is present; however, all modular forms occuring are automatically old at $\mathfrak{r}_0$.

Write U for the level structure $U_1(\mathfrak{n}) \cap U_1^1(\mathfrak{r}_0)$. Thus $f \in S_k(U \cap U_0(\mathfrak{p}))$.

Write $\mathbb{T}_U$ (resp. $\mathbb{T}_{\mathfrak{p},U}$) for the Hecke algebra $\mathbb{T}_k^D(U)$ (resp. $\mathbb{T}_k^D(U \cap U_0(\mathfrak{p}))$). So $\mathbb{T}_U$ is generated by operators $T_\mathfrak{r}$ and $S_\mathfrak{r}$ for primes $\mathfrak{r} \nmid \mathfrak{n}\mathfrak{r}_0$ and operators $U_\mathfrak{r}$ for primes $\mathfrak{r} | \mathfrak{n}\mathfrak{r}_0$, and $\mathbb{T}_{\mathfrak{p},U}$ has the same generators, except that there is an operator $U_\mathfrak{p}$ replacing the pair $T_\mathfrak{p}$ and $S_\mathfrak{p}$. On the $\mathfrak{p}$-old subspace of $S_k(U \cap U_0(\mathfrak{p}))$, the operators $S_\mathfrak{p}$, $T_\mathfrak{p}$ and $U_\mathfrak{p}$ are related by the Eichler-Shimura relation

$$U_\mathfrak{p}^2 - U_\mathfrak{p} T_\mathfrak{p} + N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{p}) S_\mathfrak{p} = 0.$$

As $\overline{\rho}$ is modular of level $U \cap U_0(\mathfrak{p})$ by hypothesis, there is a non-trivial maximal ideal $\widehat{\mathsf{m}}$ of $\mathbb{T}_{\mathfrak{p},U}$ containing 2 and a Hilbert cuspidal eigenform f whose mod 2 eigenvalues are given by the map

$$\mathbb{T}_{\mathfrak{p},U} \longrightarrow \mathbb{T}_{\mathfrak{p},U}/\widehat{\mathsf{m}} \hookrightarrow \overline{\mathbb{F}}_2$$

such that $\overline{\rho}$ is the mod 2 Galois representation associated to f.

Next, we add another auxiliary prime to the level. Its function is rather different to the first.

Let G denote the image of $\overline{\rho}$. As in [3], G must have even order; if it were to have odd order, then it could not have any degree 2 absolutely irreducible representations: its representation theory would be the same as in characteristic 0, and then the degree of any absolutely irreducible representation would divide the order of the group. We may therefore find an involution $\sigma \in G$. By the Čebotarev density theorem, there are infinitely many primes $\mathfrak{q}$ such that $\overline{\rho}(\mathsf{Frob}_\mathfrak{q}) = \sigma$. All involutions in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ have trace 0, so we conclude that these Frobenius elements $\mathsf{Frob}_\mathfrak{q}$ are special. We fix such a prime $\mathfrak{q} \nmid \mathfrak{n}\mathfrak{p}$. We will also be considering the Hecke algebra $\mathbb{T}_{\mathfrak{p}\mathfrak{q},U}$ associated to $U \cap U_0(\mathfrak{p}\mathfrak{q})$. We say that an ideal m of $\mathbb{T}_{\mathfrak{p}\mathfrak{q},U}$ is *compatible with* $\widehat{\mathsf{m}}$ if the restrictions of the two maps

$$\begin{array}{rcl} \mathbb{T}_{\mathfrak{p},U} \longrightarrow \mathbb{T}_{\mathfrak{p},U}/\widehat{\mathsf{m}} & \hookrightarrow & \overline{\mathbb{F}}_2 \\ \mathbb{T}_{\mathfrak{p}\mathfrak{q},U} \longrightarrow \mathbb{T}_{\mathfrak{p}\mathfrak{q},U}/\mathsf{m} & \hookrightarrow & \overline{\mathbb{F}}_2 \end{array}$$

agree on the intersection of the two Hecke algebras.

We have the following level raising result:

Theorem 6.3 *If* m *is a maximal ideal of* $\mathbb{T}_{\mathfrak{p}\mathfrak{q},U}$ *which is* $\mathfrak{p}$*-new, and compatible with* $\widehat{\mathsf{m}}$*, then* m *is also* $\mathfrak{q}$*-new.*

Proof. This is exactly as in [18], Theorem 5, noting that $N_{\mathrm{F}/\mathbb{Q}}(\mathfrak{q})$ is odd and $\operatorname{tr} \overline{\rho}(\mathsf{Frob}_\mathfrak{q}) = 0$, so that $T_\mathfrak{q} \in \widehat{\mathsf{m}}$. □

So there is a Hilbert cusp form in $S_k(U \cap U_0(\mathfrak{p}\mathfrak{q}))$, which is $\mathfrak{p}$-new and $\mathfrak{q}$-new and which gives rise to the representation $\overline{\rho}$. If there were a form in

$S_k(U \cap U_0(\mathfrak{q}))$, then we could apply Mazur's Principle of [14] or [11] as in Remark 2.5, as $\overline{\rho}(\mathsf{Frob}_\mathfrak{q})$ is of order 2 in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$, and is therefore not a scalar. Mazur's Principle now implies that there must be a form in $S_k(U)$ giving $\overline{\rho}$, and so the theorem above will hold.

Thus we assume for a contradiction that there is no Hilbert cusp form in $S_k(U \cap U_0(\mathfrak{q}))$ giving $\overline{\rho}$. Write $\mathbb{T}$ for the Hecke algebra $\mathbb{T}_{\mathfrak{pq},U}$.

We let B denote the quaternion algebra over F ramified at all infinite places of F except τ_1, and also at both $\mathfrak{p}$ and $\mathfrak{q}$, so differs from D only in that the invariants at $\mathfrak{p}$ and $\mathfrak{q}$ have been switched. We fix an isomorphism $B \otimes \mathrm{F}_v \cong D \otimes \mathrm{F}_v$ at all other places v, and also integral versions at all finite $v \neq \mathfrak{p}, \mathfrak{q}$. As we have already fixed isomorphisms between D and GL_2 at finite places, we obtain isomorphisms between B and GL_2 at all finite split places.

As in [18], we let $\mathcal{C}$ denote the Shimura curve associated to the quaternion algebra B with level structure U, and we write $M_{\mathfrak{pq},U}$ (resp. $M_{\mathfrak{p},U}$, $M_{\mathfrak{q},U}$) for the Shimura curve associated to D with level structure $U_0(\mathfrak{pq}) \cap U$ (resp. $U_0(\mathfrak{p}) \cap U$, $U_0(\mathfrak{q}) \cap U$). Rajaei points ([18], §3.1) out that the Hecke algebra $\mathbb{T}$ acts on the cohomology of all of these objects (which is not *a priori* clear for $\mathcal{C}$).

As remarked above, Carayol ([5], §2, §4) defines a sheaf $\mathcal{F}_k^D$ on $M_{\mathfrak{pq},U}$ corresponding to the weight k, and explains how to extend the definition to the integral model. The same construction (see [18], §3.1) gives a sheaf $\mathcal{F}_k^B$ on $\mathcal{C}$. We make the following abbreviations for objects defined in §5.1:

$$\begin{aligned}
X_\mathfrak{p}(\mathfrak{p}) &= X(M_{\mathfrak{p},U} \otimes \overline{\mathrm{F}}_\mathfrak{p}, \mathcal{F}_k^D),\\
X_\mathfrak{p}(\mathfrak{pq}) &= X(M_{\mathfrak{pq},U} \otimes \overline{\mathrm{F}}_\mathfrak{p}, \mathcal{F}_k^D),\\
X_\mathfrak{q}(\mathfrak{p}) &= X(M_{\mathfrak{p},U} \otimes \overline{\mathrm{F}}_\mathfrak{q}, \mathcal{F}_k^D),\\
X_\mathfrak{q}(\mathfrak{pq}) &= X(M_{\mathfrak{pq},U} \otimes \overline{\mathrm{F}}_\mathfrak{q}, \mathcal{F}_k^D),
\end{aligned}$$

and similarly for $\widehat{X}$ and the "component group" Φ. We will also use these definitions with $\mathfrak{p}$ and $\mathfrak{q}$ interchanged. As for $\mathcal{C}$, we define:

$$\begin{aligned}
Y_\mathfrak{p}(\mathfrak{q}) &= X(\mathcal{C} \otimes \overline{\mathrm{F}}_\mathfrak{p}, \mathcal{F}_k^B),\\
\widehat{Y}_\mathfrak{p}(\mathfrak{q}) &= \widehat{X}(\mathcal{C} \otimes \overline{\mathrm{F}}_\mathfrak{p}, \mathcal{F}_k^B),\\
\Psi_\mathfrak{p}(\mathfrak{q}) &= \Phi(\mathcal{C} \otimes \overline{\mathrm{F}}_\mathfrak{p}, \mathcal{F}_k^B);
\end{aligned}$$

again we will use these definitions with $\mathfrak{p}$ and $\mathfrak{q}$ interchanged.

The detailed studies of the dual graphs of the special fibres of $M_{\mathfrak{pq},U}$ mod $\mathfrak{q}$ and $\mathcal{C}$ mod $\mathfrak{p}$ shows that the combinatorics of the two reductions have much in common. In particular, the vertices (resp. edges) of the dual graph of the special fibre of $\mathcal{C}$ mod $\mathfrak{p}$ are in bijection with the singular points of $M_{\mathfrak{q},U}$ mod $\mathfrak{q}$ (resp. of $M_{\mathfrak{pq},U}$ mod $\mathfrak{q}$). Using this, Rajaei proves ([18], (3.15)) that there is an analogue of Ribet's exact sequence in this general weight, general totally real field, case:

$$0 \longrightarrow \widehat{X}_{\mathfrak{q}}(\mathfrak{q})^2_{\mathfrak{m}} \longrightarrow \widehat{X}_{\mathfrak{q}}(\mathfrak{pq})_{\mathfrak{m}} \longrightarrow \widehat{Y}_{\mathfrak{p}}(\mathfrak{q})_{\mathfrak{m}} \longrightarrow 0$$

and similarly with $\mathfrak{p}$ and $\mathfrak{q}$ interchanged.

By the theorem of Boston, Lenstra and Ribet ([1]), the $\mathbb{T}$-module $H^1(M_{\mathfrak{pq},U} \otimes_{\mathrm{F}} \overline{\mathrm{F}}, \mathcal{F}_k^D) \otimes \mathbb{T}/\mathfrak{m}$ is a semisimple $\mathbb{T}/\mathfrak{m}[\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})]$-module, isomorphic to $\check{\overline{\rho}}^{\lambda}$ for some $\lambda \geq 1$.

As we are assuming that $\overline{\rho}$ satisfies multiplicity one, we have $\lambda = 1$.

In the same way, $H^1(\mathcal{C} \otimes_{\mathrm{F}} \overline{\mathrm{F}}, \mathcal{F}_k^B) \otimes \mathbb{T}/\mathfrak{m}$ is a semisimple $\mathbb{T}/\mathfrak{m}[\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})]$-module, isomorphic to $\check{\overline{\rho}}^{\mu}$ for some integer μ. As $\mathfrak{m}$ corresponds to a cuspidal eigenform on $U_0(\mathfrak{pq}) \cap U$ which is new at $\mathfrak{p}$ and at $\mathfrak{q}$, the corresponding automorphic representation is special at $\mathfrak{p}$ and $\mathfrak{q}$. Then the Jacquet-Langlands correspondence furnishes a cuspidal automorphic representation on B of level $\mathcal{O}_{B,\mathfrak{p}}^{\times} \times \mathcal{O}_{B,\mathfrak{q}}^{\times} \times U$ whose associated Galois representation is $\overline{\rho}$. It follows that $\mu > 0$.

Our assumptions on $\overline{\rho}$ imply that $X_{\mathfrak{q}}(\mathfrak{q})_{\mathfrak{m}} = 0$ and $\widehat{X}_{\mathfrak{q}}(\mathfrak{q})_{\mathfrak{m}} = 0$.

Proposition 6.4 *We have:*

1. $\dim_{\mathbb{T}/\mathfrak{m}}(\widehat{Y}_{\mathfrak{p}}(\mathfrak{q}) \otimes \mathbb{T}/\mathfrak{m}) = 2\mu$,
2. $\dim_{\mathbb{T}/\mathfrak{m}}(\widehat{X}_{\mathfrak{q}}(\mathfrak{pq}) \otimes \mathbb{T}/\mathfrak{m}) \leq 1$.

Proof.

1. This is proven in the same way as the first claim of [18], Proposition 10. We have the following isomorphisms:

$$\begin{aligned} \widehat{Y}_{\mathfrak{p}}(\mathfrak{q}) \otimes \mathbb{T}/\mathfrak{m} &\cong (H^1(\mathcal{C} \otimes \overline{\mathrm{F}}_{\mathfrak{p}}, \mathcal{F}_k^B) \otimes \mathbb{T}/\mathfrak{m})^{I_{\mathfrak{p}}} \\ &\cong H^1(\mathcal{C} \otimes \overline{\mathrm{F}}_{\mathfrak{p}}, \mathcal{F}_k^B) \otimes \mathbb{T}/\mathfrak{m} \\ &\cong H^1(\mathcal{C} \otimes \overline{\mathrm{F}}, \mathcal{F}_k^B) \otimes \mathbb{T}/\mathfrak{m} \\ &\cong \check{\overline{\rho}}^{\mu} \end{aligned}$$

where the first isomorphism comes from the theory of vanishing cycles (see [18], Lemma 1), and the second occurs as $\overline{\rho}$ is unramified at $\mathfrak{p}$. Now $\overline{\rho}$ is 2-dimensional as a $\mathbb{T}/\mathfrak{m}$-vector space, and so the result follows.

2. From the specialisation exact sequence for $M_{\mathfrak{pq},U}$ mod $\mathfrak{q}$, we get the following exact sequence (as in [18]):

$$0 \longrightarrow H^1(\mathbf{M}_{\mathfrak{pq},U} \otimes \overline{\kappa}_{\mathfrak{q}}, \mathcal{F}_k^D)_{\mathfrak{m}} \longrightarrow H^1(\mathbf{M}_{\mathfrak{pq},U} \otimes \overline{\mathrm{F}}_{\mathfrak{q}}, \mathcal{F}_k^D)_{\mathfrak{m}} \longrightarrow X_{\mathfrak{q}}(\mathfrak{pq})_{\mathfrak{m}}(-1) \longrightarrow 0.$$

We see that $X_{\mathfrak{q}}(\mathfrak{pq})(-1) \otimes \mathbb{T}/\mathfrak{m}$ is a quotient of $H^1(\mathbf{M}_{\mathfrak{pq},U} \otimes \overline{\mathrm{F}}_{\mathfrak{q}}, \mathcal{F}_k^D) \otimes \mathbb{T}/\mathfrak{m}$. However, this latter space is precisely $\overline{\rho}$ (at least restricted to a decomposition group at $\mathfrak{q}$), using the multiplicity one hypothesis. We know from Carayol's Theorem ([5], Théorème (A)) that $\mathsf{Frob}_{\mathfrak{q}}$ acts on $X_{\mathfrak{q}}(\mathfrak{pq}) \otimes \mathbb{T}/\mathfrak{m}$ by a scalar. However, $\mathfrak{q}$ was chosen so that $\overline{\rho}(\mathsf{Frob}_{\mathfrak{q}})$ is an involution on a 2-dimensional space. It follows that any quotient space on which $\mathsf{Frob}_{\mathfrak{q}}$ acts as a scalar must be at most 1-dimensional.

Finally, as the integral model $\mathbf{M}_{\mathfrak{pq},U}$ is regular (as U is sufficiently small), the theory of vanishing cycles implies that $X_{\mathfrak{q}}(\mathfrak{pq})$ is isomorphic (as $\mathbb{T}$-modules, though not as Galois modules) to $\widehat{X}_{\mathfrak{q}}(\mathfrak{pq})$. They therefore have the same dimension, and the result follows.

□

Finally, however, we consider Ribet's exact sequence:

$$0 \longrightarrow \widehat{X}_{\mathfrak{q}}(\mathfrak{q})^2_{\mathfrak{m}} \longrightarrow \widehat{X}_{\mathfrak{q}}(\mathfrak{pq})_{\mathfrak{m}} \longrightarrow \widehat{Y}_{\mathfrak{p}}(\mathfrak{q})_{\mathfrak{m}} \longrightarrow 0.$$

Our assumptions on $\overline{\rho}$ imply that $\widehat{X}_{\mathfrak{q}}(\mathfrak{q})_{\mathfrak{m}} = 0$. It follows that the remaining two terms are isomorphic, but we have just shown that the first has dimension ≤ 1, while the second has dimension 2μ. As μ is a strictly positive integer, this is a contradiction. This contradiction establishes the desired result.

In the even degree case, we will construct yet another auxiliary prime $\mathfrak{r}_1$ such that $\overline{\rho}(\mathsf{Frob}_{\mathfrak{r}_1})$ is an involution as above. This implies that $T_{\mathfrak{r}_1} \in \mathfrak{m}$, and we may then use Taylor's level raising result ([19], Theorem 1) to add $\mathfrak{r}_1$ to the level. We then use exactly the same argument as above, except where all of the quaternion algebras involved are also ramified at $\mathfrak{r}_1$, and where all Hecke algebras contain the operator $U_{\mathfrak{r}_1}$ rather than $S_{\mathfrak{r}_1}$ and $T_{\mathfrak{r}_1}$. At the end of the argument we remove the prime $\mathfrak{r}_1$ from the level using Fujiwara's version of Mazur's Principle ([11], §5) for the even degree case.

In fact, this approach also works when ℓ is an odd prime. One adds an auxiliary prime to the level using Taylor's result, lowers the level using Rajaei's result (in which there is no multiplicity one hypothesis), and removes the auxiliary prime using Fujiwara's result. This therefore completes level lowering away from the characteristic for all odd primes, and completes the proof of Theorem 0.1 and Theorem 0.2. We stress that in this case, all necessary results are already due to Fujiwara and Rajaei, and the only new results in this paper concern the case $\ell = 2$.

An alternative to this method might be to compare the Shimura curve of level $U_0(\mathfrak{p}) \times H$ in characteristic $\mathfrak{q}$ for the quaternion algebra ramified at all but one infinite places and at $\mathfrak{p}$ with the Shimura curve of level $U_0(\mathfrak{q}) \times H$ in characteristic $\mathfrak{p}$ for the quaternion algebra ramified at all but one infinite places and at $\mathfrak{q}$. One might hope to derive a version of Ribet's theorem without introducing auxiliary primes, which would be rather cleaner. However, the theory of level raising already exists in the even degree case, and so we make use of it freely.

References

[1] N.Boston, H.Lenstra, K.Ribet, Quotients of group rings arising from two-dimensional representations, C. R. Acad. Sci. Paris 312 (1991) 323–328

[2] J.-F.Boutot, T.Zink, The p-adic uniformisation of Shimura curves, preprint

[3] K.Buzzard, On level-lowering for mod 2 representations, Math. Res. Lett. 7 (2000) 95–110

[4] H.Carayol, Sur la mauvaise réduction des courbes de Shimura, Comp. Math. 59 (1986) 151–230

[5] H.Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, Ann. Sci. Ec. Norm. Sup. 19 (1986) 409–468

[6] H.Carayol, Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires, Duke Math. J. 59 (1989) 785–801

[7] F.Diamond, The Taylor-Wiles construction and multiplicity one, Invent. Math. 128 (1997) 379–391

[8] F.Diamond, R.Taylor, Non-optimal levels of mod ℓ modular representations, Invent. Math. 115 (1994) 435–462

[9] F.Diamond, R.Taylor, Lifting modular mod ℓ representations, Duke Math. J. 74 (1994) 253–269

[10] K.Fujiwara, Deformation rings and Hecke algebras in the totally real case, preprint (1996)

[11] K.Fujiwara, Level optimisation in the totally real case, preprint (1999, revised 2004)

[12] H.Hida, On p-adic Hecke algebras for GL_2 over totally real fields, Ann. Math. 128 (1988) 295–384

[13] L.Illusie, Réalisation ℓ-adique de l'accouplement de monodromie, d'après A.Grothendieck, Astérisque 196–97 (1991) 27–44

[14] F.Jarvis, Mazur's Principle for totally real fields of odd degree, Comp. Math. 116 (1999) 39–79

[15] F.Jarvis, Level lowering for modular mod ℓ representations over totally real fields, Math. Ann. 313 (1999) 141–160

[16] L.Kilford, Some examples of non-Gorenstein Hecke algebras associated to modular forms, J. Number Theory 97 (2002) 157–164

[17] R.Livné, On the conductors of modulo ℓ representations coming from modular forms, Journal of Number Theory 31 (1989) 133–141

[18] A.Rajaei, On the levels of mod ℓ-Hilbert modular forms, J. reine angew. Math. 537 (2001) 33–65

[19] R.Taylor, On Galois representations associated to Hilbert modular forms, Invent. Math. 98 (1989) 265–280

[20] Y.Varshavsky, p-adic uniformisation of unitary Shimura varieties I, Publ. Math. IHES 87 (1998) 57–119

[21] Y.Varshavsky, p-adic uniformisation of unitary Shimura varieties II, J. Diff. Geom. 49 (1998) 75–113

Frazer Jarvis
Department of Pure Mathematics
Hicks Building
University of Sheffield
Sheffield S3 7RH
Great Britain
a.f.jarvis@sheffield.ac.uk

Universal Norms of p-Units in Some Non-Commutative Galois Extensions

dedicated to Professor John Coates on the occasion of his 60th birthday

Kazuya Kato

Received: September 27, 2005
Revised: June 30, 2006

2000 Mathematics Subject Classification: Primary 14M25; Secondary 14F20

1 Introduction.

Fix a prime number p. Let F be a finite extension of $\mathbb{Q}$ and let F_∞ be an algebraic extension of F. We will consider the $\mathbb{Z}_p$-submodule $U(F_\infty/F)$ of $O_F[1/p]^\times \otimes \mathbb{Z}_p$ defined by

$$U(F_\infty/F) = \mathrm{Image}(\varprojlim_L (O_L[1/p]^\times \otimes \mathbb{Z}_p) \to O_F[1/p]^\times \otimes \mathbb{Z}_p),$$

where L ranges over all finite extensions of F contained in F_∞ and where the inverse limit is taken with respect to the norm maps.
In the case F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F, the understanding of $U(F_\infty/F)$ is related to profound aspects in Iwasawa theory studied by Coates and other people, as we will shortly recall in §3. Concerning bigger Galois extensions F_∞/F, the following result is (essentially) contained in Corollary 3.23 of Coates and Sujatha [4] (see §3 of this paper).

Assume F_∞/F is a Galois extension and $\mathrm{Gal}(F_\infty/F)$ *is a commutative p-adic Lie group. Assume also that there is only one place of F lying over p. Then $U(F_\infty/F)$ is of finite index in $O_F[1/p]^\times \otimes \mathbb{Z}_p$.*

We ask what happens in the case of non-commutative Lie extensions.
The purpose of this paper is to prove the following theorem, which was conjectured by Coates.

Theorem 1.1. *Let $a_1, \cdots, a_r \in F$, and let*

$$F_n = F(\zeta_{p^n}, a_1^{1/p^n}, \cdots, a_r^{1/p^n}), \quad F_\infty = \cup_{n\geq 1} F_n,$$

where ζ_{p^n} denotes a primitive p^n-th root of 1. Let F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F. Then:

(1) The quotient group $U(F^{\mathrm{cyc}}/F)/U(F_\infty/F)$ is finite.

(2) If there is only one place of F lying over p, then $U(F_\infty/F)$ is of finite index in $O_F[1/p]^\times \otimes \mathbb{Z}_p$.

An interesting point in the proof is that we use the finiteness of the higher K-groups $K_{2n}(O_F)$ for $n \geq 1$, for this result on the muliplicative group K_1. The author does not have any result on $\varprojlim_L O_F[1/S]^\times$ without $\otimes\mathbb{Z}_p$.
The plan of this paper is as follows. In §2, we review basic facts. In §3, we review some known results in the case F_∞/F is an abelian extension. In §4 and §5, we prove Theorem 1.1 (we will prove a slightly stronger result Theorem 5.1).
The author expresses his hearty thanks to John Coates for suggesting this subject and for advice, and to Ramdorai Sujatha for advice and the hospitality in Tata Institute where a part of this work was done.

2 Basic facts.

We prepare basic facts related to $U(F_\infty/F)$. Most materials appear in Coates and Sujatha [4]. We principally follow their notation.

2.1. Let p be a prime number, and let F be a finite extension of $\mathbb{Q}$. In the case $p = 2$, we assume F is totally imaginary, for simplicity.
Let F_∞ be a Galois extension of F such that the Galois group $G = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group and such that only finitely many finite places of F ramify in F_∞.
Let $\mathbb{Z}_p[[G]]$ be the completed group ring of G, that is, the inverse limit of the group rings $\mathbb{Z}_p[G/U]$ where U ranges over all open subgroups of G.

2.2. We define $\mathbb{Z}_p[[G]]$-modules

$$\mathcal{Z}^i(F_\infty) \quad \text{and} \quad \mathcal{Z}^i_S(F_\infty) \quad (i \geq 0)$$

where S is a finite set of finite places of F contaning all places of F lying over p. Let

$$\mathcal{Z}^i_S(F_\infty) = \varprojlim_L H^i(O_L[1/S], \mathbb{Z}_p(1))$$

where L ranges over all finite extensions of F contained in F_∞, $O_L[1/S]$ denotes the subring of L consisting of all elements which are integral at any finite place of L not lying over S, and H^i is the étale cohomology. In the case S is the set of all places of F lying over p, we denote $\mathcal{Z}^i_S(F_\infty)$ simply by $\mathcal{Z}^i(F_\infty)$.

Since

$$(1) \quad H^1(O_L[1/S], \mathbb{Z}_p(1)) \simeq O_L[1/S]^\times \otimes \mathbb{Z}_p$$

by Kummer theory,

$$(2) \quad \mathcal{Z}^1_S(F_\infty) \simeq \varprojlim_L (O_L[1/S]^\times \otimes \mathbb{Z}_p).$$

Note that $H^i(O_L[1/S], \mathbb{Z}_p(1))$ are finitely generated $\mathbb{Z}_p$-modules and $\mathcal{Z}^i(F_\infty)$ are finitely generated $\mathbb{Z}_p[[G]]$-modules. These modules are zero if $i \geq 3$ for the reason of cohomological dimension (here in the case $p = 2$, we use our assumption F is totally imaginary).

2.3. Let $U_S(F_\infty/F)$ be the image of $\varprojlim_L (O_L[1/S]^\times \otimes \mathbb{Z}_p)$ in $O_F[1/S]^\times \otimes \mathbb{Z}_p$. Here L ranges over all finite extensions of F contained in F_∞.
The main points of the preparation in this section are the isomorphisms (1b) and (2b) below.

(1) Assume S contains all finite places of F which ramify in F_∞. Then there are canonical isomorphisms

$$(1a) \qquad H_0(G, \mathcal{Z}^2_S(F_\infty)) \simeq H^2(O_F[1/S], \mathbb{Z}_p(1)),$$

$$(1b) \quad H_1(G, \mathcal{Z}^2_S(F_\infty)) \simeq (O_F[1/S]^\times \otimes \mathbb{Z}_p)/U_S(F_\infty/F).$$

(2) Assume F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc}. Then we have canonical isomorphisms

$$(2a) \qquad H_0(G, \mathcal{Z}^2(F_\infty/F)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^2(O_F[1/p], \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

$$(2b) \quad H_1(G, \mathcal{Z}^2(F_\infty)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq (O_F[1/p]^\times \otimes \mathbb{Z}_p)/U(F_\infty/F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Here $H_m(G, ?) = \mathrm{Tor}_m^{\mathbb{Z}_p[[G]]}(\mathbb{Z}_p, ?)$ denotes the G-homology. Note that $H_m(G, M)$ are finitely generated $\mathbb{Z}_p$-modules for any finitely generated $\mathbb{Z}_p[[G]]$-module M.

(1a) and (1b) follow from the spectral sequence

$$E_2^{i,j} = H_{-i}(G, \mathcal{Z}^j_S(F_\infty)) \Rightarrow E^i_\infty = H^i(O_F[1/S], \mathbb{Z}_p(1)),$$

the isomorphisms 2.2 (1) (2), and the fact $\mathcal{Z}^j_S(F_\infty) = 0$ for $j \geq 3$. The above spectral sequence is given in [9] Proposition 8.4.8.3 in the case G is commutative. In general, we have the above spectral sequence by [6] 1.6.5 (3).
The proofs of (2a) and (2b) are given in 2.6 later.

2.4. By Kummer theory and by the well known structure theorem of the Brauer group of a global field, we have an exact sequence

$$(1) \quad 0 \to \mathrm{Pic}(O_F[1/S])\{p\} \to H^2(O_F[1/S], \mathbb{Z}_p(1)) \to \oplus_{v \in S} \mathbb{Z}_p \xrightarrow{\mathrm{sum}} \mathbb{Z}_p \to 0,$$

where $\{p\}$ denotes the p-primary part. Let

$$Y_S(F_\infty) = \varprojlim_L \mathrm{Pic}(O_L[1/S])\{p\},$$

where L ranges over all finite extensions of F contained in F_∞. In the case S is the set of all places of F lying over p, we denote $Y_S(F_\infty)$ simply by $Y(F_\infty)$. Then the exact sequences (1) with F replaced by L give an exact sequence of $\mathbb{Z}_p[[G]]$-modules

$$(2) \quad 0 \to Y_S(F_\infty) \to \mathcal{Z}_S^2(F_\infty) \to \oplus_{v\in S}\mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p[[G_v]]} \mathbb{Z}_p \to \mathbb{Z}_p \to 0$$

where for each $v \in S$, $G_v \subset G$ is the decomposition group of a place of F_∞ lying over v.
If S contains all finite place of F which ramify in F_∞, the composite homomorphism

$$(3) \quad (O_F[1/S]^\times \otimes \mathbb{Z}_p)/U(F_\infty/F) \simeq H_1(G, \mathcal{Z}_S^2(F_\infty))$$
$$\to \oplus_{v\in S} H_1(G, \mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p[[G_v]]} \mathbb{Z}_p) = \oplus_{v\in S} H_1(G_v, \mathbb{Z}_p)$$

induced by (1b) and (2) coincides with the homomorphism induced by the reciprocity maps

$$F_v^\times \to G_v^{\mathrm{ab}}(p) \simeq H_1(G_v, \mathbb{Z}_p)$$

of local class field theory, where G_v^{ab} denotes the abelian quotient of G_v and (p) means the pro-p part.

2.5. Assume $F_\infty \supset F^{\mathrm{cyc}}$. Then we have isomorphisms

$$\mathcal{Z}^1(F_\infty) \xrightarrow{\simeq} \mathcal{Z}_S^1(F_\infty), \quad Y(F_\infty) \xrightarrow{\simeq} Y_S(F_\infty).$$

The first isomorphism shows $U(F_\infty/F) = U_S(F_\infty/F)$.
In fact, for each finite extension L of F contained in F_∞, we have an exact sequence

$$\begin{aligned} 0 &\to O_L[1/p]^\times \otimes \mathbb{Z}_p \to O_L[1/S]^\times \otimes \mathbb{Z}_p \to \\ &\to \oplus_w \mathbb{Z}_p \to \mathrm{Pic}(O_L[1/p])\{p\} \to \mathrm{Pic}(O_L[1/S])\{p\} \to 0 \end{aligned}$$

where w ranges over all places of L lying over S but not lying over p. If L' is a finite extension of F such that $L \subset L' \subset F_\infty$, and if w' is a place of L' lying over w, the transition map from $\mathbb{Z}_p$ at w' to $\mathbb{Z}_p$ at w is the multiplication by the degree of the residue extension of w'/w. Since the residue extension of v in F^{cyc}/F for v not lying over p is a $\mathbb{Z}_p$-extension, this shows that the inverse limit of $\oplus_w \mathbb{Z}_p$ for varying L is zero. Hence we have the above isomorphisms.

2.6. We prove (2a) (2b) of 2.3. Take S containing all finite places of F which ramify in F_∞. Let T be the set of all elements of S which do not lie over p.

By 2.4 (2) and by $Y(F_\infty) \overset{\simeq}{\to} Y_S(F_\infty)$ in 2.5, we have an exact sequence of $\mathbb{Z}_p[[G]]$-modules

$$0 \to \mathcal{Z}^2(F_\infty) \to \mathcal{Z}^2_S(F_\infty) \to \oplus_{v\in T}\mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p[[G_v]]} \mathbb{Z}_p \to 0.$$

This gives a long exact sequence

$$\begin{aligned}\cdots \to H_m(G, \mathcal{Z}^2(F_\infty)) \to H_m(G, \mathcal{Z}^2_S(F_\infty)) \to \\ \to \oplus_{v\in T}H_m(G_v, \mathbb{Z}_p) \to H_{m-1}(G, \mathcal{Z}^2(F_\infty)) \to \cdots .\end{aligned}$$

Let $G^{\mathrm{cyc}} = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$ and for $v \in T$, let G_v^{cyc} be the image of G_v in G^{cyc}. Then v is unramified in F^{cyc}/F, and we have a canonical isomorphism $G_v^{\mathrm{cyc}} \simeq \mathbb{Z}_p$ which sends the Frobenius of v in G_v^{cyc} to $1 \in \mathbb{Z}_p$. Let H_v $(v \in T)$ be the kernel of $G_v \to G_v^{\mathrm{cyc}}$. Since G is a p-adic Lie group and since the characteristic of the residue field of v is different from p, H_v is of dimension ≤ 1 as a p-adic Lie group. Furthermore, if H_v is infinite, for an element σ_v of G_v whose image in G_v^{cyc} is the Frobenius of v, the inner automorphism on H_v by σ_v is of infinite order as is seen from the usual description of the tame quotient of the absolute Galois group of F_v. These prove

(1) For $v \in T$, the kernel and the cokernel of the canonical map $H_m(G_v, \mathbb{Z}_p) \to H_m(G_v^{\mathrm{cyc}}, \mathbb{Z}_p)$ are finite for any m.

Since the composition $O_F[1/S]^\times \to H_1(G, \mathcal{Z}^2_S(F_\infty)) \to H_1(G_v^{\mathrm{cyc}}, \mathbb{Z}_p) = G_v^{\mathrm{cyc}} \simeq \mathbb{Z}_p$ for $v \in T$ coincides with the v-adic valuation $O_F[1/S]^\times \to \mathbb{Z}$, (1) shows that the cokernel of $H_1(G, \mathcal{Z}^2_S(F_\infty)) \to \oplus_{v\in T}H_1(G_v, \mathbb{Z}_p)$ is finite. Hence by the above long exact sequence, we have the following commutative diagram with exact rows in which the kernel of the first arrow of each row is finite.

$$\begin{tikzcd}
H_0(G, \mathcal{Z}^2(F_\infty)) \arrow[r] \arrow[d] & H_0(G, \mathcal{Z}^2_S(F_\infty)) \arrow[r] \arrow[d] & \oplus_{v\in T}\mathbb{Z}_p \arrow[r] \arrow[d] & 0 \\
H^2(O_F[1/p], \mathbb{Z}_p(1)) \arrow[r] & H^2(O_F[1/S], \mathbb{Z}_p(1)) \arrow[r] & \oplus_{v\in T}\mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

By this diagram and by 2.3 (1a), we have 2.3 (2a).
We next prove 2.3 (2b). By the above (1), $H_2(G_v, \mathbb{Z}_p)$ is finite for $v \in T$. By this and by the case $m = 1$ of the above (1), we see that the complex $0 \to H_1(G, \mathcal{Z}^2(F_\infty)) \to H_1(G, \mathcal{Z}^2_S(F_\infty)) \to \oplus_{v\in T}H_1(G_v^{\mathrm{cyc}}, \mathbb{Z}_p)$ has finite homology groups. By 2.3 (1b) and by $U(F_\infty/F) = U_S(F_\infty/F)$ (2.5), the kernel of the last arrow of this complex is isomorphic to $(O_F[1/p]^\times \otimes \mathbb{Z}_p)/U(F_\infty/F)$. This proves 2.3 (2b).

3 ABELIAN EXTENSIONS (REVIEW).

In this section, we review the proof of the following result of Coates and Sujatha ([4] Cor. 3.23), and then recall some known facts on $U(F^{\mathrm{cyc}}/F)$.

PROPOSITION 3.1. *Assume F_∞/F is Galois and* $\mathrm{Gal}(F_\infty/F)$ *is a commutative p-adic Lie group. Assume further that there is only one place of F lying over p. Then:*

(1) $U(F_\infty/F)$ is of finite index in $O_F[1/p]^\times \otimes \mathbb{Z}_p$.

(2) $H_m(G, Y(F_\infty))$ and $H_m(G, \mathcal{Z}^2(F_\infty))$ are finite for any m.

In fact, this result was written in [4] in the situation $\mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p^2$. This was because this result appeared in [4] in the study of the arithmetic of a $\mathbb{Z}_p^2$-extension generated by p-power division points of an elliptic curve with complex multiplication. We just check here that the method of their proof works in this generality.

Proof. We may (and do) assume $F_\infty \supset F^{\mathrm{cyc}}$. In the case $p = 2$, to apply our preparation in §2, we assume F is totally imaginary without a loss of generality (we may replace F by a finite extension of F having only one place lying over p for the proof of 3.1).
(1) follows from the finiteness of $H_1(G, \mathcal{Z}^2(F_\infty))$ in (2) by 2.3 (2b). We prove (2).
We have $H_0(G, \mathcal{Z}^2(F_\infty)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^2(O_F[1/p], \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ by 2.3 (2a), and $H^2(O_F[1/p], \mathbb{Z}_p(1))$ is finite by the exact sequence 2.4 (1) and by the assumption that there is only one place of F lying oer p. Hence $H_0(G, \mathcal{Z}^2(F_\infty)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0$. This shows that $H_m(G, \mathcal{Z}^2(F_\infty)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0$ for any m (Serre [11]). (Here the assumption G is commutative is essential. See 5.6.) This proves $H_m(G, \mathcal{Z}^2(F_\infty))$ is finite for any m.
Let v be the unique place of F lying over p. Then by class field theory, the decomposition group G_v of v in G is of finite index in G. By the exact sequence

$$H_2(G_v, \mathbb{Z}_p) \to H_2(G, \mathbb{Z}_p) \to H_1(G, \mathcal{Z}^2(F_\infty)/Y(F_\infty)) \to H_1(G_v, \mathbb{Z}_p) \to H_1(G, \mathbb{Z}_p)$$

obtained from 2.4 (2), this shows that $H_1(G, \mathcal{Z}^2(F_\infty)/Y(F_\infty))$ and hence the kernel of $H_0(G, Y(F_\infty)) \to H_0(G, \mathcal{Z}^2(F_\infty))$ are finite. Hence $H_0(G, Y(F_\infty))$ is finite, and by Serre [11], $H_m(G, Y(F_\infty))$ is finite for any m. □

3.2. In the rest of this section, we recall some known facts about $U(F^{\mathrm{cyc}}/F)$. Let $G^{\mathrm{cyc}} = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. For a place v of F lying over p, let $G_v^{\mathrm{cyc}} \subset G^{\mathrm{cyc}}$ be the decomposition group of v (so $G_v^{\mathrm{cyc}} \simeq \mathbb{Z}_p$). Let $(\oplus_{v|p} G_v^{\mathrm{cyc}})^0$ be the kernel of the canoncial map $\oplus_{v|p} G_v^{\mathrm{cyc}} \to G^{\mathrm{cyc}}$.
Let

$$\alpha_F \quad : \quad (O_F[1/p]^\times \otimes \mathbb{Z}_p)/U(F^{\mathrm{cyc}}/F) \to (\oplus_{v|p} G_v^{\mathrm{cyc}})^0$$

be the homomorphism induced by the reciprocity maps of local fields F_v, which appeared in 2.4 (3).
It is known that the following conditions (1) - (3) are equivalent.

(1) $\mathrm{Ker}\,(\alpha_F)$ is finite. (That is, $U(F^{\mathrm{cyc}}/F)$ is of finite index in the kernel of $O_F[1/p]^\times \otimes \mathbb{Z}_p \to (\oplus_{v|p} G_v^{\mathrm{cyc}})^0$.)

(2) $\mathrm{Coker}\,(\alpha_F)$ is finite.

(3) $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))$ is finite.

The equivalence of (1)-(3) is proved as follows. Though this is not at all an essential point, in the case $p = 2$, to apply our preparation in §2, we assume F is totally imaginary without a loss of generality (we can replace F by a finite extension of F for the proof of the equivalence). Let σ be a topological generator of G^{cyc}. Then $H_0(G^{\mathrm{cyc}}, \mathcal{Z}^2(F^{\mathrm{cyc}}))$ is isomorphic to the cokernel of $\sigma - 1 : \mathcal{Z}^2(F^{\mathrm{cyc}}) \to \mathcal{Z}^2(F^{\mathrm{cyc}})$ and $H_1(G^{\mathrm{cyc}}, \mathcal{Z}^2(F^{\mathrm{cyc}}))$ is isomorphic to the kernel of it. Since $\mathcal{Z}^2(F^{\mathrm{cyc}})$ is a torsion $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$-module, this shows that the $\mathbb{Z}_p$-rank of $H_1(G^{\mathrm{cyc}}, \mathcal{Z}^2(F^{\mathrm{cyc}})) \simeq (O_F[1/p] \otimes \mathbb{Z}_p)/U(F^{\mathrm{cyc}}/F)$ is equal to the $\mathbb{Z}_p$-rank of $H_0(G^{\mathrm{cyc}}, \mathcal{Z}^2(F^{\mathrm{cyc}})) \simeq H^2(O_F[1/p], \mathbb{Z}_p(1))$ which is equal to the $\mathbb{Z}_p$-rank of $(\oplus_{v|p} G_v^{\mathrm{cyc}})^0$ by 2.4 (1). Hence (1) and (2) are equivalent. The exact sequence 2.4 (2) (take $F_\infty = F^{\mathrm{cyc}}$ and S to be the set of all places of F lying over p) shows that $\mathrm{Coker}\,(\alpha_F)$ is isomorphic to the kernel of $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}})) \to H_0(G^{\mathrm{cyc}}, \mathcal{Z}^2(F^{\mathrm{cyc}})) = H^2(O_F[1/p], \mathbb{Z}_p(1))$. The image of the last map is $\mathrm{Pic}(O_F[1/p])\{p\}$ by 2.4 (1) (2), and hence is finite. Hence $\mathrm{Coker}\,(\alpha_F)$ is finite if and only if $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))$ is finite.

3.3. Greenberg [7] proved that $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))$ is finite if F is an abelian extension of $\mathbb{Q}$ (hence all (1) - (3) in 3.2 are satisfied in this case).

3.4. In the case F is totally real, by Coates [2] Theorem 1.13, $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))$ is finite if Leopoldt conjecture for F is true.

3.5. Let F be a CM field. Let F^+ be the real part of F, and let $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))^\pm \subset H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))$ be the $\pm$-part with respect to the action of the complex conjugation in $\mathrm{Gal}(F/F^+)$. Then by the above result of Coates, $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))^+$ is finite if Leopoldt conjecture for F^+ is true. On the other hand, Conjecture 2.2 in Coates and Lichtenbaum [3] says that $H_0(G^{\mathrm{cyc}}, Y(F^{\mathrm{cyc}}))^-$ is finite. In [8], Gross conjectured that the kernel and the cokernel of the (-)-part α_F of α_F is finite (this finiteness is also a consequence of Conjecture 2.2 of [3]), and formulated a conjecture which relates α_F^- to the leading terms of the Taylor expansions at $s = 0$ of p-adic Artin L-functions.
Thus known conjectures support that the equivalent conditions (1) - (3) in 3.2 are satisfied by any CM field F.
A natural question arises: Are (1) - (3) in 3.2 true for any number field F?

4 A result on Tor modules.

The purpose of this section is to prove Proposition 4.2 below.

4.1. For a compact p-adic Lie group G, for a $\mathbb{Z}_p[[G]]$-module T, and for a continuous homomorphism $G \to \mathbb{Z}_p^\times$, let $T(\chi)$ be the $\mathbb{Z}_p[[G]]$-module whose underlying abelian group is that of T and on which $\mathbb{Z}_p[[G]]$ acts by $\mathbb{Z}_p[[G]] \to \mathbb{Z}_p[[G]] \to \mathrm{End}(T)$, where the first arrow is the automorphism $\sigma \mapsto \chi(\sigma)\sigma$ ($\sigma \in G$) of the topological ring $\mathbb{Z}_p[[G]]$ and the second arrow is the original action of $\mathbb{Z}_p[[G]]$ on T. We call $T(\chi)$ the twist of T by χ.

Proposition 4.2. *Let G be a compact p-adic Lie group, let H be a closed normal subgroup of G, and assume that we are given a finite family of closed normal subgroups H_i $(0 \le i \le r)$ of G such that $\{1\} = H_0 \subset H_1 \subset \cdots \subset H_r = H$, $H_i/H_{i-1} \simeq \mathbb{Z}_p$ for $1 \le i \le r$ and such that the the action of G on H_i/H_{i-1} by inner automorphisms is given by a homomorphism $\chi_i : G/H \to \mathbb{Z}_p^\times$.*
Let M be a finitely generated $\mathbb{Z}_p[[G]]$-module, and let M' be a subquotient of the $\mathbb{Z}_p[[G]]$-module M. Let $m \ge 0$. Then there is a finite family $(S_i)_{1\le i\le k}$ of $\mathbb{Z}_p[[G/H]]$-submodules of $H_m(H, M')$ satisfying the following (i) *and* (ii)*.*

(i) $0 = S_0 \subset S_1 \subset \cdots \subset S_k = H_m(H, M')$.

(ii) *For each i $(1 \le i \le k)$, there are a subquotient T of the $\mathbb{Z}_p[[G/H]]$-module $H_0(H, M)$ and a family $(s(j))_{1\le j\le r}$ of non-negative integers $s(j)$ such that $\sharp\{j|s(j) > 0\} \ge m$ and such that S_i/S_{i-1} is isomorphic to the twist $T(\prod_{1\le j\le k} \chi_j^{s(j)})$ of T.*

Note

$$H_m(H, M) = \mathrm{Tor}_m^{\mathbb{Z}_p[[H]]}(\mathbb{Z}_p, M) = \mathrm{Tor}_m^{\mathbb{Z}_p[[G]]}(\mathbb{Z}_p[[G/H]], M)$$

for $\mathbb{Z}_p[[G]]$-modules M.
A key point in the proof of Proposition 3.1 was that for commutative rings, Tor_m vanishes if Tor_0 vanishes. This is not true for non-commutative rings. In the next section, we will use the above relation of Tor_0 and Tor_m in a non-commutative situation for the proof of Theorem 1.1.

4.3. We denote this proposition with fixed r by (A_r). Let (B_r) be the case $M = M'$ of (A_r).

Since (B_r) is a special case of (A_r), (B_r) follows from (A_r).
In 4.4, we show that conversely, (A_r) follows from (B_r). In 4.5, we prove (B_1). In 4.6, for $r \ge 1$, we prove (B_r) assuming (A_{r-1}) and (B_1). These give a proof of Prop.4.2.

4.4. We can deduce (A_r) from (B_r) as follows. Let M'' be the quotient of the $\mathbb{Z}_p[[G]]$-module M such that M' is a $\mathbb{Z}_p[[G]]$-submodule of M''. We have an exact sequence of $\mathbb{Z}_p[[G/H]]$-modules

$$H_{m+1}(H, M''/M') \to H_m(H, M') \to H_m(H, M'').$$

Then (A_r) for the pair (M, M') is obtained from (B_r) applied to M''/M' and to M'' since $H_0(H, M''/M')$ and $H_0(H, M'')$ are quotients of the $\mathbb{Z}_p[[G/H]]$-module $H_0(H, M)$.

4.5. We prove (B_1). Assume $r = 1$. Let $\chi = \chi_1$.
Note that $H \simeq \mathbb{Z}_p$. Let α be a topological generator of H, and let $N = \alpha - 1 \in \mathbb{Z}_p[[G]]$. Let $I = \mathrm{Ker}\,(\mathbb{Z}_p[[G]] \to \mathbb{Z}_p[[G/H]]) = \mathbb{Z}_p[[G]]N = N\mathbb{Z}_p[[G]]$.
We have

(1) For $\sigma \in G$, $\sigma N \sigma^{-1}$ is expressed as a power series in N with coefficients in $\mathbb{Z}_p$ which is congruent to $\chi(\sigma)N \mod N^2$. In particular, $\sigma N \sigma^{-1} \equiv \chi(\sigma)N$ mod I^2.

In fact, $\sigma N \sigma^{-1} = \alpha^{\chi(\sigma)} - 1 = (1+N)^{\chi(\sigma)} - 1 = \chi(\sigma)N + \sum_{n \geq 2} c_i N^i$ for some $c_i \in \mathbb{Z}_p$.
Concerning $H_m(H, M)$ $(m \geq 0)$, we have:

(2) $N(M)$ is a $\mathbb{Z}_p[[G]]$-submodule of M, I kills $M/N(M)$, and there is an isomorphism of $\mathbb{Z}_p[[G/H]]$-modules

$$H_0(H, M) \simeq M/N(M).$$

(3) $\mathrm{Ker}\,(N : M \to M)$ is a $\mathbb{Z}_p[[G]]$-submodule of M, I kills $\mathrm{Ker}\,(N : M \to M)$, and there is an isomorphism of $\mathbb{Z}_p[[G/H]]$-modules

$$H_1(H, M) \simeq \mathrm{Ker}\,(N : M \to M)(\chi).$$

(4) $H_m(H, M) = 0$ fo $m \geq 2$.

We prove (2)–(4). We have a projective resolution

$$0 \to I \to \mathbb{Z}_p[[G]] \to \mathbb{Z}_p[[G/H]] \to 0$$

of the right $\mathbb{Z}_p[[G]]$-module $Z_p[[G/H]]$. Since $H_m(H, ?) = \mathrm{Tor}_m^{\mathbb{Z}_p[[G]]}(\mathbb{Z}_p[[G/H]], ?)$, $H_0(H, M)$ (resp. $H_1(H, M)$) is isomorphic to the cokernel (resp. kernel) of $I \otimes_{\mathbb{Z}_p[[G]]} M \to M$, and $H_m(H, M) = 0$ for all $m \geq 2$. This proves (2) and (4). Furthermore,

$$H_1(H, M) \simeq \mathrm{Ker}\,(I \otimes_{\mathbb{Z}_p[[G]]} M \to M) \simeq I \otimes_{\mathbb{Z}_p[[G]]} \mathrm{Ker}\,(N : M \to M)$$
$$\simeq I/I^2 \otimes_{\mathbb{Z}_p[[G/H]]} \mathrm{Ker}\,(N : M \to M).$$

Consider the bijection

$$\mathrm{Ker}\,(N : M \to M) \to I/I^2 \otimes_{\mathbb{Z}_p[[G/H]]} \mathrm{Ker}\,(N : M \to M)\ ;\ x \mapsto N \otimes x.$$

By the above (1), for $\sigma \in G$, we have $\sigma N \otimes x = \chi(\sigma) N \sigma \otimes x = \chi(\sigma) N \otimes \sigma x$ in $I/I^2 \otimes_{\mathbb{Z}_p[[G/H]]} \mathrm{Ker}\,(N : M \to M)$. Hence

$$I/I^2 \otimes_{\mathbb{Z}_p[[G/H]]} \mathrm{Ker}\,(N : M \to M) \simeq \mathrm{Ker}\,(N : M \to M)(\chi)$$

as $\mathbb{Z}_p[[G/H]]$-modules. This proves (3).
Let

$$V_n = \mathrm{Ker}\,(N^n : M \to M) \quad (n \geq 0), \quad V = \cup_n V_n.$$

Then, since $\mathbb{Z}_p[[G]]N^n = N^n \mathbb{Z}_p[[G]]$, V_n is a $\mathbb{Z}_p[[G]]$-submodule of M. Since $\mathbb{Z}_p[[G]]$ is Noetherian and M is a finitely generated $\mathbb{Z}_p[[G]]$-module, $V = V_n$ for some n. That is, N is nilpotent on V. Since $\mathrm{Ker}\,(N : M/V \to M/V) = 0$, we have $H_1(H, M/V) = 0$ by (3). Hence

(5) $H_1(H, V) = H_1(H, M)$,

(6) $H_0(H, V) \to H_0(H, M)$ is injective.

Consider the monodromy filtration $(W_i)_i$ on the abelian group V given by the nilpotent endomorphism N in the sense of Deligne [5] 1.6. It is an increasing filtration characterized by the properties $N(W_i) \subset W_{i-2}$ for all i, and $N^i : \mathrm{gr}_i^W \overset{\simeq}{\to} \mathrm{gr}_{-i}^W$ for all $i \geq 0$.

(7) W_i are $\mathbb{Z}_p[[G]]$-submodules of V.

In fact, for $\sigma \in G$, the filtration $(\sigma W_i)_i$ also has the characterizing property of $(W_i)_i$ by (1).
Now we define an increasing filtration $(W_i')_i$ of the $\mathbb{Z}_p[[G/H]]$-module $H_0(H, V)$ and an increasing filtration $(W_i'')_i$ on the $\mathbb{Z}_p[[G/H]]$-module $H_1(H, V) = H_1(H, M)$ as follows. By identifying $H_0(H, V)$ with $\mathrm{Coker}\,(N : V \to V)$, let $W_i' = W_i(\mathrm{Coker}\,(N : V \to V))$ (i.e. the image of W_i in $\mathrm{Coker}\,(N : V \to V)$). By identifying $H_1(H, V)$ with $\mathrm{Ker}\,(N : V \to V)(\chi)$, let $W_i'' = W_i(\mathrm{Ker}\,(N : V \to V))(\chi)$ (i.e. $(W_i \cap \mathrm{Ker}\,(N : V \to V))(\chi)$). Then $W_0'' = H_1(H, M)$, and $W_i'' = 0$ if i is sufficiently small. We prove:

(8) For any $i \geq 0$,

$$\mathrm{gr}_{-i}^{W''} \simeq \mathrm{gr}_i^{W'}(\chi^{i+1})$$

as $\mathbb{Z}_p[[G/H]]$-modules.

By the injectivity of $H_0(H, V) \to H_0(H, M)$ (6), this proves (B$_1$).

We prove (8). By (1), we have

(9) The map $N : \mathrm{gr}_i^W \to \mathrm{gr}_{i-2}^W$ satisfies $\sigma N \sigma^{-1} = \chi(\sigma) N$ for $\sigma \in G$.

Let $P_i \subset \mathrm{gr}_i^W$ $(i \leq 0)$ be the primitive part $\mathrm{Ker}\,(N : \mathrm{gr}_i^W \to \mathrm{gr}_{i-2}^W)$ ([5] 1.6.3). Then for $i \geq 0$, the canonical map $\mathrm{gr}_{-i}^W(\mathrm{Ker}\,(N : V \to V)) \to P_{-i}$ is an isomorphism of $\mathbb{Z}_p[[G/H]]$-modules ([5] 1.6.6). Furthermore, we have a bijection $P_{-i} \overset{\simeq}{\to} \mathrm{gr}_i^W(\mathrm{Coker}\,(N : V \to V))$ as the composition

$$P_{-i} \to \mathrm{gr}_{-i}^W \overset{N^i}{\leftarrow} \mathrm{gr}_i^W \to \mathrm{gr}_i^W(\mathrm{Coker}\,(N : V \to V))$$

([5] 1.6.4, 1.6.6, and the dual statement of 1.6.6 for $\mathrm{Coker}\,(N)$). By (9), this gives an isomorphism of $\mathbb{Z}_p[[G/H]]$-modules $P_{-i} \simeq \mathrm{gr}_i^W(\mathrm{Coker}\,(N : V \to V))(\chi^i)$. Hence we have (8).

4.6. Let $r \geq 1$. We prove (B_r) assuming (A_{r-1}) and (B_1). Let $J = H_1$. By the spectral sequence

$$E_2^{-i,-j} = H_i(H/J, H_j(J, M)) \Rightarrow E_\infty^{-m} = H_m(H, M)$$

in which $H_j(J,M) = 0$ for $j \geq 2$, we have an exact sequence of $\mathbb{Z}_p[[G/H]]$-modules

$$(1) \quad H_{m-1}(H/J, H_1(J,M)) \to H_m(H,M) \to H_m(H/J, H_0(J,M)).$$

We consider $H_{m-1}(H/J, H_1(J,M))$ first. By (B_1) applied to the triple (G,J,M), $H_1(J,M)$ is a successive extension of twists of subquotients of $H_0(J,M)$ by χ_1^i $(i \geq 1)$. By (A_{r-1}) applied the triple $(G/J, H/J, H_0(J,M))$, $H_{m-1}(H/J, ?)$ of these subquotients of $H_0(J,M)$ are successive extensions of twists of subquotients of $H_0(H/J, H_0(J,M)) = H_0(H,M)$ by $\prod_{2 \leq j \leq r} \chi_j^{s(j)}$ such that $s(j) \geq 0$ for all j and such that $\sharp(\{j \,|\, s(j) > 0\} \geq m-1$. Hence $H_{m-1}(H/J, H_1(J,M))$ is a successive extension of twists of subquotients of $H_0(H,M)$ by $\prod_{1 \leq j \leq r} \chi_j^{s(j)}$ such that $s(j) \geq 0$ for all j and such that $\sharp(\{j \,|\, s(j) > 0\} \geq m$.

We consider $H_m(H/J, H_0(J,M))$ next. By (B_{r-1}) (which is assumed since we assume (A_{r-1})) applied to the triple $(G/J, H/J, H_0(J,M))$, $H_m(H/J, H_0(J,M))$ is a successive extension of twists of subquotients of $H_0(H/J, H_0(J,M)) = H_0(H,M)$ by $\prod_{2 \leq j \leq r} \chi_i^{s(j)}$ such that $s(j) \geq 0$ for all j and such that $\sharp(\{j \,|\, s(j) > 0\} \geq m$.

By these properties of $H_{m-1}(H/J, H_1(J,M))$ and $H_m(H/J, H_0(J,M))$, the exact sequence (1) proves (B_r) (assuming (A_{r-1}) and (B_1)).

5 Some non-commutative Galois extensions.

Theorem 1.1 in Introduction is contained in Corollary 5.2 of the following Theorem 5.1, for the extension F_∞/F in Theorem 1.1 satisfies the assumption of Theorem 5.1 with $n(i) = 1$ for all i.

Theorem 5.1. *Assume that F_∞ is a Galois extension of F, $F_\infty \supset \cup_n F(\zeta_{p^n})$, and that there is a finite family of closed normal subgroups H_i $(1 \leq i \leq r)$ of $G = \mathrm{Gal}(F_\infty/F)$ satisfying the following condition. Let F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F and let H be the kernel of $G \to G^{\mathrm{cyc}} = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Then $\{1\} = H_0 \subset H_1 \subset \cdots \subset H_r$, H_r is an open subgroup of H, and for $1 \leq i \leq r$, $H_i/H_{i-1} \simeq \mathbb{Z}_p$ and the action of G on it by inner automorphism is the $n(i)$-th power of the cyclotomic character $G \to \mathbb{Z}_p^\times$ for some positive integer $n(i) > 0$. Let S be any finite set of finite places of F containing all places lying over p. Then the kernel and the cokernel of the canonical maps*

$$H_m(G, \mathcal{Z}_S^2(F_\infty)) \to H_m(G^{\mathrm{cyc}}, \mathcal{Z}_S^2(F^{\mathrm{cyc}})),$$
$$H_m(G, Y(F_\infty)) \to H_m(G^{\mathrm{cyc}}, Y(F^{cyc}))$$

are finite for any m.

In particular (since $H_m(G^{\mathrm{cyc}}, ?) = 0$ for $m \geq 2$), $H_m(G, \mathcal{Z}_S^2(F_\infty))$ and $H_m(G, Y(F_\infty))$ are finite for any $m \geq 2$.

Corollary 5.2. *Let the assumption be as in Theorem 5.1. Then:*

(1) The quotient group $U(F^{cyc}/F)/U(F_\infty/F)$ is finite.
(2) If there is only one place of F lying over p, then $U(F_\infty/F)$ is of finite index in $O_F[1/p]^\times \otimes \mathbb{Z}_p$, and $H_m(G, Y(F_\infty))$ and $H_m(G, \mathcal{Z}^2(F_\infty))$ are finite for any m.

(3) If F is an abelian extension over $\mathbb{Q}$, then $H_m(G, Y(F_\infty))$ is finite for any m.

In fact, by 2.3 (2b), (1) of Corollary 5.2 follows from the finiteness of the kernel and the cokernel of $H_1(G, \mathcal{Z}^2(F_\infty)) \to H_1(G^{\mathrm{cyc}}, \mathcal{Z}^2(F^{\mathrm{cyc}}))$ which is a special case of Theorem 5.1. (2) follows from (1) and the case $F_\infty = F^{\mathrm{cyc}}$ of Proposition 3.1. (3) follows from (1) and the result of Greenberg introduced in 3.3.

Corollary 5.3. *Let the assumption be as in Theorem 5.1. Then $H_m(G, \mathcal{Z}^1(F_\infty))$ for $m \geq 1$ and the kernel of the canonical map $H_0(G, \mathcal{Z}^1(F_\infty)) \to O_F[1/p]^\times \otimes \mathbb{Z}_p$ are finite.*

In fact, for S containing all finite places which ramify in F_∞, since $\mathcal{Z}^1(F_\infty) \overset{\simeq}{\to} \mathcal{Z}^1_S(F_\infty)$ (2.5), the spectral sequence in 2.3 shows that $H_m(G, \mathcal{Z}^1(F_\infty))$ for $m \geq 1$ is isomorphic to $H_{m+2}(G, \mathcal{Z}^2_S(F_\infty))$, and the kernel of $H_0(G, \mathcal{Z}^1(F_\infty)) \to O_F[1/p]^\times \otimes \mathbb{Z}_p$ is isomorphic to $H_2(G, \mathcal{Z}^2_S(F_\infty))$. Hence this corollary follows from the finiteness of $H_m(G, \mathcal{Z}^2_S(F_\infty))$ for $m \geq 2$ in Theorem 5.1.

5.4. We prove Theorem 5.1. First in this 5.4, we show that the kernel and the cokernel of $H_m(G, \mathcal{Z}^2_S(F_\infty)) \to H_m(G^{\mathrm{cyc}}, \mathcal{Z}^2_S(F^{\mathrm{cyc}}))$ are finite for any m assuming that S contains all finite places of F which ramify in F_∞,.
We may replace F by a finite extension of F. Hence we may assume that $H_r = H$, $\cup_{n\geq 1} F(\zeta_{p^n}) = F^{\mathrm{cyc}}$, and that in the case $p = 2$, F is totally imaginary. Let $\mathfrak{p}$ be the augmentation ideal of $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$. It is a prime ideal of $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$. By the spectral sequence $E_2^{-i,-j} = H_i(G^{\mathrm{cyc}}, H_j(H, ?)) \Rightarrow E_\infty^{-m} = H_m(G, ?)$, it is sufficient to prove that $H_i(G^{\mathrm{cyc}}, H_m(H, \mathcal{Z}^2_S(F_\infty)))$ is finite for any i and for any $m \geq 1$. For a finitely generated $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$-module M, $H_i(G^{\mathrm{cyc}}, M)$ is isomorphic to $M/\mathfrak{p}M$ if $i = 0$, to the part of M annihilated by $\mathfrak{p}$ if $i = 1$, and is zero if $i \geq 2$. Applying this taking $M = H_m(H, \mathcal{Z}^2_S(F_\infty))$, we see that it is sufficient to prove

$$(1) \quad H_m(H, \mathcal{Z}^2_S(F_\infty))_{\mathfrak{p}} = 0 \quad \text{for any} \quad m \geq 1,$$

where $(?)_{\mathfrak{p}}$ denotes the localization at the prime ideal $\mathfrak{p}$.
We apply Proposition 4.2 to the case $M = M' = \mathcal{Z}^2_S(F_\infty)$. By this proposition, to prove (1), it is sufficient to show that for any subquotient T of the $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$-module $H_0(H, M) = \mathcal{Z}^2_S(F^{\mathrm{cyc}})$ and for any integer $k \geq 1$, we have $T(k)_{\mathfrak{p}} = 0$. Here $T(k)$ is the k-th Tate twist. It is sufficient to prove that $H_0(G^{\mathrm{cyc}}, T(k))$ is finite. Since $\mathcal{Z}^2_S(F^{\mathrm{cyc}})$ is a finitely generated torsion $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$-module, the $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$-module T is a successive extension of $\mathbb{Z}_p[[G^{\mathrm{cyc}}]]$-modules which are

either finite or isomorphic to $\mathbb{Z}_p[[G^{\rm cyc}]]/\mathfrak{q}$ for some prime ideal $\mathfrak{q}$ of $\mathbb{Z}_p[[G^{\rm cyc}]]$ of height one. We may assume $T \simeq \mathbb{Z}_p[[G^{\rm cyc}]]/\mathfrak{q}$. Then there is a $\mathbb{Z}_p[[G^{\rm cyc}]]$-homomorphism $\mathcal{Z}^2_S(F^{\rm cyc}) \to T$ with finite cokernel. Hence it is sufficient to prove that $H_0(G^{\rm cyc}, \mathcal{Z}^2(F^{\rm cyc})(k)))$ is finite for any $k \geq 1$. But

$$H_0(G^{\rm cyc}, \mathcal{Z}^2(F^{\rm cyc})(k))) \simeq H^2(O_F[1/S], \mathbb{Z}_p(k+1)).$$

The last group is finite by Soulé [12]. In fact, by Quillen [10] and Borel [1], $K_{2k}(O_F[1/S])$ is finite, and by Soulé [12], we have a surjective Chern class map from $K_{2k}(O_F[1/S])$ to $H^2(O_F[1/S], \mathbb{Z}_p(k+1))$.

5.5. We complete the proof of Theorem 5.1. Let S be a finite set of finite places of F which contains all places of F lying over p. Take a finite set S' of finite places of F such that $S \subset S'$ and such that S' contains all finite places of F which ramify in F_∞.
By comparing the exact sequence 2.4 (2) for F_∞/F and that for $F^{\rm cyc}/F$, we see that the finiteness of the kernel and the cokernel of $H_m(G, \mathcal{Z}^2_S(F_\infty)) \to H_m(G^{\rm cyc}, \mathcal{Z}^2_S(F^{\rm cyc}))$ for all m and that of $H_m(G, Y(F_\infty)) \to H_m(G^{\rm cyc}, Y(F^{\rm cyc}))$ for all m are consequences of the following (1) - (3).

(1) The kernel and the cokernel of $H_m(G, \mathcal{Z}^2_{S'}(F_\infty)) \to H_m(G^{\rm cyc}, \mathcal{Z}^2_{S'}(F^{\rm cyc}))$ are finite for all m.

(2) The kernel and the cokernel of $H_m(G, \mathbb{Z}_p) \to H_m(G^{\rm cyc}, \mathbb{Z}_p)$ are finite for all m.

(3) The kernel and the cokernel of $H_m(G_v, \mathbb{Z}_p) \to H_m(G^{\rm cyc}_v, \mathbb{Z}_p)$ are finite for all m and for all finite places v of F. Here $G_v \subset G$ denotes a decomposition group of a place of F_∞ lying over v, and $G^{\rm cyc}_v$ denotes the image of G_v in $G^{\rm cyc}$.

We proved (1) already in 5.4. (2) and (3) follow from the case $M = M' = \mathbb{Z}_p$ of Proposition 4.2.

Remark 5.6. There is an example of a p-adic Lie extension F_∞/F for which there is only one place of F lying over p but $U(F_\infty/F)$ is not of finite index in $O_F[1/p]^\times \otimes \mathbb{Z}_p$. For example, let $F = \mathbb{Q}$, let E be an elliptic curve over F with good ordinary reduction at p, and let F_∞ be the field generated over F by p^n-division points of E for all n. Then $U(F_\infty/F) = \{1\}$ and is not of finite index in $O_F[1/p]^\times \otimes \mathbb{Z}_p = \mathbb{Z}[1/p]^\times \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p$. In fact $U(F_\infty/F)$ must be killed by the reciprocity map of local class field theory of $\mathbb{Q}_p$ into $G^{\rm ab}_p(p) \simeq \mathbb{Z}^2_p$, where $G_p \subset G = \mathrm{Gal}(F_\infty/F)$ denotes the decomposition group at p, and $G^{\rm ab}_p(p)$ denotes the pro-p part of the abelian quotient of G_p. The image of $p \in \mathbb{Z}[1/p]^\times$ in $G^{\rm ab}_p(p)$ is of infinite order. This proves $U(F_\infty/F) = \{1\}$. In this case, $H_0(G, \mathcal{Z}^2(F_\infty))$ is finite, but $H_1(G, \mathcal{Z}^2(F_\infty))$ is not finite.

Remark 5.7. There is an example of a p-adic Lie extension F_∞/F for which $G = \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}^2_p$ and $H_0(G, Y(F_\infty/F))$ is not finite. Let K be an imaginary quadratic field in which p splits, let K_∞ be the unique Galois extension of K such that $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p^2$, let F be a finite extension of K in which p splits completely, and let $F_\infty = FK_\infty$. Then the $\mathbb{Z}_p$-rank of $H_1(G, Y(F_\infty))$ is $\geq [F:K]-1$ as is shown below. Hence it is not zero if $F \neq K$. In fact, from the exact sequence 2.4 (2) with S the set of all places of F lying over p, we can obtain

$$\begin{aligned}&\mathrm{rank}_{\mathbb{Z}_p} H_1(G, Y(F_\infty)) \geq \\ &\quad \geq (\sum_{v \in S} \mathrm{rank}_{\mathbb{Z}_p} H_1(G_v, \mathbb{Z}_p)) - \mathrm{rank}_{\mathbb{Z}_p} H_1(G, \mathbb{Z}_p) - \mathrm{rank}_{\mathbb{Z}}\, O_F[1/p]^\times.\end{aligned}$$

But $\mathrm{rank}_{\mathbb{Z}_p} H_1(G_v, \mathbb{Z}_p) = 2$ for any $v \in S$, $\mathrm{rank}_{\mathbb{Z}_p} H_1(G, \mathbb{Z}_p) = 2$, $\mathrm{rank}_{\mathbb{Z}} O_F[1/p]^\times = 3[F:K]-1$ by Dirichlet's unit theorem, and hence the right hand side of the above inequality is $2[F:\mathbb{Q}]-2-(3[F:K]-1) = [F:K]-1$.

References

[1] Borel, A., *Stable real cohomology of arithmetic groups*, Ann. Sci. École Norm. Sup. 7 (1974), 235-272.

[2] Coates, J., *p-adic L-functions and Iwasawa's theory*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975), 269–353. Academic Press, (1977), 269–353.

[3] Coates, J. and Lichtenbaum, S., *On l-adic zeta functions*, Ann. of Math. 98 (1973), 498–550.

[4] Coates, J., and Sujatha, R, *Fine Selmer groups for elliptic curves with complex multiplication*, Algebra and Number Theory, Proc. of the Silver Jubilee Conference, Univ. of Hyderabad, ed. Rajat Tandon (2005), 327-337.

[5] Deligne, P., *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. 52 (1980), 137–252.

[6] Fukaya, T. and Kato, K., *A formulation of conjectures p-adic zeta functions in non-commutative Iwasawa theory* to appear in Proc. of Amer. Math. Soc.

[7] Greenberg, R., *On a certain l-adic representation*, Inventiones Math 21 (1973), 117–124.

[8] Gross, B., *p-adic L-series at $s = 0$*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), 979–994 (1982).

[9] Nekovar, J., J., *Selmer complexes*, preprint.

[10] Quillen, D., *Finite generation of the groups K_i of rings of algebraic integers*, Algebraic K-theory, I, Springer Lecture Notes 341 (1973), 179–198.

[11] Serre, J.-P., *Algèbra Locale; Multiplicités*, Springer Lecture Notes 11 (1975).

[12] Soulé, C., *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Inventiones Math 55 (1979), 251–295.

Kazuya Kato
kazuya@kusm.kyoto-u.ac.jp

An Elementary Proof of the Mazur-Tate-Teitelbaum Conjecture for Elliptic Curves

Dedicated to Professor John Coates on the occasion of his sixtieth birthday

Shinichi Kobayashi[1]

Received: November 29, 2005
Revised: February 15, 2006

Abstract. We give an elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves by using Kato's element.

2000 Mathematics Subject Classification: 11F85, 11G05, 11G07, 11G40, 11S40.
Keywords and Phrases: elliptic curves, p-adic L-functions, Iwasawa theory, the Mazur-Tate-Teitelbaum conjecture, exceptional zeros, Kato's element.

1. Introduction

The p-adic L-function $L_p(E,s)$ of an elliptic curve E defined over $\mathbb{Q}$ has an extra zero at $s=1$ coming from the interpolation factor at p if E has split multiplicative reduction at the prime p. The Mazur-Tate-Teitelbaum conjecture (now a theorem of Greenberg-Stevens) describes the first derivative of $L_p(E,s)$ as

$$\frac{d}{ds}L_p(E,s)\,|_{s=1} = \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\,\frac{L(E,1)}{\Omega_E^+}$$

where q_E is the Tate period of E coming from the p-adic uniformization of E at p, $\log_p$ is the Iwasawa p-adic logarithm, Ω_E^+ is the real period of E and $L(E,1)$ is the special value of the complex Hasse-Weil L-function at $s=1$.

Known proofs of this conjecture are classified into two kinds. One is, as Greenberg-Stevens [GS] did first, a proof using a global theory like Hida's universal ordinary deformation. The other is, as Kato-Kurihara-Tsuji [KKT] or Colmez [C] did, a proof based on local theory (except using Kato's element). Each kind of proof has its own importance but the latter type of proof makes it clear that the substantial facts behind this conjecture are of local nature. The p-adic L-function is the image of Kato's element via a purely local morphism,

[1] Supported by JSPS Postdoctoral Fellowships for Research Abroad.

the so called Coleman map or Perrin-Riou map. The extra zero phenomena discovered by Mazur-Tate-Teitelbaum is, in fact, a property of the local Coleman map.

In this paper, we prove a derivative formula (Theorem 4.1) of the Coleman map for elliptic curves by purely local and elementary method and we apply this formula to Kato's element to show the conjecture of Mazur-Tate-Teitelbaum. Of course, our proof is just a special and the simplest case of that in Kato-Kurihara-Tsuji [KKT] or Colmez [C] (they proved the formula not only for elliptic curves but for higher weight modular forms) but I believe that it is still worthwhile to write it down for the following reason. First, the important paper Kato-Kurihara-Tsuji [KKT] has not yet been published. Second, since we restrict ourselves to the case of elliptic curves, the proof is much simpler and elementary (of course, such a simple proof would be also known to specialists. In fact, Masato Kurihara informed me that Kato, Kurihara and Tsuji have two simple proofs and one is similar to ours). I hope that this paper would help those who are interested in the understanding of this interesting problem.

Acknowledgement: I would like to wish Professor John Coates a happy sixtieth birthday, and to thank him for his contribution to mathematics, especially to Iwasawa theory. It is my great pleasure to dedicate this article to him on this occasion.

This paper was written during the author's visit at the university of Paris 6. He would like to thank P. Colmez and L. Merel for the accommodation. He also would like to thank K. Bannai and N. Otsubo for discussion. Finally, he is grateful to the referee for his careful reading of the manuscript.

2. A structure of the group of local units in $k_\infty/\mathbb{Q}_p$.

Let k_∞ be the (local) cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty}) := \cup_{n=0}^{\infty}\mathbb{Q}_p(\zeta_{p^n})$ with Galois group Γ and let k_n be its n-th layer in k_∞ with Galois group Γ_n. We identify the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ with $\mathbb{Z}_p^\times$ by the cyclotomic character κ. Then Γ is identified with $1+p\mathbb{Z}_p$ and the torsion subgroup Δ of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ is regarded as $\mu_{p-1} \subset \mathbb{Z}_p^\times$.

Let U_n^1 be the subgroup of $\mathcal{O}_{k_n}^\times$ consisting of the elements which are congruent to 1 modulo the maximal ideal $\mathfrak{m}_n$ of $\mathcal{O}_{k_n}$.

Following the Appendix of Rubin [R] or [Ko], for a fixed generator $(\zeta_{p^n})_{n\in\mathbb{N}}$ of $\mathbb{Z}_p(1)$, we construct a certain canonical system of local points $(d_n)_n \in \varprojlim_n U_n^1$ and we determine the Galois module structure of U_n^1 by using these points. The idea of the construction of such a system is as follows. First we consider a certain formal group $\mathcal{F}$ isomorphic to $\widehat{\mathbb{G}}_m$ whose formal logarithm has a certain compatible property with the trace operator of k_∞. Then the system of local points is essentially the image of cyclotomic units by the isomorphism $\mathcal{F} \cong \widehat{\mathbb{G}}_m$. We let

$$\ell(X) = \log(1+X) + \sum_{k=0}^{\infty}\sum_{\delta\in\Delta}\frac{(X+1)^{p^k\delta}-1}{p^k}.$$

This power series is convergent in $\mathbb{Q}_p[[X]]$ due to the summation $\sum_{\delta\in\Delta}$. It is straightforward to see that

$$\ell'(X) \in 1 + X\mathbb{Z}_p[[X]], \quad \ell(0) = 0, \quad (\varphi - p)\circ\ell(X) \in p\mathbb{Z}_p[[X]]$$

where φ is the Frobenius operator such that $(\varphi\circ\ell)(X) = \ell((X+1)^p - 1)$. Hence by Honda's theory, there is a formal group $\mathcal{F}$ over $\mathbb{Z}_p$ whose logarithm is given by ℓ, and $\iota(X) = \exp\circ\,\ell\,(X) - 1 \in \mathbb{Z}_p[[X]]$ gives an isomorphism of formal groups $\mathcal{F} \cong \widehat{\mathbb{G}}_m$ over $\mathbb{Z}_p$. (See for example, Section 8 of [Ko].) Take an element ε of $p\mathbb{Z}_p$ such that $\ell(\varepsilon) = p$ and we define

$$c_n := \iota((\zeta_{p^{n+1}} - 1)\,[+]_{\mathcal{F}}\,\varepsilon).$$

Since this element is fixed by the group Δ, this is an element of $\widehat{\mathbb{G}}_m(\mathfrak{m}_n)$. Then by construction, $d_n = 1 + c_n \in U_n^1$ satisfies the relation

$$\log_p(d_n) = \ell(\varepsilon) + \ell(\zeta_{p^{n+1}} - 1) = p + \sum_{k=0}^{n}\sum_{\delta\in\Delta}\frac{\zeta_{p^{n+1-k}}{}^{\delta} - 1}{p^k}.$$

Proposition 2.1. *i)* $(d_n)_n$ *is a norm compatible system and* $d_0 = 1$.
ii) Let u *be a generator of* U_0^1. *Then as* $\mathbb{Z}_p[\Gamma_n]$*-module,* d_n *and* u *generate* U_n^1, *and* d_n *generates* $(U_n^1)^{\mathrm{N}=1}$ *where* N *is the absolute norm from* k_n *to* $\mathbb{Q}_p$.

Proof. Since $\zeta_p - 1$ is not contained in $\mathfrak{m}_n$, the group $\widehat{\mathbb{G}}_m(\mathfrak{m}_n)$ does not contain p-power torsion points. Therefore to see i), it suffices to show the trace compatibility of $(\log_p(d_n))_n$, and this is done by direct calculations. For ii), we show that $(\iota^{-1}(c_n)^\sigma)_{\sigma\in\Gamma_n}$ and ε generate $\mathcal{F}(\mathfrak{m}_n)$ as $\mathbb{Z}_p$-module by induction for n. The proof is the same as that of Proposition 8.11 of [Ko] but we rewrite it for the ease of the reader. The case $n = 0$ is clear. For arbitrary n, we show that $\ell(\mathfrak{m}_n) \subset \mathfrak{m}_n + k_{n-1}$ and

$$\mathcal{F}(\mathfrak{m}_n)/\mathcal{F}(\mathfrak{m}_{n-1}) \cong \ell(\mathfrak{m}_n)/\ell(\mathfrak{m}_{n-1}) \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}.$$

Here the first isomorphism is induced by the logarithm ℓ and the last isomorphism is by $(\mathfrak{m}_n + k_{n-1})/k_{n-1} \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}$. As a set, $\mathcal{F}(\mathfrak{m}_n)$ is the maximal ideal $\mathfrak{m}_n$, and we write $x \in \mathcal{F}(\mathfrak{m}_n)$ in the form $x = \sum_{\delta\in\Delta}\sum_i a_i\,\zeta_{p^{n+1}}^{i\delta}$, $a_i \in \mathbb{Z}_p$. Then for $y = \sum_{\delta\in\Delta}\sum_i a_i\,\zeta_{p^n}^{i\delta} \in \mathfrak{m}_{n-1}$, we have that $x^p \equiv y \mod p\mathcal{O}_{k_n}$. Therefore for $k \geq 1$, we have

$$\sum_{\delta\in\Delta}\frac{(x+1)^{p^k\delta} - 1}{p^k} \equiv \sum_{\delta\in\Delta}\frac{(x^p+1)^{p^{k-1}\delta} - 1}{p^k} \equiv \sum_{\delta\in\Delta}\frac{(y+1)^{p^{k-1}\delta} - 1}{p^k} \mod \mathfrak{m}_n.$$

Hence we have $\sum_\delta \frac{(x+1)^{p^k\delta}-1}{p^k} \in \mathfrak{m}_n + k_{n-1}$. Since $\ell(x)$ is convergent, for sufficiently large k_0, we have $\sum_{k=k_0}^{\infty}\sum_\delta \frac{(x+1)^{p^k\delta}-1}{p^k} \in \mathfrak{m}_n$, and therefore $\ell(x)$ is contained in $\mathfrak{m}_n + k_{n-1}$. Since ℓ is injective on $\mathcal{F}(\mathfrak{m}_n)$ (there is no torsion point in $\mathcal{F}(\mathfrak{m}_n) \cong \widehat{\mathbb{G}}_m(\mathfrak{m}_n)$) and is compatible with the Galois action, we have $\ell\,(\mathfrak{m}_n) \cap k_{n-1} = \ell\,(\mathfrak{m}_{n-1})$. Therefore we have an injection

$$\ell(\mathfrak{m}_n)/\ell(\mathfrak{m}_{n-1}) \hookrightarrow (\mathfrak{m}_n + k_{n-1})/k_{n-1} \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}.$$

By direct calculations, we have $\ell(\iota^{-1}(c_n)) \equiv \sum_\delta(\zeta_{p^{n+1}}^\delta - 1) \mod k_{n-1}$. Since $\sum_\delta(\zeta_{p^{n+1}}^\delta - 1)$ generates $\mathfrak{m}_n/\mathfrak{m}_{n-1}$ as a $\mathbb{Z}_p[\Gamma_n]$-module with respect to the usual addition, the above injection is in fact a bijection. Thus $(\iota^{-1}(c_n)^\sigma)_{\sigma\in\Gamma_n}$ generate $\mathcal{F}(\mathfrak{m}_n)/\mathcal{F}(\mathfrak{m}_{n-1})$. By induction $(\iota^{-1}(c_n)^\sigma)_{\sigma\in\Gamma_n}$ and ε generate $\mathcal{F}(\mathfrak{m}_n)$. Since $\widehat{\mathbb{G}}_m$ is isomorphic to $\mathcal{F}$ by ι, we have ii). □

Since $Nd_n = d_0 = 1$, by Hilbert's theorem 90, there exists an element $x_n \in k_n$ such that $d_n = x_n^\gamma/x_n$ for a fixed generator γ of Γ. We put $\pi_n = \prod_{\delta\in\Delta}(\zeta_{p^{n+1}}^\delta - 1)$. Then π_n is a norm compatible uniformizer of k_n. By the previous proposition, x_n can be taken of the form $x_n = \pi_n^{e_n}u_n$ for some integer e_n and $u_n \in (U_n^1)^{\mathrm{N}=1}$.

Proposition 2.2. *In the same notation as the above, we have*

$$p \equiv e_n\,(p-1)\,\log_p\kappa(\gamma) \mod p^{n+1}.$$

Proof. If we put

$$G(X) = \exp(p)\cdot\exp\circ\,\ell\,(X) = \exp\circ\,\ell\,(X[+]\varepsilon) \in 1 + (p, X)\mathbb{Z}_p[[X]],$$

then by definition

$$G_\sigma(\zeta_{p^{m+1}} - 1) = d_m^\sigma$$

where $G_\sigma(X) = G((X+1)^{\kappa(\sigma)} - 1)$ for $\sigma \in \Gamma$. By Proposition 2.1 ii), u_n is written as a product in the form $u_n = \prod(d_n^\sigma)^a$. If we put $H(X) = \prod G_\sigma(X)^a$, then $H(X)$ satisfies $H(\zeta_{p^{m+1}} - 1) = N_{k_n/k_m}u_n$ for $0 \le m \le n$. We put

$$F(X) = \left(\prod_{\delta\in\Delta}\frac{(X+1)^{\delta\kappa(\gamma)} - 1}{(X+1)^\delta - 1}\right)^{e_n}\frac{H((X+1)^{\kappa(\gamma)} - 1)}{H(X)}.$$

Then we have

$$G(X) \equiv F(X) \qquad \mod \frac{(X+1)^{p^{n+1}} - 1}{X}$$

since they are equal if we substitute $X = \zeta_{p^{m+1}} - 1$ for $0 \le m \le n$. Substituting $X = 0$ in this congruence and taking the p-adic logarithm, we have that $p \equiv e_n(p-1)\log_p\kappa(\gamma) \mod p^{n+1}$. □

3. The Coleman map for the Tate curve.

We construct the Coleman map for the Tate curve following the Appendix of [R] or Section 8 of [Ko]. See also [Ku]. In this section we assume that E is the Tate curve

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

where $q = q_E \in \mathbb{Q}_p^\times$ satisfying $|q|_p < 1$ and

$$s_k(q) = \sum_{n\ge1}\frac{n^k q^n}{1-q^n}, \quad a_4(q) = -s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

Then we have the uniformization

$$\phi :\ \mathbb{C}_p{}^\times/q^{\mathbb{Z}} \cong E_q(\mathbb{C}_p), \qquad u \mapsto (X(u,q), Y(u,q))$$

where

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q).$$

(Of course, we put $\phi(q^{\mathbb{Z}}) = O$.) This isomorphism induces the isomorphism of the formal groups $\widehat{\phi} : \widehat{\mathbb{G}}_m \cong \widehat{E}$. It is straightforward to see that the pull back by $\widehat{\phi}$ of the invariant differential $\omega_E = \frac{dx}{2y+x}$ on $\widehat{E}$ with the parameter $t = -x/y$ is the invariant differential $\omega_{\widehat{\mathbb{G}}_m} = \frac{dX}{1+X}$ on $\widehat{\mathbb{G}}_m$ with the parameter $X = u - 1$. Hence $\widehat{\phi}$ is given by the power series $t = \exp_{\widehat{E}} \circ \log(1+X) - 1 \in \mathbb{Z}_p[[X]]$. From now we identify $\widehat{\mathbb{G}}_m$ with $\widehat{E}$ by $\widehat{\phi}$. In particular, we regard $c_n \in \widehat{\mathbb{G}}_m(\mathfrak{m}_n)$ in the previous section as an element of $\widehat{E}(\mathfrak{m}_n)$.

Let $T = T_pE$ be the p-adic Tate module of E and $V = T \otimes \mathbb{Q}_p$. The cup product induces a non-degenerate pairing of Galois cohomology groups

$$(\ ,\ )_{E,n} :\ H^1(k_n, T) \times H^1(k_n, T^*(1)) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

If there is no fear of confusion, we write $(\ ,\ )_{E,n}$ simply as $(\ ,\ )_E$. By the Kummer map, we regard $\widehat{E}(\mathfrak{m}_n)$ as a subgroup of $H^1(k_n, T)$. Then we define a morphism $\mathrm{Col}_n : H^1(k_n, T^*(1)) \to \mathbb{Z}_p[\Gamma_n]$ by

$$z \quad \longmapsto \sum_{\sigma\in\Gamma_n} (c_n^\sigma,\ z)_{E,n}\, \sigma.$$

This morphism is compatible with the natural Galois action and since the sequence $(c_n)_n$ is norm compatible, Col_n is also compatible for n with respect to the corestrictions and the natural projections. We define the Coleman map

$$\mathrm{Col} :\quad \varprojlim_n H^1(k_n, T^*(1)) \ \longrightarrow\ \Lambda = \mathbb{Z}_p[[\Gamma]]$$

as the projective limit of Col_n over all n.

We recall the dual exponential map. For every n let $\tan(E/k_n)$ denote the tangent space of E/k_n at the origin, and consider the Lie group exponential map

$$\exp_{E,n} :\ \tan(E/k_n) \to E(k_n) \otimes \mathbb{Q}_p.$$

The cotangent space $\mathrm{cotan}(E/k_n)$ is generated by the invariant differential ω_E over k_n, and we let ω_E^* be the corresponding dual basis of $\tan(E/k_n)$. Then there is a dual exponential map

$$\exp_{E,n}^* :\ H^1(k_n, V^*(1)) \longrightarrow \mathrm{cotan}(E/k_n) = k_n\, \omega_E,$$

which has a property

$$(x, z)_{E,n} = \mathrm{Tr}_{k_n/\mathbb{Q}_p} \log_{\widehat{E}}(x)\ \exp_{\omega_E,n}^*(z)$$

for every $x \in \hat{E}(\mathfrak{m}_n)$ and $z \in H^1(k_n, V^*(1))$. Here $\exp_{\omega_E,n}^* = \omega_E^* \circ \exp_{E,n}^*$. If there is no fear of confusion, we write $\exp_{\omega_E,n}^*(z)$ as $\exp_{\omega_E}^*(z)$. Then using the identification $\widehat{\phi} : \widehat{\mathbb{G}}_m \cong \widehat{E}$, the morphism Col_n is described in terms of the dual exponential map as follows.

$$\begin{aligned}\mathrm{Col}_n(z) &= \sum_{\sigma\in\Gamma_n} (c_n^\sigma, z)_{E,n}\, \sigma \\ &= \sum_{\sigma\in\Gamma_n} (\,\mathrm{Tr}_{k_n/\mathbb{Q}_p} \log_p(d_n^\sigma)\, \exp^*_{\omega_E}(z)\,)\, \sigma \\ &= \left(\sum_{\sigma\in\Gamma_n} \log_p(d_n^\sigma)\, \sigma\right) \left(\sum_{\sigma\in\Gamma_n} \exp^*_{\omega_E}(z^\sigma)\, \sigma^{-1}\right).\end{aligned}$$

Let G_n be the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ and let χ be a finite character of G_{n+1} of conductor p^{n+1} which is trivial on Δ. Then we have

$$\sum_{\sigma\in\Gamma_n} \log_p(d_n^\sigma)\, \chi(\sigma) = \begin{cases} \tau(\chi) & \text{if } \chi \text{ is non-trivial,} \\ 0 & \text{otherwise} \end{cases}$$

where $\tau(\chi)$ is the Gauss sum $\sum_{\sigma\in G_{n+1}} \chi(\sigma)\, \zeta_{p^{n+1}}^\sigma$. Hence for $\chi \neq 1$, we have

$$\chi \circ \mathrm{Col}(z) = \tau(\chi) \sum_{\sigma\in\Gamma_n} \exp^*_{\omega_E}(z^\sigma)\, \chi(\sigma)^{-1}.$$

Kato showed that there exists an element $z^{\mathrm{Kato}} \in \varprojlim_n H^1(k_n, T^*(1))$ such that

$$\sum_{\sigma\in\Gamma_n} \exp^*_{\omega_E}((z^{\mathrm{Kato}})^\sigma)\, \chi(\sigma)^{-1} = e_p(\overline{\chi}) \frac{L(E, \overline{\chi}, 1)}{\Omega_E^+}$$

where $e_p(\chi)$ is the value at $s = 1$ of the p-Euler factor of $L(E, \chi, s)$, that is, $e_p(\chi) = 1$ if χ is non-trivial and $e_p(\chi) = \left(1 - \frac{1}{p}\right)$ if χ is trivial. (See [Ka], Theorem 12.5.) Hence we have

$$\chi \circ \mathrm{Col}(z^{\mathrm{Kato}}) = \tau(\chi) \frac{L(E, \overline{\chi}, 1)}{\Omega_E^+}$$

if χ is non-trivial. The p-adic L-function $L_p(E, s)$ is written of the form

$$L_p(E, s) = \mathcal{L}_{p,\gamma}(E, \kappa(\gamma)^{s-1} - 1)$$

for some power series $\mathcal{L}_{p,\gamma}(E, X) \in \mathbb{Z}_p[[X]]$. If we identify $\Lambda = \mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[X]]$ by sending $\gamma \mapsto 1 + X$, then it satisfies an interpolation formula

$$\chi \circ \mathcal{L}_{p,\gamma}(E, X) = \tau(\chi) \frac{L(E, \overline{\chi}, 1)}{\Omega_E^+}.$$

Since an element of Λ has only finitely many zeros, we conclude that

$$\mathrm{Col}(z^{\mathrm{Kato}})(X) = \mathcal{L}_{p,\gamma}(E, X).$$

Here we denote $\mathrm{Col}(z^{\mathrm{Kato}})$ by $\mathrm{Col}(z^{\mathrm{Kato}})(X)$ to emphasis that we regard $\mathrm{Col}(z^{\mathrm{kato}})$ as a power series in $\mathbb{Z}_p[[X]]$. Note that we have $\mathbf{1} \circ \mathrm{Col}(z) = 0$ for the trivial character $\mathbf{1}$, or $\mathrm{Col}(z)(0) = 0$, namely, any Coleman power series $\mathrm{Col}(z)(X)$ for the Tate curve has a trivial zero at $X = 0$.

4. The first derivative of the Coleman map.

We compute the first derivative of the Coleman map $\mathrm{Col}(z)(X)$. By Tate's uniformization, there is an exact sequence of local Galois representations

$$0 \to T_1 \to T \to T_2 \to 0 \tag{1}$$

where $T_1 = T_p\widehat{E} \cong \mathbb{Z}_p(1)$ and $T_2 \cong \mathbb{Z}_p$. The cup product induces a non-degenerate paring

$$H^1(k_n, T_1) \times H^1(k_n, T_1^*(1)) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

With the identification by $\widehat{\phi} : T_1 \cong \mathbb{Z}_p(1)$, this is in fact the cup product pairing of $\mathbb{G}_m$

$$(\ ,\ )_{\mathbb{G}_m,n} :\ H^1(k_n, \mathbb{Z}_p(1)) \times H^1(k_n, \mathbb{Z}_p) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

If there is no fear of confusion, we write $(\ ,\ )_{\mathbb{G}_m,n}$ simply as $(\ ,\ )_{\mathbb{G}_m}$. Since $c_n \in \widehat{E}(k_n) \subset H^1(k_n, T_1)$, we have

$$(c_n^\sigma,\ z)_{E,n} = (d_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}$$

for $z \in H^1(k_n, T^*(1))$ where π is the morphism induced by the projection $T^*(1) \to T_1^*(1)$. Tate's uniformization ϕ also induces a commutative diagram

$$\begin{tikzcd}
H^1(k_n, V^*(1)) \arrow[r, "\exp_E^*"] \arrow[d, "\pi"'] & k_n\,\omega_E \arrow[r, "\omega_E^*"] & k_n \arrow[d] \\
H^1(k_n, V_1^*(1)) \arrow[r, "\exp_{\mathbb{G}_m}^*"] & k_n\,\omega_{\mathbb{G}_m} \arrow[r, "\omega_{\mathbb{G}_m}^*"] & k_n
\end{tikzcd}$$

where $\omega_{\mathbb{G}_m}$ is the invariant differential of $\mathbb{G}_m$ which is $\frac{dX}{1+X}$ on $\widehat{\mathbb{G}}_m$, and $\omega_{\mathbb{G}_m}^*$ is the dual basis for $\omega_{\mathbb{G}_m}$. We also put $\exp_{\omega_{\mathbb{G}_m}}^* = \omega_{\mathbb{G}_m}^* \circ \exp_{\mathbb{G}_m}^*$.

Now we compute the derivative. With the same notation as the previous section, we have

$$\begin{aligned}
\mathrm{Col}_n(z) &= \sum_{\sigma\in\Gamma_n} (c_n^\sigma,\ z)_{E,n}\,\sigma = \sum_{\sigma\in\Gamma_n} (d_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma \\
&= \sum_{\sigma\in\Gamma_n} ((x_n^\gamma/x_n)^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma \\
&= (\gamma^{-1}-1) \sum_{\sigma\in\Gamma_n} (x_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma.
\end{aligned}$$

Therefore by the identification $\mathbb{Z}_p[X]/((X+1)^{p^n}-1) \cong \mathbb{Z}_p[\Gamma_n]$, $X \mapsto \gamma - 1$, we have

$$\frac{\mathrm{Col}(z)(X)}{X} \ \equiv\ -\frac{1}{\gamma} \sum_{\sigma\in\Gamma_n} (x_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma \quad \mathrm{mod}\ \frac{(X+1)^{p^n}-1}{X}.$$

Hence

$$\mathrm{Col}(z)'(0)\ \equiv\ -\,(\mathrm{N}x_n,\ \pi(z))_{\mathbb{G}_m,0} \quad \mathrm{mod}\ p^n.$$

Since $\mathrm{N}x_n = p^{e_n}\mathrm{N}(u_n) = p^{e_n}$ and by Proposition 2.2, we have

$$(\mathrm{N}x_n,\, \pi(z))_{\mathbb{G}_m} = e_n\,(p,\, \pi(z))_{\mathbb{G}_m} \equiv \frac{p}{(p-1)\log_p \kappa(\gamma)}\,(p,\, \pi(z))_{\mathbb{G}_m} \mod p^n.$$

Taking limit for n, we have that

$$\mathrm{Col}(z)'(0) = -\frac{p}{(p-1)\log_p \kappa(\gamma)}\,(p,\, \pi(z))_{\mathbb{G}_m}. \tag{2}$$

Next we compute $(p,\, \pi(z))_{\mathbb{G}_m}$. We consider the exact sequence

$$H^1(\mathbb{Q}_p, T^*(1)) \xrightarrow{\ \pi\ } H^1(\mathbb{Q}_p, T_1^*(1)) \xrightarrow{\ \delta_2\ } H^2(\mathbb{Q}_p, T_2^*(1))$$

induced by (1), and a diagram

$$\begin{tikzcd}
H^1(\mathbb{Q}_p, T_1) \times H^1(\mathbb{Q}_p, T_1^*(1)) \arrow[r, "(\,,\,)_{\mathbb{G}_m}"] \arrow[d, phantom, ""] & H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) = \mathbb{Z}_p \arrow[d] \\
H^0(\mathbb{Q}_p, T_2) \times H^2(\mathbb{Q}_p, T_2^*(1)) \arrow[u, "\delta_1"] \arrow[r, "(\,,\,)_{\mathbb{G}_m}"] & H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) = \mathbb{Z}_p.
\end{tikzcd}$$

$$\delta_1 \uparrow \quad \delta_2 \downarrow$$

It is straightforward to see that the connecting morphism δ_1 is given by

$$H^0(\mathbb{Q}_p, T_2) = \mathbb{Z}_p \;\to\; \mathbb{Q}_p^\times \otimes \mathbb{Z}_p = H^1(\mathbb{Q}_p, T_1), \quad 1 \;\mapsto\; q_E \otimes 1.$$

Hence for $w \in H^1(\mathbb{Q}_p, T_1^*(1))$, we have

$$(q_E \otimes 1,\, w)_{\mathbb{G}_m} = (\delta_1(1),\, w)_{\mathbb{G}_m} = (1,\, \delta_2(w))_{\mathbb{G}_m}.$$

In particular, if w comes from $H^1(\mathbb{Q}_p, T^*(1))$, namely, it is of the form $\pi(z)$, then

$$(q_E \otimes 1,\, w)_{\mathbb{G}_m} = (q_E \otimes 1,\, \pi(z))_{\mathbb{G}_m} = (1,\, \delta_2 \circ \pi(z))_{\mathbb{G}_m} = 0. \tag{3}$$

On the other hand, if we put $q_E = p^{\mathrm{ord}_p(q_E)}\,\rho\, u_q$ where $\rho \in \mu_{p-1}$ and $u_q \in 1 + p\mathbb{Z}_p$, we have

$$\begin{aligned}
(q_E \otimes 1,\, w)_{\mathbb{G}_m} &= \mathrm{ord}_p(q_E)\,(p,\, w)_{\mathbb{G}_m} + (u_q,\, w)_{\mathbb{G}_m} && (4)\\
&= \mathrm{ord}_p(q_E)\,(p,\, w)_{\mathbb{G}_m} + \log_p(u_q)\,\exp^*_{\omega_{\mathbb{G}_m}}(w). && (5)
\end{aligned}$$

Hence by (3) and (5) we have

$$(p,\, \pi(z))_{\mathbb{G}_m} = -\frac{\log_p(u_q)}{\mathrm{ord}_p(q_E)}\exp^*_{\omega_{\mathbb{G}_m}}(\pi(z)) = -\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\exp^*_{\omega_E}(z). \tag{6}$$

Combining (2) and (6), we obtain

Theorem 4.1. *For $z \in \varprojlim_n H^1(k_n, T^*(1))$, the first derivative of the Coleman map* $\mathrm{Col}(z)$ *is given by*

$$\frac{d}{dX}\mathrm{Col}(z)(X)\,|_{X=0} = \frac{p}{(p-1)\log_p \kappa(\gamma)}\,\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\exp^*_{\omega_E}(z).$$

Now if $E/\mathbb{Q}$ has split multiplicative reduction at p, then we may assume that E is locally the Tate curve for some $q_E \in \mathbb{Q}_p^\times$. We apply the above formula to Kato's element $z = z^{\mathrm{Kato}}$. Since $\exp^*_{\omega_E}(z^{\mathrm{Kato}}) = (1 - \frac{1}{p})\frac{L(E,1)}{\Omega_E^+}$, we have

Corollary 4.2. *Let $\mathcal{L}_{p,\gamma}(E,X)$ be the power series in $\mathbb{Z}_p[[X]]$ such that $L_p(E,s) = \mathcal{L}_{p,\gamma}(E,\kappa(\gamma)^{s-1}-1)$. Then*

$$\frac{d}{dX}\mathcal{L}_{p,\gamma}(E,X)\mid_{X=0} = \frac{1}{\log_p \kappa(\gamma)}\,\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\,\frac{L(E,1)}{\Omega_E^+},$$

or

$$\frac{d}{ds}L_p(E,s)\mid_{s=1} = \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\,\frac{L(E,1)}{\Omega_E^+}.$$

References

[C] P. Colmez, La conjecture de Birch et Swinnerton-Dyer p-adique, Séminaire Bourbaki - Volume 2002/2003 - Exposés 909-923 Astérisque 294 (2004)

[H] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970), 213–246.

[GS] R. Greenberg and G. Stevens, p-adic L-functions and p-adic periods of modular forms, Invent. Math. 111 (1993), 2, 407-447.

[Ka] K. Kato, P-adic Hodge theory and values of zeta funcions of modular forms, Cohomologies p-adiques et applications arithmétiques (III), Astérisque 295 (2004), 117-290.

[KKT] K. Kato, M. Kurihara, T. Tsuji, Local Iwasawa theory of Perrin-Riou and syntomic complexes, preprint 1996.

[Ku] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent.Math. 149 (2002), 195-224.

[Ko] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. math. 152 (2003) 1, 1-36.

[MTT] B. Mazur, J. Tate, J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. math. 84 (1986) 1-48.

[R] K. Rubin, Euler systems and modular elliptic curves. Galois representations in arithmetic algebraic geometry (Durham, 1996), 351–367, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[S1] J. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics 106, Springer-Verlag.

[S2] J. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics 151, Springer-Verlag.

Shinichi Kobayashi
Graduate School of Mathematics
Nagoya University
Furo-cho Chikusa-ku
Nagoya 464-8602
Japan
shinichi@math.nagoya-u.ac.jp

Computation of p-Adic Heights and Log Convergence

In celebration of John Coates' 60th birthday

Barry Mazur, William Stein[1], John Tate

Received: September 9, 2005
Revised: May 2, 2006

Abstract. This paper is about computational and theoretical questions regarding p-adic height pairings on elliptic curves over a global field K. The main stumbling block to computing them efficiently is in calculating, for each of the completions K_v at the places v of K dividing p, a *single quantity*: the value of the p-adic modular form $\mathbf{E}_2$ associated to the elliptic curve. Thanks to the work of Dwork, Katz, Kedlaya, Lauder and Monsky-Washnitzer we offer an efficient algorithm for computing these quantities, i.e., for computing the value of $\mathbf{E}_2$ of an elliptic curve. We also discuss the p-adic convergence rate of canonical expansions of the p-adic modular form $\mathbf{E}_2$ on the Hasse domain. In particular, we introduce a new notion of log convergence and prove that $\mathbf{E}_2$ is log convergent.

2000 Mathematics Subject Classification: 11F33, 11Y40, 11G50
Keywords and Phrases: p-adic heights, algorithms, p-adic modular forms, Eisenstein series, sigma-functions

1 Introduction

Let p be an odd prime number, and E an elliptic curve over a global field K that has good ordinary reduction at p. Let L be any (infinite degree) Galois extension with a continuous injective homomorphism ρ of its Galois group to

[1] This material is based upon work supported by the National Science Foundation under Grant No. 0555776.

$\mathbf{Q}_p$. To the data (E, K, ρ), one associates[2] a canonical (bilinear, symmetric) (p-adic) height pairing

$$(\ ,\ )_\rho : E(K) \times E(K) \longrightarrow \mathbf{Q}_p.$$

Such pairings are of great interest for the arithmetic of E over K, and they arise specifically in p-adic analogues of the Birch and Swinnerton-Dyer conjecture.[3]

The goal of this paper is to discuss some computational questions regarding p-adic height pairings. The main stumbling block to computing them efficiently is in calculating, for each of the completions K_v at the places v of K dividing p, the value of the p-adic modular form $\mathbf{E}_2$ associated to the elliptic curve with a chosen Weierstrass form of good reduction over K_v.

We shall offer an algorithm for computing these quantities, i.e., for computing the value of $\mathbf{E}_2$ of an elliptic curve (that builds on the works of Katz and Kedlaya listed in our bibliography) and we also discuss the p-adic convergence rate of canonical expansions of the p-adic modular form $\mathbf{E}_2$ on the Hasse domain, where for $p \geq 5$ we view $\mathbf{E}_2$ as an infinite sum of classical modular forms divided by powers of the (classical) modular form $\mathbf{E}_{p-1}$, while for $p \leq 5$ we view it as a sum of classical modular forms divided by powers of $\mathbf{E}_4$.

We were led to our fast method of computing $\mathbf{E}_2$ by our realization that the more naive methods, of computing it by integrality or by approximations to it as function on the Hasse domain, were not practical, because the convergence is "logarithmic" in the sense that the nth convergent gives only an accuracy of $\log_p(n)$. We make this notion of log convergence precise in Part II, where we also prove that $\mathbf{E}_2$ is log convergent.

The reason why this constant $\mathbf{E}_2$ enters the calculation is because it is needed for the computation of the p-adic sigma function [MT91], which in turn is the critical element in the formulas for height pairings.

For example, let us consider the *cyclotomic* p-adic height pairing in the special case where $K = \mathbf{Q}$ and $p \geq 5$.

If $G_{\mathbf{Q}}$ is the Galois group of an algebraic closure of $\mathbf{Q}$ over $\mathbf{Q}$, we have the natural surjective continuous homomorphism $\chi : G_{\mathbf{Q}} \to \mathbf{Z}_p^*$ pinned down by the standard formula $g(\zeta) = \zeta^{\chi(g)}$ where $g \in G_{\mathbf{Q}}$ and ζ is any p-power root of unity. The p-adic logarithm $\log_p : \mathbf{Q}_p^* \to (\mathbf{Q}_p, +)$ is the unique group homomorphism with $\log_p(p) = 0$ that extends the homomorphism $\log_p : 1 + p\mathbf{Z}_p \to \mathbf{Q}_p$ defined by the usual power series of $\log(x)$ about 1. Explicitly, if $x \in \mathbf{Q}_p^*$, then

$$\log_p(x) = \frac{1}{p-1} \cdot \log_p(u^{p-1}),$$

where $u = p^{-\operatorname{ord}_p(x)} \cdot x$ is the unit part of x, and the usual series for log converges at u^{p-1}.

[2] See [MT83], [Sch82] [Sch85], [Zar90], [Col91], [Nek93], [Pla94], [IW03], and [Bes04].

[3] See [Sch82], [Sch85] [MT83], [MT87], [PR03a]. See also the important recent work of Jan Nekovář [Nek03].

The composition $(\frac{1}{p} \cdot \log_p) \circ \chi$ is a cyclotomic linear functional $G_{\mathbf{Q}} \to \mathbf{Q}_p$ which, in the body of our text, will be dealt with (thanks to class field theory) as the idele class functional that we denote $\rho_{\mathbf{Q}}^{\text{cycl}}$.

Let $\mathcal{E}$ denote the Néron model of E over $\mathbf{Z}$. Let $P \in E(\mathbf{Q})$ be a non-torsion point that reduces to $0 \in E(\mathbf{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbf{F}_\ell}$ at all primes ℓ of bad reduction for E. Because $\mathbf{Z}$ is a unique factorization domain, any nonzero point $P = (x(P), y(P)) \in E(\mathbf{Q})$ can be written uniquely in the form $(a/d^2, b/d^3)$, where $a, b, d \in \mathbf{Z}$, $\gcd(a, d) = \gcd(b, d) = 1$, and $d > 0$. The function $d(P)$ assigns to P this square root d of the denominator of $x(P)$.

Here is the formula for the *cyclotomic* p-adic height of P, i.e., the value of

$$h_p(P) := -\frac{1}{2}(P, P)_p \in \mathbf{Q}_p$$

where $(\ ,\ )_p$ is the height pairing attached to $G_{\mathbf{Q}} \to \mathbf{Q}_p$, the cyclotomic linear functional described above:

$$h_p(P) = \frac{1}{p} \cdot \log_p\left(\frac{\sigma(P)}{d(P)}\right) \in \mathbf{Q}_p. \tag{1.1}$$

Here $\sigma = \sigma_p$ is the p-adic sigma function of [MT91] associated to the pair (E, ω). The σ-function depends only on (E, ω) and not on a choice of Weierstrass equation, and behaves like a modular form of weight -1, that is $\sigma_{E,c\omega} = c \cdot \sigma_{E,\omega}$. It is "quadratic" the sense that for any $m \in \mathbf{Z}$ and point Q in the formal group $E^f(\overline{\mathbf{Z}}_p)$, we have

$$\sigma(mQ) = \sigma(Q)^{m^2} \cdot f_m(Q), \tag{1.2}$$

where f_m is the mth division polynomial of E relative to ω (as in [MT91, App. 1]). The σ-function is "bilinear" in that for any $P, Q \in E^f(\mathbf{Z}_p)$, we have

$$\frac{\sigma(P - Q) \cdot \sigma(P + Q)}{\sigma^2(P) \cdot \sigma^2(Q)} = x(Q) - x(P). \tag{1.3}$$

See [MT91, Thm. 3.1] for proofs of the above properties of σ.

The height function h_p of (1.1) extends uniquely to a function on the full Mordell-Weil group $E(\mathbf{Q})$ that satisfies $h_p(nQ) = n^2 h_p(Q)$ for all integers n and $Q \in E(\mathbf{Q})$. For $P, Q \in E(\mathbf{Q})$, setting

$$(P, Q)_p = h_p(P) + h_p(Q) - h_p(P + Q),$$

we obtain a pairing on $E(\mathbf{Q})$. The *p-adic regulator* of E is the discriminant of the induced pairing on $E(\mathbf{Q})_{/\,\text{tor}}$ (well defined up to sign), and we have the following standard conjecture about this height pairing.

Conjecture 1.1. *The cyclotomic height pairing $(\ ,\ )_p$ is nondegenerate; equivalently, the p-adic regulator is nonzero.*

Remark 1.2. Height pairings attached to other p-adic linear functionals can be degenerate; in fact, given an elliptic curve defined over $\mathbf{Q}$ with good ordinary reduction at p, and K a quadratic imaginary field over which the Mordell-Weil group $E(K)$ is of odd rank, the p-adic anticyclotomic height pairing for E over K is *always* degenerate.

The p-adic σ function is the most mysterious quantity in (1.1). There are many ways to define σ, e.g., [MT91] contains 11 different characterizations of σ! We now describe a characterization that leads directly to an algorithm (see Algorithm 3.3) to compute $\sigma(t)$. Let

$$x(t) = \frac{1}{t^2} + \cdots \in \mathbf{Z}_p((t)) \tag{1.4}$$

be the formal power series that expresses x in terms of the local parameter $t = -x/y$ at infinity. The following theorem, which is proved in [MT91], uniquely determines σ and c.

Theorem 1.3. *There is exactly one odd function $\sigma(t) = t + \cdots \in t\mathbf{Z}_p[[t]]$ and constant $c \in \mathbf{Z}_p$ that together satisfy the differential equation*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right), \tag{1.5}$$

where ω is the invariant differential $dx/(2y + a_1x + a_3)$ associated with our chosen Weierstrass equation for E.

Remark 1.4. The condition that σ is odd and that the coefficient of t is 1 are essential.

In (1.1), by $\sigma(P)$ we mean $\sigma(-x/y)$, where $P = (x, y)$. We have thus given a complete definition of $h_p(Q)$ for any point $Q \in E(\mathbf{Q})$ and a prime $p \geq 5$ of good ordinary reduction for E.

1.1 The p-adic σ-function

The differential equation (1.5) leads to a slow algorithm to compute $\sigma(t)$ to any desired precision. This is Algorithm 3.3 below, which we now summarize. If we expand (1.5), we can view c as a formal variable and solve for $\sigma(t)$ as a power series with coefficients that are polynomials in c. Each coefficient of $\sigma(t)$ must be in $\mathbf{Z}_p$, so we obtain conditions on c modulo powers of p. Taking these together for many coefficients must eventually yield enough information to compute $c \pmod{p^n}$, for a given n, hence $\sigma(t) \pmod{p^n}$. This integrality algorithm is hopelessly slow in general.

Another approach to computing σ is to observe that, up to a constant, c is closely related to the value of a certain p-adic modular form. More precisely, suppose that E is given by a (not necessarily minimal) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.6}$$

and let $\omega = dx/(2y + a_1x + a_3)$. Let $x(t)$ be as in (1.4). Then the series

$$\wp(t) = x(t) + \frac{a_1^2 + 4a_2}{12} \in \mathbf{Q}((t)) \tag{1.7}$$

satisfies $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$. In [MT91] we find[4] that

$$x(t) + c = \wp(t) - \frac{1}{12} \cdot \mathbf{E}_2(E, \omega), \tag{1.8}$$

where $\mathbf{E}_2(E, \omega)$ is the value of the Katz p-adic weight 2 Eisenstein series at (E, ω), and the equality is of elements of $\mathbf{Q}_p((t))$. Using the definition of $\wp(t)$ and solving for c, we find that

$$c = \frac{a_1^2 + 4a_2}{12} - \frac{1}{12}\mathbf{E}_2(E, \omega). \tag{1.9}$$

Thus computing c is equivalent to computing the p-adic number $\mathbf{E}_2(E, \omega)$. Having computed c to some precision, we then solve for σ in (1.5) using Algorithm 3.1 below.

1.2 p-adic analogues of the Birch and Swinnerton-Dyer conjecture

One motivation for this paper is to provide tools for doing computations in support of p-adic analogues of the BSD conjectures (see [MTT86]), especially when $E/\mathbf{Q}$ has rank at least 2. For example, in [PR03b], Perrin-Riou uses her results about the p-adic BSD conjecture in the supersingular case to prove that $Ш(E/\mathbf{Q})[p] = 0$ for certain p and elliptic curves E of rank > 1, for which the work of Kolyvagin and Kato does not apply.

Another motivation for this work comes from the study of the fine structure of Selmer modules. Let K be a number field and Λ the p-adic integral group ring of the Galois group of the maximal $\mathbf{Z}_p$-power extension of K. Making use of fundamental results of Nekovář [Nek03] and of Greenberg [Gre03] one can construct (see [RM05]) for certain elliptic curves defined over K, a skew-Hermitian matrix with coefficients in Λ from which one can read off a free Λ-resolution of the canonical Selmer Λ-module of the elliptic curve in question over K. To compute the entries of this matrix modulo the square of the augmentation ideal in Λ one must know *all* the p-adic height pairings of the elliptic curve over K. Fast algorithms for doing this provide us with an important first stage in the computation of free Λ-resolutions of Selmer Λ-modules.

The paper [GJP$^+$05] is about computational verification of the full Birch and Swinnerton-Dyer conjecture for specific elliptic curves E. There are many cases in which the rank of E is 1 and the upper bound on $\#Ш(E/\mathbf{Q})$ coming from Kolyvagin's Euler system is divisible by a prime $p \geq 5$ that also divides a Tamagawa number. In such cases, theorems of Kolyvagin and Kato combined

[4] There is a sign error in [MT91].

with explicit computation do not give a sufficiently sharp upper bound on $\#Ш(E/\mathbf{Q})$. However, it should be possible in these cases to compute p-adic heights and p-adic L-functions, and use results of Kato, Schneider, and others to obtain better bounds on $\#Ш(E/\mathbf{Q})$. Wuthrich and the second author (Stein) are writing a paper on this.

1.3 Sample computations

In Section 4 we illustrate our algorithms with curves of ranks $1, 2, 3, 4$ and 5, and two twists of $X_0(11)$ of rank 2.

Acknowledgement: It is a pleasure to thank Nick Katz for feedback that led to Section 3. We would also like to thank Mike Harrison for discussions about his implementation of Kedlaya's algorithm in Magma, Kiran Kedlaya for conversations about his algorithm, Christian Wuthrich for feedback about computing p-adic heights, Alan Lauder for discussions about computing $\mathbf{E}_2$ in families, and Fernando Gouvea for remarks about non-overconvergence of $\mathbf{E}_2$. We would also like to thank all of the above people for comments on early drafts of the paper. Finally, we thank Jean-Pierre Serre for the proof of Lemma 6.6.

Part I
Heights, σ-functions, and $\mathbf{E}_2$

2 The Formulas

In this section we give formulas for the p-adic height pairing in terms of the σ function. We have already done this over $\mathbf{Q}$ in Section 1. Let p be an (odd) prime number, K a number field, and E an elliptic curve over K with good ordinary reduction at all places of K above p. For any non-archimedean place w of K, let k_w denote the residue class field at w.

2.1 General global height pairings

By the *idele class* $\mathbf{Q}_p$*-vector space* of K let us mean

$$I(K) = \mathbf{Q}_p \otimes_{\mathbf{Z}} \left\{ \mathbf{A}_K^*/\left(K^* \cdot \prod_{v \nmid p} \mathcal{O}_v^* \cdot \mathrm{C} \right) \right\},$$

where $\mathbf{A}_K^*$ is the group of ideles of K, and C denotes its connected component containing the identity. Class field theory gives us an identification $I(K) = \Gamma(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $\Gamma(K)$ is the Galois group of the maximal $\mathbf{Z}_p$-power extension of K. For every (nonarchimedean) place v of K, there is a natural homomorphism $\iota_v : K_v^* \to I(K)$.

For K-rational points $\alpha, \beta \in E(K)$ we want to give explicit formulas for an element that we might call the "universal" p-adic height pairing of α and β; denote it $(\alpha, \beta) \in I(K)$. If $\rho : I(K) \to \mathbf{Q}_p$ is any linear functional, then the *ρ-height pairing* is a symmetric bilinear pairing

$$(\ , \ )_\rho : E(K) \times E(K) \to \mathbf{Q}_p,$$

defined as the composition of the universal pairing with the linear functional ρ:

$$(\alpha, \beta)_\rho = \rho(\alpha, \beta) \in \mathbf{Q}_p.$$

We define the *ρ-height* of a point $\alpha \in E(K)$ by:

$$h_\rho(\alpha) = -\frac{1}{2}(\alpha, \alpha)_\rho \in \mathbf{Q}_p.$$

Of course, any such (nontrivial) linear functional ρ uniquely determines a $\mathbf{Z}_p$-extension, and we sometimes refer to the ρ-height pairing in terms of this $\mathbf{Z}_p$-extension. E.g., if ρ cuts out the cyclotomic $\mathbf{Z}_p$-extension, then the ρ-height pairing is a normalization of the *cyclotomic height pairing* that has, for the rational field, already been discussed in the introduction.

If K is quadratic imaginary, and ρ is the anti-cyclotomic linear functional, meaning that it is the unique linear functional (up to normalization) that has the property that $\rho(\bar{x}) = -\rho(x)$ where $\bar{x}$ is the complex conjugate of x, then we will be presently obtaining explicit formulas for this anti-cyclotomic height pairing.

We will obtain a formula for $(\alpha, \beta) \in I(K)$ by defining, for every nonarchimedean place, v, of K a "local height pairing," $(\alpha, \beta)_v \in K_v^*$. These local pairings will be very sensitive to some auxiliary choices we make along the way, but for a fixed α and β the local height pairings $(\alpha, \beta)_v$ will vanish for all but finitely many places v; the global height is the sum of the local ones and will be independent of all the choices we have made.

2.2 Good representations

Let $\alpha, \beta \in E(K)$. By a *good representation* of the pair α, β we mean that we are given a four-tuple of points (P, Q, R, S) in $E(K)$ (or, perhaps, in $E(K')$ where K'/K is a number field extension of K) such that

- α is the divisor class of the divisor $[P] - [Q]$ of E, and β is the divisor class of the divisor $[R] - [S]$,
- P, Q, R, S are four distinct points,
- for each $v \mid p$ all four points P, Q, R, S specialize to the same point on the fiber at v of the Néron model of E.
- at all places v of K the points P, Q, R, S specialize to the same component of the fiber at v of the Néron model of E.

We will show how to erase these special assumptions later, but for now, let us assume all this, fix a choice of a good representation, P, Q, R, S, of (α, β) as above, and give the formulas in this case.

2.3 Local height pairings when $v \mid p$

Let σ_v be the canonical p-adic σ-function attached to the elliptic curve E over K_v given in Weierstrass form. We may view σ_v as a mapping from $E_1(K_v)$ to K_v^*, where $E_1(K_v)$ is the kernel of the reduction map $E(K_v) \to E(k_v)$, and $E(k_v)$ denotes the group of points on the reduction of E modulo v. Define $(\alpha, \beta)_v \in K_v^*$ by the formula,

$$(\alpha, \beta)_v = \frac{\sigma_v(P-R)\sigma_v(Q-S)}{\sigma_v(P-S)\sigma_v(Q-R)} \ \in \ K_v^*.$$

The dependence of σ on the Weierstrass equation is through the differential $\omega = dx/(2y + a_1x + a_3)$, and $\sigma_{c\omega} = c\sigma_\omega$, so this depends upon the choice of P, Q, R, S, but does not depend on the choice of Weierstrass equation for E.

2.4 Local height pairings when $v \nmid p$

First let x denote the "x-coordinate" in some minimal Weierstrass model for A at v. Define for a point T in $E(K_v)$ the rational number $\lambda_v(T)$ to be *zero* if $x(T) \in \mathcal{O}_v$, and to be $-\frac{1}{2}v(x(T))$ if $x(T) \notin \mathcal{O}_v$.

Next, choose a uniformizer π_v of K_v and define:

$$\tilde{\sigma}_v(T) = \pi_v^{\lambda_v(T)},$$

the square of which is in K_v^*. We think of $\tilde{\sigma}_v$ as a rough replacement for σ_v in the following sense. The v-adic valuation of $\tilde{\sigma}_v$ is the same as v-adic valuation of the v-adic sigma function (if such a function is definable at v) and therefore, even if σ_v cannot be defined, $\tilde{\sigma}_v$ is a perfectly serviceable substitute at places v at which our p-adic idele class functionals ρ are necessarily unramified, and therefore sensitive only to the v-adic valuation.

For $v \nmid p$, put:

$$(\alpha, \beta)_v = \frac{\tilde{\sigma}_v(P-R)\tilde{\sigma}_v(Q-S)}{\tilde{\sigma}_v(P-S)\tilde{\sigma}_v(Q-R)}.$$

The square of this is in K_v^*. However, note that $\pi_v^{\lambda_v(T)}$ really means $\sqrt{\pi_v}^{2\lambda_v(T)}$, for a fixed choice of $\sqrt{\pi_v}$ and that the definition of $(\alpha, \beta)_v$ is independent of the choice of square root and therefore that $(\alpha, \beta)_v$, not only its square, is in K_v^*.

Our local height $(\alpha, \beta)_v$, depends upon the choice of P, Q, R, S and of the uniformizer π_v.

2.5 How the local heights change, when we change our choice of divisors

Let $\beta \in E(K)$ be represented by both $[R]-[S]$ and $[R']-[S']$. Let $\alpha \in E(K)$ be represented by $[P]-[Q]$. Moreover let both four-tuples P, Q, R, S and P, Q, R', S' satisfy the *good representation* hypothesis described at the beginning of Section 2.2. Since, by hypothesis, $[R]-[S]-[R']+[S']$ is linearly equivalent to zero, there is a rational function f whose divisor of zeroes and poles is

$$(f) = [R]-[S]-[R']+[S'].$$

If v is a nonarchimedean place of K define $(\alpha, \beta)_v$ to be as defined in the previous sections using the choice of four-tuple of points P, Q, R, S, (and of uniformizer π_v when $v \nmid p$). Similarly, define $(\alpha, \beta)'_v$ to be as defined in the previous sections using the choice of four-tuple of points P, Q, R', S', (and of uniformizer π_v when $v \nmid p$).

Proposition 2.1. *1. If $v \mid p$ then*

$$(\alpha, \beta)_v = \frac{f(P)}{f(Q)} \cdot (\alpha, \beta)'_v \ \in \ K_v^*.$$

2. If $v \nmid p$ then there is a unit u in the ring of integers of K_v such that

$$(\alpha, \beta)_v^2 = u \cdot \left(\frac{f(P)}{f(Q)} \cdot (\alpha, \beta)'_v \right)^2 \ \in \ K_v^*.$$

2.6 The global height pairing more generally

We can then form the sum of local terms to define the global height

$$(\alpha, \beta) = \quad \frac{1}{2} \sum_v \iota_v((\alpha, \beta)_v^2) \ \in \ I(K).$$

This definition is independent of any of the (good representation) choices P, Q, R, S and the π_v's made. It is independent of the choice of π_v's because the units in the ring of integers of K_v is in the kernel of ι_v if $v \nmid p$. It is independent of the choice of P, Q, R, S because by the previous proposition, a change (an allowable one, given our hypotheses) of P, Q, R, S changes the value of (α, β) by a factor that is a principal idele, which is sent to zero in $I(K)$.

What if, though, our choice of P, Q, R, S does *not* have the property that α and β reduce to the same point in the Néron fiber at v for all $v \mid p$, or land in the same connected component on each fiber of the Néron model? In this case the pair α, β do not have a *good representation.* But replacing α, β by $m \cdot \alpha, n \cdot \beta$ for sufficiently large positive integers m, n we can guarantee that the pair $m \cdot \alpha, n \cdot \beta$ does possess a good representation, and obtain formulas for (α, β) by:

$$(\alpha, \beta) = \frac{1}{mn}(m \cdot \alpha, n \cdot \beta).$$

Note in passing that to compute the global height pairing (α, α) for a non-torsion point $\alpha \in E(K)$ that specializes to 0 in the Néron fiber at v for all $v \mid p$, and that lives in the connected component containing the identity in all Néron fibers, we have quite a few natural choices of *good representations*. For example, for positive integers $m \neq n$, take

$$P = (m+1) \cdot \alpha;\ Q = m \cdot \alpha;\ R = (n+1) \cdot \alpha;\ S = n \cdot \alpha.$$

Then for any p-adic idele class functional ρ the global ρ-height pairing $(\alpha, \alpha)_\rho$ is given by

$$\sum_{v \mid p} \rho_v \left\{ \frac{\sigma_v((m-n)\alpha)^2}{\sigma_v((m-n+1)\alpha) \cdot \sigma_v((m-n-1)\alpha)} \right\} \\ + \sum_{v \nmid p} \rho_v \left\{ \frac{\tilde{\sigma}_v((m-n)\alpha)^2}{\tilde{\sigma}_v((m-n+1)\alpha) \cdot \tilde{\sigma}_v((m-n-1)\alpha)} \right\},$$

which simplifies to

$$(2(m-n)^2 - (m-n+1)^2 - (m-n-1)^2) \cdot \left\{ \sum_{v \mid p} \rho_v \sigma_v(\alpha) + \sum_{v \nmid p} \rho_v \tilde{\sigma}_v(\alpha) \right\}.$$

Since $(2(m-n)^2 - (m-n+1)^2 - (m-n-1)^2) = -2$ we have the formula

$$h_\rho(\alpha) = -\frac{1}{2}(\alpha, \alpha)_\rho$$

quoted earlier.

2.7 Formulas for the ρ-height

For each v, let σ_v be the canonical p-adic σ-function of E over K_v given in Weierstrass form. Suppose $P \in E(K)$ is a (non-torsion) point that reduces to 0 in $E(k_v)$ for each $v \mid p$, and to the connected component of all special fibers of the Néron model of E. Locally at each place w of K, we have a denominator $d_w(P)$, well defined up to units.

We have

$$h_\rho(P) = \sum_{v \mid p} \rho_v(\sigma_v(P)) - \sum_{w \nmid p} \rho_w(d_w(P)).$$

Note that h_ρ is quadratic because of the quadratic property of σ from (1.2), and the h_ρ-pairing is then visibly bilinear. See also property (1.3).

2.8 Cyclotomic p-adic heights

The idele class $\mathbf{Q}_p$-vector space $I(\mathbf{Q})$ attached to $\mathbf{Q}$ is canonically isomorphic to $\mathbf{Q}_p \otimes \mathbf{Z}_p^*$. Composition of this canonical isomorphism with the mapping $1 \times \frac{1}{p}\log_p$ induces an isomorphism

$$\rho_{\text{cycl}}^{\mathbf{Q}} : I(\mathbf{Q}) = \mathbf{Q}_p \otimes \mathbf{Z}_p^* \xrightarrow{\cong} \mathbf{Q}_p.$$

For K any number field, consider the homomorphism on idele class $\mathbf{Q}_p$-vector spaces induced by the norm $N_{K/\mathbf{Q}} : I(K) \to I(\mathbf{Q})$, and define

$$\rho_{\text{cycl}}^{K} : I(K) \to \mathbf{Q}_p$$

as the composition

$$\rho_{\text{cycl}}^{K} = \rho_{\text{cycl}}^{\mathbf{Q}} \circ N_{K/\mathbf{Q}}.$$

By the *cyclotomic height pairing* for an elliptic curve E over K (of good ordinary reduction at all places v of K above p) we mean the ρ_{cycl}^{K}-height pairing $E(K) \times E(K) \to \mathbf{Q}_p$. We put

$$h_p(P) = h_{\rho_{\text{cycl}}^{K}}(P)$$

for short. Here is an explicit formula for it.

$$h_p(P) = \frac{1}{p} \cdot \left(\sum_{v|p} \log_p(N_{K_v/\mathbf{Q}_p}(\sigma_v(P))) - \sum_{w\nmid p} \text{ord}_w(d_w(P)) \cdot \log_p(\#k_w) \right).$$

If we assume that P lies in a sufficiently small (finite index) subgroup of $E(K)$ (see [Wut04, Prop. 2]), then there will be a global choice of denominator $d(P)$, and the formula simplifies to

$$h_p(P) = \frac{1}{p} \cdot \log_p \left(\prod_{v|p} N_{K_v/\mathbf{Q}_p} \left(\frac{\sigma_v(P)}{d(P)} \right) \right).$$

2.9 Anti-cyclotomic p-adic heights

Let K be a quadratic imaginary field in which p splits as $(p) = \pi \cdot \bar{\pi}$. Suppose $\rho : \mathbf{A}_K^*/K^* \to \mathbf{Z}_p$ is a nontrivial *anti-cyclotomic* idele class character, meaning that if $\mathbf{c} : \mathbf{A}_K^*/K^* \to \mathbf{A}_K^*/K^*$ denotes the involution of the idele class group induced by complex conjugation $x \mapsto \bar{x}$ in K, then $\rho \cdot \mathbf{c} = -\rho$. Then the term

$$\sum_{v \mid p} \rho_v(\sigma_v(P))$$

in the formula for the ρ-height at the end of Section 2.7 is just

$$\sum_{v \mid p} \rho_v(\sigma_v(P)) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(\bar{P})),$$

so we have the following formula for the ρ-height of P:

$$h_\rho(P) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(\bar{P})) - \sum_{w \nmid p} \rho_w(d_w(P)).$$

Remark 2.2. The Galois equivariant property of the p-adic height pairing implies that if P is a $\mathbf{Q}$-rational point, its anti-cyclotomic height is 0. Specifically, let K/k be any Galois extension of number fields, with Galois group $G = \mathrm{Gal}(K/k)$. Let $V = V(K)$ be the $\mathbf{Q}_p$-vector space (say) defined as $(G_K)^{\mathrm{ab}} \otimes \mathbf{Q}_p$, so that V is naturally a G-representation space. Let E be an elliptic curve over k and view the Mordell-Weil group $E(K)$ as equipped with its natural G-action. Then (if p is a good ordinary prime for E) we have the p-adic height pairing

$$\langle P, Q\rangle \in V,$$

for $P, Q \in E(K)$ and we have Galois equivariance,

$$\langle g \cdot P, g \cdot Q\rangle = g \cdot \langle P, Q\rangle,$$

for any g in the Galois group.

Put $k = \mathbf{Q}$, K/k a quadratic imaginary field. Then V is of dimension two, with $V = V^+ \oplus V^-$ each of the $V^\pm$ being of dimension one, with the action of complex conjugation, $g \in G$ on $V^\pm$ being given by the sign; so that V^+ corresponds to the cyclotomic $\mathbf{Z}_p$-extension and V^- corresponds to the anticyclotomic $\mathbf{Z}_p$- extension. In the notation above, the anticyclotomic height of P and Q is just $\langle g \cdot P, g \cdot Q\rangle^-$ where the superscript $-$ means projection to V^-. Suppose that $P \in E(\mathbf{Q})$, so that $g \cdot P = P$. Then we have by Galois equivariance

$$\langle P, P\rangle^- = \langle g \cdot P, g \cdot P\rangle^- = -\langle P, P\rangle^-,$$

so $\langle P, P\rangle^- = 0$. More generally, the anticyclotomic height is zero as a pairing on either $E(K)^+ \times E(K)^+$ or $E(K)^- \times E(K)^-$ and can only be nonzero on $E(K)^+ \times E(K)^-$. If $E(K)$ is of odd rank, then the ranks of $E(K)^+$ and $E(K)^-$ must be different, which obliges the pairing on $E(K)^+ \times E(K)^-$ to be either left-degenerate or right-degenerate (or, of course, degenerate on both sides). Rubin and the first author conjecture that it is nondegenerate on one side (the side, of course having smaller rank); for more details see, e.g., [MR04, Conj. 11].

3 The Algorithms

Fix an elliptic curve E over $\mathbf{Q}$ and a good ordinary prime $p \geq 5$. In this section we discuss algorithms for computing the cyclotomic p-adic height of elements of $E(\mathbf{Q})$.

3.1 Computing the p-adic σ-function

First we explicitly solve the differential equation (1.5). Let $z(t)$ be the formal logarithm on E, which is given by $z(t) = \int \frac{\omega}{dt} = t + \cdots$ (here the symbol $\int$

means formal integration with 0 constant term). There is a unique function $F(z) \in \mathbf{Q}((z))$ such that $t = F(z(t))$. Set $x(z) = x(F(z))$. Rewrite (1.5) as

$$x(z) + c = -\frac{d}{\omega}\left(\frac{d\log(\sigma)}{\omega}\right). \tag{3.1}$$

A crucial observation is that

$$x(z) + c = \frac{1}{z^2} - \frac{a_1^2 + 4a_2}{12} + c + \cdots ;$$

in particular, the coefficient of $1/z$ in the expansion of $g(z) = x(z) + c$ is 0.

Since $z = \int(\omega/dt)$ we have $dz = (\omega/dt)dt = \omega$, hence $dz/\omega = 1$, so

$$-\frac{d}{\omega}\left(\frac{d\log(\sigma)}{\omega}\right) = -\frac{dz}{\omega}\frac{d}{dz}\left(\frac{d\log(\sigma)}{\omega}\right) = -\frac{d}{dz}\left(\frac{d\log(\sigma)}{dz}\right). \tag{3.2}$$

Write $\sigma(z) = z\sigma_0(z)$ where $\sigma_0(z)$ has nonzero constant term. Then

$$-\frac{d}{dz}\left(\frac{d\log(\sigma)}{dz}\right) = \frac{1}{z^2} - \frac{d}{dz}\left(\frac{d\log(\sigma_0)}{dz}\right). \tag{3.3}$$

Thus combining (3.1)–(3.3) and changing sign gives

$$\frac{1}{z^2} - x(z) - c = \frac{d}{dz}\left(\frac{d\log(\sigma_0)}{dz}\right).$$

This is particularly nice, since $g(z) = \frac{1}{z^2} - x(z) - c \in \mathbf{Q}[[z]]$. We can thus solve for $\sigma_0(z)$ by formally integrating twice and exponentiating:

$$\sigma_0(z) = \exp\left(\int\int g(z)dzdz\right),$$

where we choose the constants in the double integral to be 0, so $\int\int g = 0 + 0z + \cdots$. Using (1.8) we can rewrite $g(z)$ in terms of $e_2 = \mathbf{E}_2(E,\omega)$ and $\wp(z)$ as

$$g(z) = \frac{1}{z^2} - (x(z) + c) = \frac{1}{z^2} - \wp(z) + \frac{e_2}{12}.$$

Combining everything and using that $\sigma(z) = z\sigma_0(z)$ yields

$$\sigma(z) = z \cdot \exp\left(\int\int\left(\frac{1}{z^2} - \wp(z) + \frac{e_2}{12}\right)dzdz\right),$$

Finally, to compute $\sigma(t)$ we compute $\sigma(z)$ and obtain $\sigma(t)$ as $\sigma(z(t))$.

We formalize the resulting algorithm below.

Algorithm 3.1 (The Canonical p-adic Sigma Function). Given an elliptic curve E over $\mathbf{Q}$, a good ordinary prime p for E, and an approximation e_2 for $\mathbf{E}_2(E,\omega)$, this algorithm computes an approximation to $\sigma(t) \in \mathbf{Z}_p[[t]]$.

1. [Compute Formal Log] Compute the formal logarithm $z(t) = t + \cdots \in \mathbf{Q}((t))$ using that

$$z(t) = \int \frac{dx/dt}{2y(t) + a_1 x(t) + a_3}, \qquad \text{(0 constant term)} \tag{3.4}$$

   where $x(t) = t/w(t)$ and $y(t) = -1/w(t)$ are the local expansions of x and y in terms of $t = -x/y$, and $w(t) = \sum_{n \geq 0} s_n t^n$ is given by the following explicit inductive formula (see, e.g., [Blu, pg. 18]):

$$s_0 = s_1 = s_2 = 0, \qquad s_3 = 1, \qquad \text{and for } n \geq 4,$$

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 \sum_{i+j=n} s_i s_j + a_4 \sum_{i+j=n-1} s_i s_j + a_6 \sum_{i+j+k=n} s_i s_j s_k.$$

2. [Reversion] Using a power series "reversion" (functional inverse) algorithm, find the unique power series $F(z) \in \mathbf{Q}[[z]]$ such that $t = F(z)$. Here F is the reversion of z, which exists because $z(t) = t + \cdots$.
3. [Compute $\wp$] Compute $\alpha(t) = x(t) + (a_1^2 + 4a_2)/12 \in \mathbf{Q}[[t]]$, where the a_i are as in (1.6). Then compute the series $\wp(z) = \alpha(F(z)) \in \mathbf{Q}((z))$.
4. [Compute $\sigma(z)$] Set $g(z) = \dfrac{1}{z^2} - \wp(z) + \dfrac{e_2}{12} \in \mathbf{Q}_p((z))$, and compute

$$\sigma(z) = z \cdot \exp\left(\int \int g(z) dz dz\right) \in \mathbf{Q}_p[[z]].$$

5. [Compute $\sigma(t)$] Set $\sigma(t) = \sigma(z(t)) \in t \cdot \mathbf{Z}_p[[t]]$, where $z(t)$ is the formal logarithm computed in Step 1. Output $\sigma(t)$ and terminate.

3.2 Computing $\mathbf{E}_2(E, \omega)$ using cohomology

This section is about a fast method of computation of $\mathbf{E}_2(E, \omega)$ for individual ordinary elliptic curves, "one at a time". The key input is [Kat73, App. 2] (see also [Kat76]), which gives an interpretation of $\mathbf{E}_2(E, \omega)$ as the "direction" of the unit root eigenspace (cf. formula A.2.4.1 of [Kat73, App. 2]) of Frobenius acting on the one-dimensional de Rham cohomology of E.

Concretely, consider an elliptic curve E over $\mathbf{Z}_p$ with good ordinary reduction. Assume that $p \geq 5$. Fix a Weierstrass equation for E of the form $y^2 = 4x^3 - g_2 x - g_3$, The differentials $\omega = dx/y$ and $\eta = x dx/y$ form a $\mathbf{Z}_p$-basis for the first p-adic de Rham cohomology group H^1 of E, and we wish to compute the matrix F of absolute Frobenius with respect to this basis. Frobenius is $\mathbf{Z}_p$-linear, since we are working over $\mathbf{Z}_p$; if we were working over the Witt vectors of $\mathbf{F}_q$, then Frobenius would only be semi-linear.

We explicitly calculate F (to a specified precision) using Kedlaya's algorithm, which makes use of Monsky-Washnitzer cohomology of the affine curve $E - \mathcal{O}$. Kedlaya designed his algorithm for computation of zeta functions of hyperelliptic curves over finite fields. An intermediate step in Kedlaya's algorithm is computation of the matrix of absolute Frobenius on p-adic de Rham cohomology, via Monsky-Washnitzer cohomology. For more details see [Ked01] and [Ked03]. For recent formulations and applications of fast algorithms to compute Frobenius eigenvalues, see [LW02].

Now that we have computed F, we deduce $\mathbf{E}_2(E,\omega)$ as follows. The unit root subspace is a direct factor, call it U, of H^1, and we know that a complementary direct factor is the $\mathbf{Z}_p$ span of ω. We also know that $F(\omega)$ lies in $p\,\mathrm{H}^1$, and this tells us that, mod p^n, the subspace U is the span of $F^n(\eta)$. Thus if for each n, we write $F^n(\eta) = a_n\omega + b_n\eta$, then b_n is a unit (congruent (mod p) to the nth power of the Hasse invariant) and $\mathbf{E}_2(E,\omega) \equiv -12a_n/b_n \pmod{p^n}$. Note that a_n and b_n are the entries of the second column of the matrix F^n.

Algorithm 3.2 (Evaluation of $\mathbf{E}_2(E,\omega)$). Given an elliptic curve over $\mathbf{Q}$ and a good ordinary prime $p \geq 5$, this algorithm approximates $\mathbf{E}_2(E,\omega) \in \mathbf{Z}_p$ modulo p^n.

1. [Invariants] Let c_4 and c_6 be the c-invariants of a minimal model of E. Set
$$a_4 = -\frac{c_4}{2^4\cdot 3} \qquad \text{and} \qquad a_6 = -\frac{c_6}{2^5\cdot 3^3}.$$
2. [Kedlaya] Apply Kedlaya's algorithm to the hyperelliptic curve $y^2 = x^3 + a_4x + a_6$ (which is isomorphic to E) to obtain the matrix F (modulo p^n) of the action of absolute Frobenius on the basis
$$\omega = \frac{dx}{y}, \qquad \eta = \frac{xdx}{y}.$$
We view F as acting from the left.
3. [Iterate Frobenius] Compute the second column $\begin{pmatrix} a \\ b \end{pmatrix}$ of F^n, so $\mathrm{Frob}^n(\eta) = a\omega + b\eta$.
4. [Finished] Output $-12a/b$ (which is a number modulo p^n, since b is a unit).

3.3 Computing $\mathbf{E}_2(E,\omega)$ using integrality

The algorithm in this section is more elementary than the one in Section 3.2, and is directly motivated by Theorem 1.3. In practice it is very slow, except if p is small (e.g., $p = 5$) and we only require $\mathbf{E}_2(E,\omega)$ to very low precision. Our guess is that it should be exponentially hard to compute a quantity using a log convergent series for it, and that this "integrality" method is essentially the same as using log convergent expansions.

Let c be an indeterminate and in view of (1.9), write $e_2 = -12c + a_1^2 + 4a_2 \in \mathbf{Q}[c]$. If we run Algorithm 3.1 with this (formal) value of e_2, we obtain a series $\sigma(t,c) \in \mathbf{Q}[c][[t]]$. For each prime $p \geq 5$, Theorem 1.3 implies that there is a unique choice of $c_p \in \mathbf{Z}_p$ such that $\sigma(t,c_p) = t + \cdots \in t\mathbf{Z}_p[[t]]$

is odd. Upon fixing a prime p, we compute the coefficients of $\sigma(t,c)$, which are polynomials in $\mathbf{Q}[c]$; integrality of $\sigma(t,c_p)$ then imposes conditions that together must determine c_p up to some precision, which depends on the number of coefficients that we consider. Having computed c_p to some precision, we recover $\mathbf{E}_2(E,\omega)$ as $-12c_p+a_1^2+4a_2$. We formalize the above as an algorithm.

Algorithm 3.3 (Integrality). Given an elliptic curve over $\mathbf{Q}$ and a good ordinary prime $p \geq 5$, this algorithm approximates the associated p-adic σ-function.

1. [Formal Series] Use Algorithm 3.1 with $e_2 = -12c + a_1^2 + 4a_2$ to compute $\sigma(t) \in \mathbf{Q}[c][[t]]$ to some precision.
2. [Approximate c_p] Obtain constraints on c using that the coefficients of σ must be in $\mathbf{Z}_p$. These determine c to some precision. (For more details see the example in Section 4.1).

3.4 Computing cyclotomic p-adic heights

Finally we give an algorithm for computing the cyclotomic p-adic height $h_p(P)$ that combines Algorithm 3.2 with the discussion elsewhere in this paper. We have computed σ and h_p in numerous cases using the algorithm described below, and implementations of the "integrality" algorithm described above, and the results match.

Algorithm 3.4 (The p-adic Height). Given an elliptic curve E over $\mathbf{Q}$, a good ordinary prime p, and a non-torsion element $P \in E(\mathbf{Q})$, this algorithm approximates the p-adic height $h_p(P) \in \mathbf{Q}_p$.

1. [Prepare Point] Compute a positive integer m such that mP reduces to $\mathcal{O} \in E(\mathbf{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbf{F}_\ell}$ at all bad primes ℓ. For example, m could be the least common multiple of the Tamagawa numbers of E and $\#E(\mathbf{F}_p)$. Set $Q = mP$ and write $Q = (x,y)$.
2. [Denominator] Let d be the positive integer square root of the denominator of x.
3. [Compute σ] Approximate $\sigma(t)$ using Algorithm 3.1 together with either Algorithm 3.2 or Algorithm 3.3, and set $s = \sigma(-x/y) \in \mathbf{Q}_p$.
4. [Height] Compute $h_p(Q) = \dfrac{1}{p}\log_p\left(\dfrac{s}{d}\right)$, then $h_p(P) = \dfrac{1}{m^2} \cdot h_p(Q)$. Output $h_p(P)$ and terminate.

4 Sample Computations

We did the calculations in this section using SAGE [SJ05] and Magma [BCP97]. In particular, SAGE includes an optimized implementation due to J. Balakrishnan, R. Bradshaw, D. Harvey, Y. Qiang, and W. Stein of our algorithm for computing p-adic heights for elliptic curves over $\mathbf{Q}$. This implementation includes further tricks, e.g., for series manipulation, which are not described in this paper.

4.1 The rank one curve of conductor 37

Let E be the rank 1 curve $y^2 + y = x^3 - x$ of conductor 37. The point $P = (0,0)$ is a generator for $E(\mathbf{Q})$. We illustrate the above algorithms in detail by computing the p-adic height of P for the good ordinary prime $p = 5$. The steps of Algorithm 3.4 are as follows:

1. [Prepare Point] The component group of $\mathcal{E}_{\mathbf{F}_{37}}$ is trivial. The group $E(\mathbf{F}_5)$ has order 8 and the reduction of P to $E(\mathbf{F}_5)$ also has order 8, so let
$$Q = 8P = \left(\frac{21}{25}, -\frac{69}{125}\right).$$

2. [Denominator] We have $d = 5$.

3. [Compute σ] We illustrate computation of $\sigma(t)$ using both Algorithm 3.2 and Algorithm 3.3.

   (a) [Compute $\sigma(t,c)$] We use Algorithm 3.1 with $e_2 = 12c - a_1^2 - 4a_2$ to compute σ as a series in t with coefficients polynomials in c, as follows:

   i. [Compute Formal Log] Using the recurrence, we find that
$$w(t) = t^3 + t^6 - t^7 + 2t^9 - 4t^{10} + 2t^{11} + 5t^{12} - 5t^{13} + 5t^{14} + \cdots$$
Thus
$$x(t) = t^{-2} - t + t^2 - t^4 + 2t^5 - t^6 - 2t^7 + 6t^8 - 6t^9 - 3t^{10} + \cdots$$
$$y(t) = -t^{-3} + 1 - t + t^3 - 2t^4 + t^5 + 2t^6 - 6t^7 + 6t^8 + 3t^9 + \cdots$$
so integrating (3.4) we see that the formal logarithm is
$$z(t) = t + \frac{1}{2}t^4 - \frac{2}{5}t^5 + \frac{6}{7}t^7 - \frac{3}{2}t^8 + \frac{2}{3}t^9 + 2t^{10} - \frac{60}{11}t^{11} + 5t^{12} + \cdots$$

   ii. [Reversion] Using reversion, we find F with $F(z(t)) = t$:
$$F(z) = z - \frac{1}{2}z^4 + \frac{2}{5}z^5 + \frac{1}{7}z^7 - \frac{3}{10}z^8 + \frac{2}{15}z^9 - \frac{1}{28}z^{10} + \frac{54}{385}z^{11} + \cdots$$

   iii. [Compute $\wp$] We have $a_1 = a_2 = 0$, so
$$\alpha(t) = x(t) + (a_1^2 + 4a_2)/12 = x(t),$$
so
$$\wp(z) = x(F(z)) = z^{-2} + \frac{1}{5}z^2 - \frac{1}{28}z^4 + \frac{1}{75}z^6 - \frac{3}{1540}z^8 + \cdots$$
Note that the coefficient of z^{-1} is 0 and all exponents are even.

iv. [Compute $\sigma(t,c)$] Noting again that $a_1 = a_2 = 0$, we have

$$\begin{aligned} g(z,c) &= \frac{1}{z^2} - \wp(z) + \frac{12c - a_1^2 - 4a_2}{12} \\ &= c - \frac{1}{5}z^2 + \frac{1}{28}z^4 - \frac{1}{75}z^6 + \frac{3}{1540}z^8 - \frac{1943}{3822000}z^{10} + \cdots \end{aligned}$$

Formally integrating twice and exponentiating, we obtain

$$\begin{aligned} \sigma(z,c) &= z \cdot \exp\left(\int\int g(z,c)dzdz\right) \\ &= z \cdot \exp\Big(\frac{c}{2} \cdot z^2 - \frac{1}{60}z^4 + \frac{1}{840}z^6 - \frac{1}{4200}z^8 + \frac{1}{46200}z^{10} \\ &\qquad - \frac{1943}{504504000}z^{12} + \cdots\Big) \\ &= z + \frac{1}{2}cz^3 + \left(\frac{1}{8}c^2 - \frac{1}{60}\right)z^5 + \left(\frac{1}{48}c^3 - \frac{1}{120}c + \frac{1}{840}\right)z^7 + \\ &\qquad \left(\frac{1}{384}c^4 - \frac{1}{480}c^2 + \frac{1}{1680}c - \frac{1}{10080}\right)z^9 + \cdots \end{aligned}$$

Finally,

$$\begin{aligned} \sigma(t) = \sigma(z(t)) = t + \frac{1}{2}ct^3 + \frac{1}{2}t^4 + \left(\frac{1}{8}c^2 - \frac{5}{12}\right)t^5 + \frac{3}{4}ct^6 + \\ \left(\frac{1}{48}c^3 - \frac{73}{120}c + \frac{103}{120}\right)t^7 + \cdots \end{aligned}$$

(b) [Approximate] The first coefficient of $\sigma(t)$ that gives integrality information is the coefficient of t^7. Since

$$\frac{1}{48}c^3 - \frac{73}{120}c + \frac{103}{120} \in \mathbf{Z}_5,$$

multiplying by 5 we see that

$$\frac{5}{48}c^3 - \frac{73}{24}c + \frac{103}{24} \equiv 0 \pmod{5}.$$

Thus

$$c \equiv \frac{103}{24} \cdot \frac{24}{73} \equiv 1 \pmod{5}.$$

The next useful coefficient is the coefficient of t^{11}, which is

$$\frac{1}{3840}c^5 - \frac{169}{2880}c^3 + \frac{5701}{6720}c^2 + \frac{127339}{100800}c - \frac{40111}{7200}$$

Multiplying by 25, reducing coefficients, and using integrality yields the congruence

$$10c^5 + 5c^3 + 20c^2 + 2c + 3 \equiv 0 \pmod{25}.$$

Writing $c = 1 + 5d$ and substituting gives the equation $10d + 15 \equiv 0 \pmod{25}$, so $2d + 3 \equiv 0 \pmod 5$. Thus $d \equiv 1 \pmod 5$, hence $c = 1 + 5 + O(5^2)$. Repeating the procedure above with more terms, we next get new information from the coefficient of t^{31}, where we deduce that $c = 1 + 5 + 4 \cdot 5^2 + O(5^3)$.

Using Algorithm 3.2: Using Kedlaya's algorithm (as implemented in [BCP97]) we find almost instantly that

$$\mathbf{E}_2(E, \omega) = 2 + 4 \cdot 5 + 2 \cdot 5^3 + 5^4 + 3 \cdot 5^5 + 2 \cdot 5^6 + 5^8 + 3 \cdot 5^9 + 4 \cdot 5^{10} + \cdots .$$

Thus

$$c = \frac{1}{12}\mathbf{E}_2(E, \omega) = 1+5+4\cdot 5^2+5^3+5^4+5^6+4\cdot 5^7+3\cdot 5^8+2\cdot 5^9+4\cdot 5^{10}+\cdots ,$$

which is consistent with what we found above using integrality.

4. [Height] For $Q = (x, y) = 8(0, 0)$ as above, we have

$$s = \sigma\left(-\frac{x}{y}\right) = \sigma\left(\frac{35}{23}\right) = 4 \cdot 5 + 5^2 + 5^3 + 5^4 + \cdots ,$$

so

$$\begin{aligned} h_5(Q) &= \frac{1}{5} \cdot \log_5\left(\frac{s}{5}\right) = \frac{1}{5} \cdot \log_5(4 + 5 + 5^2 + 5^3 + 2 \cdot 5^5 + \cdots) \\ &= 3 + 5 + 2 \cdot 5^3 + 3 \cdot 5^4 + \cdots . \end{aligned}$$

Finally,

$$h_5(P) = \frac{1}{8^2} \cdot h_5(Q) = 2 + 4 \cdot 5 + 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + \cdots .$$

Remark 4.1. A *very* good check to see whether or not any implementation of the algorithms in this paper is really correct, is just to make control experiments every once in a while, by computing $h(P)$ and then comparing it with $h(2P)/4$, $h(3P)/9$, etc. In particular, compute $h(P) - h(nP)/n^2$ for several n and check that the result is p-adically small. We have done this in many cases for the implementation used to compute the tables in this section.

4.2 Curves of ranks 1, 2, 3, 4, and 5

4.2.1 Rank 1

The first (ordered by conductor) curve of rank 1 is the curve with Cremona label 37A, which we considered in Section 4.1 above.

p	p-adic regulator of 37A
5	$1 + 5 + 5^2 + 3 \cdot 5^5 + 4 \cdot 5^6 + O(5^7)$
7	$1 + 7 + 3 \cdot 7^2 + 7^3 + 6 \cdot 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + O(7^7)$
11	$7 + 9 \cdot 11 + 7 \cdot 11^2 + 8 \cdot 11^3 + 9 \cdot 11^4 + 2 \cdot 11^5 + 7 \cdot 11^6 + O(11^7)$
13	$12 \cdot 13 + 5 \cdot 13^2 + 9 \cdot 13^3 + 10 \cdot 13^4 + 4 \cdot 13^5 + 2 \cdot 13^6 + O(13^7)$
23	$20 + 10 \cdot 23 + 18 \cdot 23^2 + 16 \cdot 23^3 + 13 \cdot 23^4 + 4 \cdot 23^5 + 15 \cdot 23^6 + O(23^7)$
29	$19 + 4 \cdot 29 + 26 \cdot 29^2 + 2 \cdot 29^3 + 26 \cdot 29^4 + 26 \cdot 29^5 + 17 \cdot 29^6 + O(29^7)$
31	$15 + 10 \cdot 31 + 13 \cdot 31^2 + 2 \cdot 31^3 + 24 \cdot 31^4 + 9 \cdot 31^5 + 8 \cdot 31^6 + O(31^7)$
41	$30 + 2 \cdot 41 + 23 \cdot 41^2 + 15 \cdot 41^3 + 27 \cdot 41^4 + 8 \cdot 41^5 + 17 \cdot 41^6 + O(41^7)$
43	$30 + 30 \cdot 43 + 22 \cdot 43^2 + 38 \cdot 43^3 + 11 \cdot 43^4 + 29 \cdot 43^5 + O(43^6)$
47	$11 + 37 \cdot 47 + 27 \cdot 47^2 + 23 \cdot 47^3 + 22 \cdot 47^4 + 34 \cdot 47^5 + 3 \cdot 47^6 + O(47^7)$
53	$26 \cdot 53^{-2} + 30 \cdot 53^{-1} + 20 + 47 \cdot 53 + 10 \cdot 53^2 + 32 \cdot 53^3 + O(53^4)$

Note that when $p = 53$ we have $\#E(\mathbf{F}_p) = p$, i.e., p is anomalous.

4.3 Rank 2

The first curve of rank 2 is the curve 389A of conductor 389. The p-adic regulators of this curve are as follows:

p	p-adic regulator of 389A
5	$1 + 2 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + O(5^7)$
7	$6 + 3 \cdot 7^2 + 2 \cdot 7^3 + 6 \cdot 7^4 + 7^5 + 2 \cdot 7^6 + O(7^7)$
11	$4 + 7 \cdot 11 + 6 \cdot 11^2 + 11^3 + 9 \cdot 11^4 + 10 \cdot 11^5 + 3 \cdot 11^6 + O(11^7)$
13	$9 + 12 \cdot 13 + 10 \cdot 13^2 + 5 \cdot 13^3 + 5 \cdot 13^4 + 13^5 + 9 \cdot 13^6 + O(13^7)$
17	$4 + 8 \cdot 17 + 15 \cdot 17^2 + 11 \cdot 17^3 + 13 \cdot 17^4 + 16 \cdot 17^5 + 6 \cdot 17^6 + O(17^7)$
19	$3 + 5 \cdot 19 + 8 \cdot 19^2 + 16 \cdot 19^3 + 13 \cdot 19^4 + 14 \cdot 19^5 + 11 \cdot 19^6 + O(19^7)$
23	$17 + 23 + 22 \cdot 23^2 + 16 \cdot 23^3 + 3 \cdot 23^4 + 15 \cdot 23^5 + O(23^7)$
29	$9 + 14 \cdot 29 + 22 \cdot 29^2 + 29^3 + 22 \cdot 29^4 + 29^5 + 20 \cdot 29^6 + O(29^7)$
31	$1 + 17 \cdot 31 + 4 \cdot 31^2 + 16 \cdot 31^3 + 18 \cdot 31^4 + 21 \cdot 31^5 + 8 \cdot 31^6 + O(31^7)$
37	$28 + 37 + 11 \cdot 37^2 + 7 \cdot 37^3 + 3 \cdot 37^4 + 24 \cdot 37^5 + 17 \cdot 37^6 + O(37^7)$
41	$20 + 26 \cdot 41 + 41^2 + 29 \cdot 41^3 + 38 \cdot 41^4 + 31 \cdot 41^5 + 23 \cdot 41^6 + O(41^7)$
43	$40 + 25 \cdot 43 + 15 \cdot 43^2 + 18 \cdot 43^3 + 36 \cdot 43^4 + 35 \cdot 43^5 + O(43^6)$
47	$25 + 24 \cdot 47 + 7 \cdot 47^2 + 11 \cdot 47^3 + 35 \cdot 47^4 + 3 \cdot 47^5 + 9 \cdot 47^6 + O(47^7)$

4.4 Rank 3

The first curve of rank 3 is the curve 5077A of conductor 5077. The p-adic regulators of this curve are as follows:

p	p-adic regulator of 5077A
5	$5^{-2} + 5^{-1} + 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 4 \cdot 5^4 + 2 \cdot 5^5 + 5^6 + O(5^7)$
7	$1 + 3 \cdot 7 + 3 \cdot 7^2 + 4 \cdot 7^3 + 4 \cdot 7^5 + O(7^7)$
11	$6 + 11 + 5 \cdot 11^2 + 11^3 + 11^4 + 8 \cdot 11^5 + 3 \cdot 11^6 + O(11^7)$
13	$2 + 6 \cdot 13 + 13^3 + 6 \cdot 13^4 + 13^5 + 4 \cdot 13^6 + O(13^7)$
17	$11 + 15 \cdot 17 + 8 \cdot 17^2 + 16 \cdot 17^3 + 9 \cdot 17^4 + 5 \cdot 17^5 + 11 \cdot 17^6 + O(17^7)$
19	$17 + 9 \cdot 19 + 10 \cdot 19^2 + 15 \cdot 19^3 + 6 \cdot 19^4 + 13 \cdot 19^5 + 17 \cdot 19^6 + O(19^7)$
23	$7 + 17 \cdot 23 + 19 \cdot 23^3 + 21 \cdot 23^4 + 19 \cdot 23^5 + 22 \cdot 23^6 + O(23^7)$
29	$8 + 16 \cdot 29 + 11 \cdot 29^2 + 20 \cdot 29^3 + 9 \cdot 29^4 + 8 \cdot 29^5 + 24 \cdot 29^6 + O(29^7)$
31	$17 + 11 \cdot 31 + 28 \cdot 31^2 + 3 \cdot 31^3 + 17 \cdot 31^5 + 29 \cdot 31^6 + O(31^7)$
43	$9 + 13 \cdot 43 + 15 \cdot 43^2 + 32 \cdot 43^3 + 28 \cdot 43^4 + 18 \cdot 43^5 + 3 \cdot 43^6 + O(43^7)$
47	$29 + 3 \cdot 47 + 46 \cdot 47^2 + 4 \cdot 47^3 + 23 \cdot 47^4 + 25 \cdot 47^5 + 37 \cdot 47^6 + O(47^7)$

For $p = 5$ and E the curve 5077A, we have $\#E(\mathbf{F}_5) = 10$, so $a_p \equiv 1 \pmod{5}$, hence p is anamolous.

4.5 Rank 4

Next we consider the curve of rank 4 with smallest known conductor ($234446 = 2 \cdot 117223$):

$$y^2 + xy = x^3 - x^2 - 79x + 289.$$

Note that computation of the p-adic heights is just as fast for this curve as the above curves, i.e., our algorithm for computing heights is insensitive to the conductor, only the prime p (of course, computing the Mordell-Weil group could take much longer if the conductor is large).

p	p-adic regulator of rank 4 curve
5	$2 \cdot 5^{-2} + 2 \cdot 5^{-1} + 3 \cdot 5 + 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + O(5^7)$
7	$6 \cdot 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + 5 \cdot 7^5 + 3 \cdot 7^6 + O(7^7)$
11	$5 + 10 \cdot 11 + 5 \cdot 11^2 + 11^3 + 3 \cdot 11^5 + 11^6 + O(11^7)$
13	$12 + 2 \cdot 13 + 4 \cdot 13^2 + 10 \cdot 13^3 + 3 \cdot 13^4 + 5 \cdot 13^5 + 7 \cdot 13^6 + O(13^7)$
17	$15 + 8 \cdot 17 + 13 \cdot 17^2 + 5 \cdot 17^3 + 13 \cdot 17^4 + 7 \cdot 17^5 + 14 \cdot 17^6 + O(17^7)$
19	$14 + 16 \cdot 19 + 15 \cdot 19^2 + 6 \cdot 19^3 + 10 \cdot 19^4 + 7 \cdot 19^5 + 13 \cdot 19^6 + O(19^7)$
23	$3 + 15 \cdot 23 + 15 \cdot 23^2 + 12 \cdot 23^4 + 20 \cdot 23^5 + 7 \cdot 23^6 + O(23^7)$
29	$25 + 4 \cdot 29 + 18 \cdot 29^2 + 5 \cdot 29^3 + 27 \cdot 29^4 + 23 \cdot 29^5 + 27 \cdot 29^6 + O(29^7)$
31	$21 + 26 \cdot 31 + 22 \cdot 31^2 + 25 \cdot 31^3 + 31^4 + 3 \cdot 31^5 + 14 \cdot 31^6 + O(31^7)$
37	$34 + 14 \cdot 37 + 32 \cdot 37^2 + 25 \cdot 37^3 + 28 \cdot 37^4 + 36 \cdot 37^5 + O(37^6)$
41	$33 + 38 \cdot 41 + 9 \cdot 41^2 + 35 \cdot 41^3 + 25 \cdot 41^4 + 15 \cdot 41^5 + 30 \cdot 41^6 + O(41^7)$
43	$14 + 34 \cdot 43 + 12 \cdot 43^2 + 26 \cdot 43^3 + 32 \cdot 43^4 + 26 \cdot 43^5 + O(43^6)$
47	$43 + 47 + 17 \cdot 47^2 + 28 \cdot 47^3 + 40 \cdot 47^4 + 6 \cdot 47^5 + 7 \cdot 47^6 + O(47^7)$

4.6 Rank 5

Next we consider the curve of rank 5 with smallest known conductor, which is the prime 19047851. The curve is

$$y^2 + y = x^3 - 79x + 342$$

p	p-adic regulator of rank 5 curve
5	$2 \cdot 5 + 5^2 + 5^3 + 2 \cdot 5^4 + 5^5 + 5^6 + O(5^7)$
7	$2 + 6 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^3 + 6 \cdot 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + O(7^7)$
11	$10 + 11 + 6 \cdot 11^2 + 2 \cdot 11^3 + 6 \cdot 11^4 + 7 \cdot 11^5 + 5 \cdot 11^6 + O(11^7)$
13	$11 + 8 \cdot 13 + 3 \cdot 13^2 + 4 \cdot 13^3 + 10 \cdot 13^4 + 5 \cdot 13^5 + 6 \cdot 13^6 + O(13^7)$
17	$4 + 11 \cdot 17 + 4 \cdot 17^2 + 5 \cdot 17^3 + 13 \cdot 17^4 + 5 \cdot 17^5 + 2 \cdot 17^6 + O(17^7)$
19	$11 + 7 \cdot 19 + 11 \cdot 19^2 + 7 \cdot 19^3 + 9 \cdot 19^4 + 6 \cdot 19^5 + 10 \cdot 19^6 + O(19^7)$
23	$14 + 14 \cdot 23 + 20 \cdot 23^2 + 6 \cdot 23^3 + 19 \cdot 23^4 + 9 \cdot 23^5 + 15 \cdot 23^6 + O(23^7)$
29	$3 + 5 \cdot 29 + 20 \cdot 29^3 + 21 \cdot 29^4 + 18 \cdot 29^5 + 11 \cdot 29^6 + O(29^7)$
31	$4 + 26 \cdot 31 + 11 \cdot 31^2 + 12 \cdot 31^3 + 3 \cdot 31^4 + 15 \cdot 31^5 + 22 \cdot 31^6 + O(31^7)$
37	$3 + 20 \cdot 37 + 11 \cdot 37^2 + 17 \cdot 37^3 + 33 \cdot 37^4 + 5 \cdot 37^5 + O(37^7)$
41	$3 + 41 + 35 \cdot 41^2 + 29 \cdot 41^3 + 22 \cdot 41^4 + 27 \cdot 41^5 + 25 \cdot 41^6 + O(41^7)$
43	$35 + 41 \cdot 43 + 43^2 + 11 \cdot 43^3 + 32 \cdot 43^4 + 11 \cdot 43^5 + 18 \cdot 43^6 + O(43^7)$
47	$25 + 39 \cdot 47 + 45 \cdot 47^2 + 25 \cdot 47^3 + 42 \cdot 47^4 + 13 \cdot 47^5 + O(47^6)$

Note that the regulator for $p = 5$ is not a unit, and $\#E(F_5) = 9$. This is the only example of a regulator in our tables with positive valuation.

Part II
Computing expansions for $\mathbf{E}_2$ in terms of classical modular forms

We next study convergence of $\mathbf{E}_2$ in the general context of p-adic and overconvergent modular forms. Coleman, Gouvea, and Jochnowitz prove in [CGJ95] that $\mathbf{E}_2$ is *transcendental* over the ring of overconvergent modular forms, so $\mathbf{E}_2$ is certainly non-overconvergent. However, $\mathbf{E}_2$ is *log convergent* in a sense that we make precise in this part of the paper.

5 Questions about rates of convergence

Fix p a prime number, which, in this section, we will assume is ≥ 5. We only consider modular forms of positive even integral weight, on $\Gamma_0(M)$ for some M, and with Fourier coefficients in $\mathbf{C}_p$. By a *classical modular form* we will mean one with these properties, and by a *Katz modular form* we mean a p-adic modular form in the sense of Katz ([Kat73]), again with these properties, i.e., of integral weight $k \geq 0$, of tame level N for a positive integer N prime to p, and with Fourier coefficients in $\mathbf{C}_p$. A *p-integral modular form* is a modular form with Fourier coefficients in $\mathbf{Z}_p$. Note that throughout Sections 5 and 6, all our modular forms can be taken to be with coefficients in $\mathbf{Q}_p$.

If f is a classical, or Katz, modular form, we will often simply identify the form f with its Fourier expansion, $f = \sum_{n\geq 0} c_f(n)q^n$. By $\mathrm{ord}_p(f)$ we mean the greatest lower bound of the non-negative integers $\mathrm{ord}_p(c_f(n))$ for $n \geq 0$. The valuation ord_p on $\mathbf{C}_p$ here is given its natural normalization, i.e., $\mathrm{ord}_p(p) = 1$.

We say two p-integral modular forms are *congruent* modulo p^n, denoted

$$f \equiv g \pmod{p^n},$$

if their corresponding Fourier coefficients are congruent modulo p^n. Equivalently, $f \equiv g \pmod{p^n}$ if $\mathrm{ord}_p(f - g) \geq n$.

Recall the traditional notation,

$$\sigma_{k-1}(n) = \sum_{0\,<\,d\,\mid\,n} d^{k-1},$$

and put $\sigma(n) = \sigma_1(n)$.

Let $E_k = -b_k/2k + \sum_{n=0}^{\infty} \sigma_{k-1}(n)q^n$ be the Eisenstein series of even weight $k \geq 2$, and denote by $\mathcal{E}_k$ the "other natural normalization" of the Eisenstein series,

$$\mathcal{E}_k = 1 - \frac{2k}{b_k} \cdot \sum_{n=0}^{\infty} \sigma_{k-1}(n)q^n,$$

for $k \geq 2$. We have

$$\mathcal{E}_{p-1} \equiv 1 \pmod{p}.$$

(Note that $\mathcal{E}_k$ is the q-expansion of the Katz modular form that we denote by $\mathbf{E}_k$ elsewhere in this paper.)

For $k > 2$ these are classical modular forms of level 1, while the Fourier series $E_2 = -1/24 + \sum_{n=0}^{\infty} \sigma(n)q^n$, and the corresponding $\mathcal{E}_2$, are not; nevertheless, they may all be viewed as Katz modular forms of tame level 1.

Put

$$\sigma^{(p)}(n) = \sum_{0\,<\,d\,\mid\,n;\ (p,d)=1} d,$$

so that we have:

$$\sigma(n) = \sigma^{(p)}(n) + p\sigma^{(p)}(n/p) + p^2\sigma^{(p)}(n/p^2) + \cdots \tag{5.1}$$

where the convention is that $\sigma^{(p)}(r) = 0$ if r is not an integer.

Let $V = V_p$ be the operator on power series given by the rule:

$$V\left(\sum_{n\geq 0} c_n q^n\right) = \sum_{n\geq 0} c_n q^{pn}.$$

If $F = \sum_{n\geq 0} c_n q^n$ is a classical modular form of weight k on $\Gamma_0(M)$, then $V(F)$ is (the Fourier expansion of) a classical modular form of weight k on $\Gamma_0(Mp)$ (cf. [Lan95, Ch. VIII]).

The Fourier series

$$E_2^{(p)} = (1 - pV)E_2 = \frac{p-1}{24} + \sum \sigma_1^{(p)}(n)q^n$$

is, in contrast to E_2, a classical modular form (of weight 2 on $\Gamma_0(p)$) and we can invert the formula of its definition to give the following equality of Fourier series:

$$E_2 = \sum_{\nu \geq 0} p^\nu V^\nu E_2^{(p)}, \tag{5.2}$$

this equality being, for the corresponding Fourier coefficients other than the constant terms, another way of phrasing (5.1).

Definition 5.1 (Convergence Rate). We call a function $\alpha(\nu)$ taking values that are either positive integers or $+\infty$ on integers $\nu = 0, \pm 1, \pm 2, \dots$ a *convergence rate* if $\alpha(\nu)$ is a non-decreasing function such that $\alpha(\nu) = 0$ for $\nu \leq 0$, $\alpha(\nu+\mu) \leq \alpha(\nu) + \alpha(\mu)$, and $\alpha(\nu)$ tends to $+\infty$ as ν does.

A simple nontrivial example of a convergence rate is

$$\alpha(\nu) = \begin{cases} 0 & \text{for } \nu \leq 0, \\ \nu & \text{for } \nu \geq 0. \end{cases}$$

If $\alpha(\nu)$ is a convergence rate, put $T\alpha(\nu) = \alpha(\nu - 1)$; note that $T\alpha(\nu)$ is also a convergence rate (T translates the graph of α one to the right). Given a collection $\{\alpha_j\}_{j \in J}$ of convergence rates, the "max" function $\alpha(\nu) = \max_{j \in J} \alpha_j(\nu)$ is again a convergence rate.

Definition 5.2 (α-Convergent). Let α be a convergence rate. A Katz modular form f is *α-convergent* if there is a function $a : \mathbf{Z}_{\geq 0} \to \mathbf{Z}_{\geq 0}$ such that

$$f = \sum_{\nu=0}^{\infty} p^{a(\nu)} f_\nu \mathcal{E}_{p-1}^{-\nu} \tag{5.3}$$

with f_ν a classical p-integral modular form (of weight $k + \nu(p-1)$ and level N) and $a(\nu) \geq \alpha(\nu)$ for all $\nu \geq 0$.

If $\alpha' \leq \alpha$ are convergence rates and a modular form f is *α-convergent* then it is also *α'-convergent.* As formulated, an expansion of the shape of (5.3) for a given f is not unique but [Kat73] and [Gou88] make a certain sequence of choices that enable them to get canonical expansions of the type (5.3), dependent on those initial choices. Specifically, let $M_{\text{classical}}(N, k, \mathbf{Z}_p)$ denote the $\mathbf{Z}_p$-module of classical modular forms on $\Gamma_0(N)$ of weight k and with Fourier coefficients in $\mathbf{Z}_p$. Multiplication by $\mathcal{E}_{p-1}$ allows one to identify $M_{\text{classical}}(N, k, \mathbf{Z}_p)$ with a saturated $\mathbf{Z}_p$-lattice in $M_{\text{classical}}(N, k+p-1, \mathbf{Z}_p)$. (The lattice is saturated because multiplication by $E_{p-1}(\text{mod } p)$ is injective, since it is the identity map on q-expansions.) *Fix*, for each k, a $\mathbf{Z}_p$-module,

$$C(N, k+p-1, \mathbf{Z}_p) \subset M_{\text{classical}}(N, k+p-1, \mathbf{Z}_p)$$

that is complementary to $\mathcal{E}_{p-1} \cdot M_{\text{classical}}(N, k, \mathbf{Z}_p) \subset M_{\text{classical}}(N, k+p-1, \mathbf{Z}_p)$. Requiring the classical modular forms f_ν of the expansion (5.3) to lie in these complementary submodules, i.e., $f_\nu \in C(N, k + \nu(p-1), \mathbf{Z}_p)$ for all ν, pins down the expansion uniquely. Let us call an expansion of the form

$$f = \sum_{\nu=0}^{\infty} p^{\alpha(\nu)} f_\nu \mathcal{E}_{p-1}^{-\nu}$$

pinned down by a choice of complementary submodules as described above a *Katz expansion* of f.

A *classical* p-integral modular form is, of course, α-convergent for every α. For any given convergence rate α, the α-convergent Katz modular forms of tame level N are closed under multiplication, and the collection of them forms an algebra over the ring of classical modular forms of level N (with Fourier coefficients in $\mathbf{Z}_p$). Any Katz p-integral modular form is α-convergent, for some convergence rate α (see [Gou88]).

Proposition 5.3. *A Katz p-integral modular form f of weight k and tame level N as above is α-convergent if and only if the Fourier series of $f\mathcal{E}_{p-1}^{\nu}$ is congruent to the Fourier series of a classical p-integral modular form (of weight $k + \nu(p-1)$ and level N) modulo $p^{\alpha(\nu+1)}$ for every integer $\nu \geq 0$.*

Proof. We use the q-expansion principle. Specifically, if G_ν is a classical modular form such that $f\mathcal{E}_{p-1}^{\nu} \equiv G_\nu \pmod{p^{\alpha(\nu+1)}}$ then $g_\nu = p^{-\alpha(\nu+1)}(f\mathcal{E}_{p-1}^{\nu} - G_\nu)$ is again a Katz modular form, and we can produce the requisite α-convergent Katz expansion by inductive consideration of these g_ν's. (Note that the other implication is trivial. Also note our running hypothesis that $p \geq 5$.) □

In view of this, we may define, for any f as in Proposition 5.3, the function $a_f(\nu)$ (for $\nu \geq 0$) as follows: $a_f(0) = 0$, and for $\nu \geq 1$, $a_f(\nu)$ is the largest integer a such that $f\mathcal{E}_{p-1}^{\nu-1}$ is congruent to a classical p-integral modular form (of weight $k + (\nu-1)(p-1)$ and level N) modulo p^a.

Corollary 5.4. *The Katz p-integral modular form f is α-convergent for any convergence rate α that is majorized by the function a_f. (I.e., for which $\alpha(\nu) \leq a_f(\nu)$ for all $\nu \geq 0$.)*

Definition 5.5 (Overconvergent of Radius r). Let $r \in \mathbf{Q}$ be a positive rational number. A Katz p-integral modular form f of tame level N is *overconvergent of radius r* if and only if it is α-convergent for some function α such that $\alpha(\nu) \geq r \cdot \nu$ for all ν, and $\alpha(\nu) - r \cdot \nu$ tends to infinity with ν.

Remarks 5.6. It is convenient to say, for two function $\alpha(\nu)$ and $\alpha'(\nu)$, that

$$\alpha(\nu) \ggg \alpha'(\nu)$$

if $\alpha(\nu) \geq \alpha'(\nu)$ and $\alpha(\nu) - \alpha'(\nu)$ tends to infinity with ν. So, we may rephrase the above definition as saying that f is overconvergent with radius r if it is

α-convergent with $\alpha(\nu) \gg r \cdot \nu$. The above definition is equivalent to the definition of [Kat73, Gou88] except for the fact that the word *radius* in these references does not denote the rational number r above, but rather a choice of p-adic number whose ord_p is r. We may think of our manner of phrasing the definition as being a *definition by Katz expansion convergence rate* as opposed to what one might call the *definition by rigid analytic geometric behavior*, meaning the equivalent, and standard, formulation (cf. [Kat73]) given by considering f as a rigid analytic function on an appropriate extension of the Hasse domain in the (rigid analytic space associated to) $X_0(N)$.

Definition 5.7 ((Precisely) Log Convergent). A Katz p-integral modular form f is *log-convergent* if $c \cdot \log(\nu) \leq a_f(\nu)$ for some positive constant c and all but finitely many ν (equivalently: if it is α-convergent for $\alpha(\nu) = c \cdot \log(\nu)$ for some positive constant c). We will say that f is *precisely log-convergent* if there are positive constants c, C such that $c \cdot \log(\nu) \leq a_f(\nu) \leq C \cdot \log(\nu)$ for all but finitely many ν.

Remark 5.8. As in Definition 5.1 above, we may think of this manner of phrasing the definition as being a *definition by Katz expansion convergence rate*. This seems to us to be of some specific interest in connection with the algorithms that we present in this article for the computation of $\mathbf{E}_2$. For more theoretical concerns, however, we think it would be interesting to give, if possible, an equivalent *definition by rigid analytic geometric behavior*: is there some explicit behavior at the "rim" of the Hasse domain that characterizes log-convergence?

Proposition 5.9. *Let $p \geq 5$. Let f be a Katz p-integral modular form of weight k and tame level N that admits an expansion of the type*

$$f = \sum_{\nu=0}^{\infty} p^{\nu} \mathcal{F}_{\nu} \mathcal{E}_{p-1}^{-\nu}$$

where, for all $\nu \geq 0$, $\mathcal{F}_{\nu}$ is a classical p-integral modular form (of weight $k + \nu(p-1)$) on $\Gamma_0(p^{\nu+1})$. Then f is log-convergent and

$$\liminf_{n \to \infty} \frac{a_f(n)}{\log(n)} \geq \frac{1}{\log(p)}.$$

Proof. The classical modular form $\mathcal{F}_{\nu}$ on $\Gamma_0(p^{\nu+1})$ is an overconvergent Katz modular form of radius r for any r such that $r < \frac{1}{p^{\nu-1}(p+1)}$ (cf. [Kat73], [Gou88, Cor. II.2.8]). Let

$$\mathcal{F}_{\nu} = \sum_{\mu=0}^{\infty} f_{\mu}^{(\nu)} \mathcal{E}_{p-1}^{-\mu}$$

be its Katz expansion. So,

$$\mathrm{ord}_p(f_{\mu}^{(\nu)}) \gg \left(\frac{1}{p^{\nu-1}(p+1)} - \epsilon_{\mu,\nu} \right) \cdot \mu$$

for any choice of positive $\epsilon_{\mu,\nu}$. We have

$$f = \sum_{\nu=0}^{\infty} p^{\nu} \sum_{\mu=0}^{\infty} f_{\mu}^{(\nu)} \mathcal{E}_{p-1}^{-(\mu+\nu)},$$

or (substituting $\gamma = \mu + \nu$)

$$f = \sum_{\gamma=0}^{\infty} \left\{ \sum_{\nu=0}^{\gamma} p^{\nu}\ f_{\gamma-\nu}^{(\nu)} \right\} \mathcal{E}_{p-1}^{-\gamma}.$$

Putting $G_{\gamma} = \sum_{\nu=0}^{\gamma} p^{\nu}\ f_{\gamma-\nu}^{(\nu)}$ we may write the above expansion as

$$f = \sum_{\gamma=0}^{\infty} G_{\gamma} \mathcal{E}_{p-1}^{-\gamma},$$

and we must show that

$$\mathrm{ord}_p(G_{\gamma}) \geq c \cdot \log(\gamma)$$

for some positive constant c.

For any $\nu \leq \gamma$ we have

$$\mathrm{ord}_p \left(p^{\nu}\ f_{\gamma-\nu}^{(\nu)} \right) \ \geqq\ \nu + \left(\frac{1}{p^{\nu-1}(p+1)} - \epsilon_{\gamma-\nu,\nu} \right) (\gamma - \nu).$$

We need to find a lower bound for the minimum value achieved by the right-hand side of this equation. To prepare for this, first note that at the extreme value $\nu = 0$ we compute $\mathrm{ord}_p(\ f_{\gamma}^{(0)}) \geq \left(\frac{p}{(p+1)} - \epsilon_{\gamma,0} \right) \cdot \gamma$, and to study the remaining cases, $\nu = 1, \ldots, \gamma$, we look at the function

$$R(t) = t + \left(\frac{1}{p^{t-1}(p+1)} \right) (\gamma - t)$$

in the range $1 \leq t \leq \gamma$. This, by calculus, has a unique minimum at $t = t_{\gamma} \in (1, \gamma)$ given by the equation

$$\frac{p+1}{p} \cdot p^{t_{\gamma}} = \log(p) \cdot (\gamma - t_{\gamma}) + 1. \tag{5.4}$$

Define $e_{\gamma} = t_{\gamma} - \log_p(\gamma)$ and substituting, we get:

$$p^{e_{\gamma}} = \frac{p \log(p)}{p+1} - \frac{p \log(p)}{p+1} \frac{e_{\gamma}}{\gamma} + A_{\gamma} \tag{5.5}$$

where A_{γ} goes to zero, as γ goes to ∞.

If e_{γ} is positive we get that

$$p^{e_{\gamma}} \leq \frac{p \log(p)}{p+1} + A_{\gamma}$$

and so e_γ is bounded from above, independent of γ, while if $e_\gamma = -d_\gamma$ with d_γ positive, we have

$$\frac{1}{p^{d_\gamma}} = \frac{p\log(p)}{p+1} + \frac{p\log(p)}{p+1}\frac{d_\gamma}{\gamma} + A_\gamma.$$

Recall that since $t_\gamma > 0$ we also have $d_\gamma < \log_p(\gamma)$, so that the right hand side of the displayed equation tends to $\frac{p\log(p)}{p+1}$ as γ goes to ∞, so the equation forces d_γ to be bounded from above, as γ tends to ∞.

This discussion gives:

Lemma 5.10. *The quantity $|t_\gamma - \log_p(\gamma)|$ is bounded independent of γ.*

Substituting $t_\gamma = \log_p(\gamma) + e_\gamma$ in the defining equation for $R(t)$ and noting the boundedness of $|e_\gamma|$, we get that $|R(t_\gamma) - \log_p(\gamma)|$ is bounded as γ goes to ∞, thereby establishing our proposition.

□

Corollary 5.11. *For all $p \geq 5$, the Katz modular form $f = E_2$ is log-convergent and*

$$\liminf_{n\to\infty} \frac{a_f(n)}{\log(n)} \geq \frac{1}{\log(p)}.$$

Proof. The modular forms $V^\nu E_2^{(p)}$ are classical modular forms on $\Gamma_0(p^{\nu+1})$ and therefore formula (5.1) exhibits E_2 as having a Katz expansion of the shape of (5.3). Proposition 5.9 then implies the corollary. □

Remark 5.12. Is E_2 *precisely* log-convergent? The minimal c (cf. Definition 5.7) that can be taken in the log-convergence rate for $f = E_2$ is $\limsup_{n\to\infty}(a_f(n)/\log(n))$. Is this minimal c equal to $1/\log(p)$? It is for $p = 5$, as we will show in Section 6. The previous discussion tells us that, as a kind of generalization of the well-known congruence

$$E_2\mathcal{E}_{p-1} \equiv E_{p+1} \pmod{p},$$

we have that for any $\epsilon > 0$, and all but finitely many ν, there are classical modular forms $\mathcal{G}_\nu$ of level 1 and weight $2 + \nu(p-1)$ such that

$$E_2\mathcal{E}_{p-1}^{\nu} \equiv \mathcal{G}_\nu \pmod{p^{\lfloor(1-\epsilon)\log_p(\nu)\rfloor}}.$$

Let $\theta = qd/dq$ denote the standard shift operator; so that if $f = \sum_{n\geq 0} c_n q^n$, then $\theta(f) = \sum_{n\geq 0} nc_n q^n$. We have $\mathrm{ord}_p(\theta(f)) \geq \mathrm{ord}_p(f)$. The operator θ preserves Katz modular forms, and *almost* preserves classical modular forms in the sense that if f is a classical modular form of weight $k \geq 2$ then so is $F = \theta(f) - kfE_2/12$ (cf. [Kat73]). Note, also, that $\mathrm{ord}_p(F) \geq \mathrm{ord}_p(f)$.

Corollary 5.13. *The operator θ preserves log-convergent Katz modular forms.*

Proof. Let f be a log-convergent Katz p-integral modular form of weight k, of tame conductor N with a Katz expansion,

$$f = \sum_{\nu=0}^{\infty} p^{a(\nu)} f_\nu \mathcal{E}_{p-1}^{-\nu} \tag{5.6}$$

where $a(\nu) \geq c \cdot \log(\nu)$ for some positive c, and the f_ν's are classical p-integral modular forms on $\Gamma_0(N)$. Let $F_\nu = \theta(f_\nu) - (k + \nu(p-1)) f_\nu E_2/12$ (which is a classical modular form of weight $k + 2 + \nu(p-1)$ on $\Gamma_0(N)$). Put

$$G = \theta(E_{p-1}) - \frac{p-1}{12}\mathcal{E}_{p-1}E_2.$$

Apply the derivation θ to (5.6) to get

$$\theta(f) = \sum_{\nu=0}^{\infty} p^{a(\nu)} \Big\{ (F_\nu + (k + \nu(p-1)) f_\nu E_2/12)\mathcal{E}_{p-1}^{-\nu} - \\ \nu f_\nu \mathcal{E}_{p-1}^{-\nu-1}\left(G + \frac{p-1}{12}\mathcal{E}_{p-1}E_2\right)\Big\}.$$

or:

$$\theta(f) = A + BE_2 - C - DE_2,$$

where

$$\begin{aligned} A &= \sum_{\nu=0}^{\infty} p^{a(\nu)} F_\nu \mathcal{E}_{p-1}^{-\nu}, \\ B &= \sum_{\nu=0}^{\infty} p^{a(\nu)} (k + \nu(p-1)) f_\nu/12)\mathcal{E}_{p-1}^{-\nu}, \\ C &= \sum_{\nu=0}^{\infty} p^{a(\nu)} \nu f_\nu G \mathcal{E}_{p-1}^{-\nu-1}, \\ D &= \sum_{\nu=0}^{\infty} p^{a(\nu)} \frac{p-1}{12} \nu f_\nu \mathcal{E}_{p-1}. \end{aligned}$$

Now A, B, C, D are all log-convergent, as is E_2 by Corollary 5.11. Therefore so is $\theta(f)$. □

6 Precise log convergence of E_2 for $p = 2, 3, 5$

In this section we assume $p = 2$, 3 or 5 and let P, Q, R denote the Eisenstein series of level 1 of weights $2, 4, 6$, respectively, normalized so that the constant term in its Fourier expansion is 1. Let f be a Katz form of tame level 1 and weight k. Write $k = 4d + 6e$, with d an integer ≥ -1 and $e = 0$ or 1. Then $fQ^{-d}R^{-e}$ is a Katz form of weight 0, that is, a Katz function. Since 0 is the only supersingular value of j for $p = 2, 3, 5$, a Katz function has an expansion in powers of j^{-1} convergent everywhere on the disc $|j^{-1}| \leq 1$. Hence, putting $z = j^{-1}$, we can write

$$f = Q^d R^e \sum_{n=0}^{\infty} c_f(n) z^n = \sum_{n=0}^{\infty} R^e \Delta^n Q^{-3n+d}.$$

with $c_f(n) \in \mathbf{Q}_p$ and $c_f(n) \to 0$ as $n \to \infty$. Let

$$C_{f,p}(N) = \min_{n>N}(\mathrm{ord}_p(c_f(n))).$$

Theorem 6.1. *For $p = 5$, we have $C_{f,5}(N) = a_f(3N + 1 - d)$, for all large N.*

Proof. Notice that for $p = 5$, $\mathcal{E}_{p-1} = Q$. Let $\nu = 3N + 1 - d$ for large N. Then

$$Q^{\nu-1} f = \sum_{n=0}^{N} c(n) R^e \Delta^n Q^{3(N-n)} + R^e Q^d \sum_{n>N} c(n) z^n = F + G,$$

say. We have $\mathrm{ord}_5(G) = \min_{n>N}(\mathrm{ord}_5(c(n)) = C_{f,5}(N)$. [5]

Since F is a classical modular form of weight $12N + 6e$ it follows from the definition of a_f that $a_f(\nu) \geq C_{f,5}(N)$. On the other hand, since $\{R^e \Delta^n Q^{3(N-n)} : 0 \leq n \leq N\}$ is a basis for the space of classical modular forms of weight $12N + 6e$, it is clear that for any such classical form F', the difference $Q^{\nu-1} f - F'$ is a 5-adic Katz form which can be written as $R^e Q^{3N} g$ with g a Katz function whose z-expansion coefficients are $c(n)$ for $n > N$. Thus $\mathrm{ord}_5(Q^{\nu-1} f - F') \leq C_{f,5}(N)$. □

We have defined f to be log convergent if

$$\liminf_{n\to\infty} \frac{a_f(n)}{\log(n)} > 0,$$

and to be precisely log convergent if in addition

$$\limsup_{n\to\infty} \frac{a_f(n)}{\log(n)} < \infty.$$

Lemma 6.2. *Suppose $h(n)$ and $H(n)$ are nondecreasing funcions defined for all sufficiently large positive integers n. If for some integers $r > 0$ and s we have $H(N) = h(rN + s)$ for all sufficiently large integers N, then*

$$\liminf_{n\to\infty} \frac{h(n)}{\log(n)} = \liminf_{N\to\infty} \frac{H(N)}{\log(N)},$$

[5] To justify this claim we extend our definition of ord_p from the ring of Katz forms with Fourier coefficients in $\mathbf{Z}$ to the ring $\mathbf{Z}_p[[q]]$ of all formal power series with coefficients in $\mathbf{Z}$. Moreover, since $z \in q + q^2\mathbf{Z}_p[[q]]$, we have $\mathbf{Z}_p[[q]] = \mathbf{Z}_p[[z]]$, and for a formal series $g = \sum a_n q^n = \sum b^n z^n$, we have $\mathrm{ord}_p(g) = \min(\mathrm{ord}_p(a_n)) = \min(\mathrm{ord}_p(b_n))$. Also (Gauss Lemma) the rule $\mathrm{ord}(g_1 g_2) = \mathrm{ord}(g_1) + \mathrm{ord}(g_2)$ holds. Since $\mathrm{ord}_5(R) = \mathrm{ord}_5(Q) = 0$, it follows that $\mathrm{ord}_5(G) = C_{f,5}(N)$ as claimed.

and

$$\limsup_{n\to\infty} \frac{h(n)}{\log(n)} = \limsup_{N\to\infty} \frac{H(N)}{\log(N)}.$$

Proof. We use the fact that $\frac{\log(rx+s)}{\log(x)} \to 1$ as $x \to \infty$. For n and N related by

$$rN + s \le n \le r(N+1) + s$$

we have

$$\frac{h(n)}{\log(n)} \le \frac{h(r(N+1)+s}{\log(rN+s)} = \frac{H(N+1)}{\log(N+1)} \cdot \frac{\log(N+1)}{\log(rN+s)}.$$

Similarly,

$$\frac{h(n)}{\log(n)} \ge \frac{h(rN+s}{\log(r(N+1)+s)} = \frac{H(N)}{\log(N)} \cdot \frac{\log(N)}{\log(r(N+1)+s)}.$$

This proves the lemma, because the second factor of the right hand term in each line approaches 1 as N goes to infinity. □

Theorem 6.1 and Lemma 6.2 show that for $p = 5$ we can replace a_f by C_f in the definition of log convergent and precisely log convergent. Therefore we define log convergent and precisely log convergent for $p = 2$ and $p = 3$ by using $C_{f,p}$ as a replacement for a_f.

Theorem 6.3. *For $p = 2, 3$ or 5, the weight 2 Eisenstein series $P = \mathbf{E}_2$ is precisely log convergent. In fact,*

$$\lim_{n\to\infty} \frac{C_{P,p}(n)}{\log(n)} = \frac{1}{\log(p)}.$$

During the proof of this theorem we write $c(n) = c_P(n)$ and $C_p(n) = C_{P,p}$.

The cases $p = 2, 3$ follow immediately from results of Koblitz (cf. [Kob77]). Koblitz writes $P = \sum a_n j^{-n} \frac{qdj}{jdq}$. Since $dj/j = -dz/z$, and as we will see later in this proof, $qdz/zdq = R/Q$, Koblitz's a_n is the negative of our $c(n)$, hence $\mathrm{ord}_p(c(n)) = \mathrm{ord}_p(a_n)$. Koblitz shows that if we let $l_p(n) = 1 + \lfloor \log(n)/\log(p) \rfloor$, the number of digits in the expression of n in base p, and let $s_p(n)$ denote the sum of those digits, then $\mathrm{ord}_2(c(n)) = l_2(n) + 3s_2(n)$ and $\mathrm{ord}_3(c(n)) = l_3(n) + s_3(n)$. From this it is an easy exercise to show

$$C_2(n) = \lfloor \log(n+1)/\log(2) \rfloor + 4 \quad \text{and} \quad C_3(n) = \lfloor (\log(n+1)/\log(3) \rfloor + 2,$$

formulas from which cases $p = 2$ and $p = 3$ of the theorem are evident.

Investigating the case $p = 5$ we found experimentally with a PARI program that the following conjecture holds for $n < 1029$.

Conjecture 6.4. *We have $\mathrm{ord}_5(c(n)) \ge l_5(2n)$, with equality if n written in base 5 contains only the digits 0,1 or 2, but no 3 or 4.*

It is easy to see that Conjecture 6.4 implies that

$$\limsup_{n\to\infty} \frac{C_5(n)}{\log(n)} = \frac{1}{\log(5)}.$$

We already know from Corollary 5.11 that

$$\liminf_{n\to\infty} \frac{a_P(n)}{\log(n)} \geq \frac{1}{\log(5)}.$$

By Lemma 6.2, this is equivalent to

$$\liminf_{n\to\infty} \frac{C_{P,5}(n)}{\log(n)} \geq \frac{1}{\log(5)}.$$

Hence to finish the proof of Theorem 6.3, we need only prove

$$\limsup_{n\to\infty} \frac{C_{P,5}(n)}{\log(n)} \leq \frac{1}{\log(5)}. \tag{6.1}$$

To prove (6.1) it is enough to prove that Conjecture 6.4 holds for $n = 5^m$, that is, $\mathrm{ord}_5(c(n)) = m+1$. Indeed that equality implies that $C_5(n) \leq m+1$ for $n < 5^m$ and, choosing m such that $5^{m-1} \leq n < 5^m$, shows that for every n we have $C_5(n) \leq m+1 \leq \log(n)/\log(5) + 2$.

To prove $\mathrm{ord}_5(c(n)) = m+1$ we use two lemmas.

Lemma 6.5. *We have* $\frac{PQ}{R} - 1 = 3\frac{zdQ}{Qdz}$.

Proof. Let θ denote the classical operator qd/dq. From the formula $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$ we get by logarithmic differentiation the classical formula

$$\frac{\theta\Delta}{\Delta} = P.$$

From $z = 1/j = \Delta/Q^3$ we get by logarithmic differentiation that

$$\frac{\theta z}{z} = \frac{\theta\Delta}{\Delta} - 3\frac{\theta Q}{Q} = P - 3\frac{\theta Q}{Q}.$$

By a formula of Ramanujan (cf. [Ser73, Thm. 4]) we have

$$3\frac{\theta Q}{Q} = P - \frac{R}{Q}.$$

Substituting gives

$$\frac{\theta z}{z} = \frac{R}{Q},$$

and dividing the next to last equation by the last proves the lemma. □

Lemma 6.6. *Let* $F = \sum_{n\geq 1} \sigma_3(n) q^n$, *so that* $Q = 1 + 240F$. *Then* $F \equiv \sum_{m\geq 0}(z^{5^m} + z^{2\cdot 5^m})$ (mod 5).

Proof. Guessing this result by computer experiment, we asked Serre for a proof. He immediately supplied two, one of which is the following. During the rest of this proof all congruences are understood to be modulo 5. Since $F = z + 3z^2 + \cdots$, the statement to be proved is equivalent to $F - F^5 \equiv z + 3z^2$. Using the trivial congruence $Q \equiv 1$ and the congruence $P \equiv R$ (the case $p = 5$ of a congruence of Swinnerton-Dyer, (cf. [Ser73, Thm. 5]), we note that

$$z = \Delta/Q^3 \equiv \Delta = (Q^3 - R^2)/1728 \equiv 2 - 2R^2.$$

The case $p = 5, k = 4$ of formula (**) in section 2.2 of [Ser73] reads $F - F^5 \equiv \theta^3 R$. By Ramanujan's formula

$$\theta R = (PR - Q^2)/2 \equiv 3R^2 - 3,$$

one finds that indeed

$$\theta^3 R \equiv 2R^4 - R^2 - 1 \equiv z + 3z^2,$$

which proves Lemma 6.6. □

Let $F = \sum_{n \geq 1} b(n) z^n$. By Lemma 6.6, $b(5^m)$ and $b(2 \cdot 5^m)$ are not divisible by 5. Therefore the 5^mth and $2 \cdot 5^m$th coefficients of $zdF/dz = \sum_{n \geq 1} nb(n) z^n$ are divisible exactly by 5^m. By Lemma 6.5 we have

$$\sum_{n \geq 1} c(n) z^n = \frac{PQ}{R} - 1 = 3\frac{zdQ}{Qdz} = 3\frac{240 zdF}{(1 + 240F)dz}.$$

This shows that $\text{ord}_5(c(5^m)) = \text{ord}_5(c(2 \cdot 5^m)) = m + 1$ thereby completing the proof of Theorem 6.3.

Remark 6.7. For $p = 2$ or 3 a simple analogue of Lemma 6.6 holds, namely $F \equiv \sum_{m \geq 0} z^{p^m} \pmod{p}$. This can be used to obtain Koblitz's result for the very special case $n = p^m$.

7 Discussion

7.1 Log convergence

The running hypothesis in Section 5 is that $p \geq 5$, but in Section 6 we considered only $p = 2, 3, 5$. In dealing with the different primes, our discussion changes strikingly, depending on the three slightly different cases:

(1) $p = 2, 3$

(2) $p = 5$

(3) $p \geq 5$

For (7.1), in Section 6 we used expansions in powers of $z = 1/j$ to give a careful analysis of convergence rates, and in contrast, the general discussion of Section 5 *must* keep away from those cases $p = 2, 3$, in order to maintain the formulation that it currently has. The prime $p = 5$ is in a very fortunate position because it can be covered by the general discussion a la (7.1); but we have also given a precise "power series in $1/j$" treatment of $p = 5$. These issues suggest four questions:

1. Is there any relationship between the convergence rate analysis we give, and computation-time estimates for the actual algorithms?

2. We have produced an algebra of log-convergent modular forms, and it has at least one new element that the overconvergent forms do not have, namely $\mathbf{E}_2$. Moreover, it is closed under the action of θ, i.e., "Tate twist". Are there other interesting Hecke eigenforms in this algebra that we should know about? Going the other way, are there any Hecke eigenforms that are *not* log-convergent? Is there something corresponding to the "eigencurve" (it would have to be, at the very least, a surface) that p-adically interpolates log-convergent eigenforms? Is a limit (in the sense of ord_p's of Fourier coefficients) of log-convergent eigenforms again log-convergent? For this last question to make sense, we probably need to know the following:

3. Is there a rigid-analytic growth type of definition (growth at the rim of the Hasse domain) that characterizes log-convergence, just as there is such a definition characterizing overconvergence?

4. Almost certainly one could treat the case $p = 7$ by expansions in powers of $1/(j - 1728) = \Delta/R^2$ in the same way that we did $p = 5$ with powers of $1/j = \Delta/Q^3$. The case $p = 13$ might be more interesting.

7.2 Uniformity in the algorithms

We are most thankful to Kiran Kedlaya and Alan Lauder for some e-mail communications regarding an early draft of our article. The topic they address is the extent to which the algorithms for the computation of $\mathbf{E}_2$ of an elliptic curve are "uniform" in the elliptic curve, and, in particular, whether one can get fast algorithms for computing $\mathbf{E}_2$ of specific families of elliptic curves. In this section we give a brief synopsis of their comments.

A "reason" why $\mathbf{E}_2$ should turn out not to be overconvergent is that Katz's formula relates it to the direction of the unit-root subspace in one-dimensional de Rham cohomology, and that seems only to make (at least naive) sense in the ordinary case (and not for points in a supersingular disc, not even ones close to the boundary).

Nevertheless, part of the algorithm has good uniformity properties.

1. *Calculating the matrix of Frobenius:* One can calculate the matrix of Frobenius for, say, all elliptic curves in the Legendre family (or any one-parameter family) and the result is overconvergent everywhere, so this should be relatively efficient. This can be done either by the algorithm developed by Kedlaya, or also using the Gauss-Manin connection, as in Lauder's work, which is probably faster. An approach to computing the "full" Frobenius matrix "all at once" for elliptic curves in the Legendre family has been written up and implemented in Magma by Ralf Gerkmann: See [Ger05] for the paper and program. Lauder's paper [Lau03] also discusses Kedlaya's algorithm "all at once" for a one-parameter family of hyperelliptic curves using the Gauss-Manin connection.

2. *Extracting the unit root subspace in de Rham cohomology:* To compute $\mathbf{E}_2$ for an individual elliptic curve, one can specialize the Frobenius matrix and extract the unit root. But extracting only the unit root part over the entire family at once would involve non-overconvergent series, and consequently might be slow. The *unit root zeta function*, which encodes the unit root of Frobenius over a family of ordinary elliptic curves, has been very well studied by Dwork and Wan (cf. [Wan99]).

7.3 Other future projects

1. Explicitly compute anticyclotomic p-adic heights, and apply this to the study of universal norm questions that arise in [RM05].

2. Further investigate Kedlaya's algorithm with a parameter in connection with log convergence and computation of heights.

3. Determine if the equality $\lim_{n\to\infty} a_P(n)/\log(n) = 1/\log(p)$ holds for all primes p, as it does for $p = 5$ by Theorem 6.3.

References

[Bes04] Amnon Besser, *The p-adic height pairings of Coleman-Gross and of Nekovář*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 13–25. MR 2076563 (2005f:11130)

[Blu] Antonia W. Bluher, *A Leisurely Introduction to Formal Groups and Elliptic Curves,* `http://www.math.uiuc.edu/algebraic-number-theory/0076/`.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[Col91] Robert F. Coleman, *The universal vectorial bi-extension and p-adic heights*, Invent. Math. 103 (1991), no. 3, 631–650. MR 1091621 (92k:14021)

[CGJ95] Robert F. Coleman, Fernando Q. Gouvêa, and Naomi Jochnowitz, *E_2, Θ, and overconvergence*, Internat. Math. Res. Notices (1995), no. 1, 23–41 (electronic). MR 1317641 (96d:11047)

[Ger05] Ralf Gerkmann, `http://www.mathematik.uni-mainz.de/~gerkmann/ellcurves.html`, (2005).

[Gre03] Ralph Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. 136 (2003), no. 3, 255–297. MR 1977007 (2004c:11097)

[GJP$^+$05] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, (Submitted) `http://modular.fas.harvard.edu/papers/bsdalg/` (2005).

[Gou88] F. Q. Gouvêa, *Arithmetic of p-adic modular forms*, Springer-Verlag, Berlin, 1988. MR 91e:11056

[IW03] Adrian Iovita and Annette Werner, *p-adic height pairings on abelian varieties with semistable ordinary reduction*, J. Reine Angew. Math. 564 (2003), 181–203. MR 2021039 (2004j:11066)

[SJ05] William Stein and David Joyner, *Sage: System for algebra and geometry experimentation*, Communications in Computer Algebra (SIGSAM Bulletin) (July 2005), `http://sage.sourceforge.net/`.

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR 0447119 (56 #5434)

[Kat76] ———, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) 104 (1976), no. 3, 459–571. MR 0506271 (58 #22071)

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. 16 (2001), no. 4, 323–338. MR 1877805 (2002m:14019)

[Ked03] K. S. Kedlaya, *Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc.* 16 *(2001), no. 4, 323–338*, J. Ramanujan Math. Soc. 18 (2003), no. 4, 417–418, Dedicated to Professor K. S. Padmanabhan. MR 2 043 934

[Kob77] Neil Koblitz, 2*-adic and* 3*-adic ordinals of the (1/j)-expansion coefficients for the weight 2 Eisenstein series, Bull. L.M.S. 9 (1977), 188-192.*

[Lan95] S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[Lau03] A. G. B. Lauder, *Rigid cohomology and p-adic point counting*, to appear in a special issue of J. de Thorie des Nombres de Bordeaux, `http://www.maths.ox.ac.uk/~lauder/`.

[LW02] A. G. B. Lauder and D. Wan, *Counting rational points on varieties over finite fields of small characteristic*, to appear in an MSRI Computational Number Theory Proceedings (October, 2002).

[MR04] Barry Mazur and Karl Rubin, *Pairings in the arithmetic of elliptic curves*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 151–163. MR MR2058649 (2005g:11095)

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237. MR 717595 (85j:14081)

[MT87] ______, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. 54 (1987), no. 2, 711–750. MR 899413 (88k:11039)

[MT91] ______, *The p-adic sigma function*, Duke Math. J. 62 (1991), no. 3, 663–688. MR 93d:11059

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. 84 (1986), no. 1, 1–48. MR 830037 (87e:11076)

[Nek93] Jan Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202. MR 1263527 (95j:11050)

[Nek03] ______, *Selmer Complexes*, 2003, see `http://www.math.jussieu.fr/~nekovar/pu/`.

[Pla94] Andrew Plater, *Supersingular p-adic height pairings on elliptic curves*, Arithmetic geometry (Tempe, AZ, 1993), Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 95–105. MR 1299736 (95h:11056)

[PR03a] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. 12 (2003), no. 2, 155–186. MR 2016704 (2005h:11138)

[PR03b] ______, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. 12 (2003), no. 2, 155–186. MR 2016704

[RM05] K. Rubin and B. Mazur, *Organizing the arithmetic of elliptic curves*, in preparation.

[Sch82] Peter Schneider, *p-adic height pairings. I*, Invent. Math. 69 (1982), no. 3, 401–409. MR 679765 (84e:14034)

[Sch85] ______, *p-adic height pairings. II*, Invent. Math. 79 (1985), no. 2, 329–374. MR 778132 (86j:11063)

[Ser73] J-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416 (Berlin), Springer, 1973, pp. 319–338. Lecture Notes in Math., Vol. 317.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Wan99] Daqing Wan, *Dwork's conjecture on unit root zeta functions*, Ann. of Math. (2) 150 (1999), no. 3, 867–927. MR MR1740990 (2001a:11108)

[Wut04] Christian Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) 70 (2004), no. 1, 23–40. MR 2064750

[Zar90] Yuri G. Zarhin, *p-adic heights on abelian varieties*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, pp. 317–341. MR 1042777 (91f:11043)

Barry Mazur
Department of Mathematics
Harvard University
mazur@math.harvard.edu

John Tate
Department of Mathematics
University of Texas at Austin
tate@math.utexas.edu

William A. Stein
Department of Mathematics
University of California at San Diego
wstein@ucsd.edu

Kida's Formula and Congruences

To John Coates, for his 60th birthday

Robert Pollack and Tom Weston

Received: August 30, 2005
Revised: June 21, 2006

Abstract. We consider a generalization of a result of Kida in classical Iwasawa theory which relates Iwasawa invariants of p-extensions of number fields. In this paper, we consider Selmer groups of a general class of Galois representations which includes the case of p-ordinary Hilbert modular forms and p-supersingular modular forms.

2000 Mathematics Subject Classification: 11R23
Keywords and Phrases: Iwasawa theory, Kida's formula

1. Introduction

Let f be a modular eigenform of weight at least two and let F be a finite abelian extension of $\mathbf{Q}$. Fix an odd prime p at which f is ordinary in the sense that the p^{th} Fourier coefficient of f is not divisible by p. In Iwasawa theory, one associates two objects to f over the cyclotomic $\mathbf{Z}_p$-extension F_∞ of F: a Selmer group $\mathrm{Sel}(F_\infty, A_f)$ (where A_f denotes the divisible version of the two-dimensional Galois representation attached to f) and a p-adic L-function $L_p(F_\infty, f)$. In this paper we prove a formula, generalizing work of Kida and Hachimori–Matsuno, relating the Iwasawa invariants of these objects over F with their Iwasawa invariants over p-extensions of F.

For Selmer groups our results are significantly more general. Let T be a lattice in a nearly ordinary p-adic Galois representation V; set $A = V/T$. When $\mathrm{Sel}(F_\infty, A)$ is a cotorsion Iwasawa module, its Iwasawa μ-invariant $\mu^{\text{alg}}(F_\infty, A)$ is said to vanish if $\mathrm{Sel}(F_\infty, A)$ is cofinitely generated and its λ-invariant $\lambda^{\text{alg}}(F_\infty, A)$ is simply its p-adic corank. We prove the following result relating these invariants in a p-extension.

Theorem 1. *Let F'/F be a finite Galois p-extension that is unramified at all places dividing p. Assume that T satisfies the technical assumptions (1)–(5) of Section 2. If $\mathrm{Sel}(F_\infty, A)$ is Λ-cotorsion with $\mu^{\mathrm{alg}}(F_\infty, A) = 0$, then $\mathrm{Sel}(F'_\infty, A)$ is Λ-cotorsion with $\mu^{\mathrm{alg}}(F'_\infty, A) = 0$. Moreover, in this case*

$$\lambda^{\mathrm{alg}}(F'_\infty, A) = [F'_\infty : F_\infty] \cdot \lambda^{\mathrm{alg}}(F_\infty, A) + \sum_{w'} m(F'_{\infty,w'}/F_{\infty,w}, V)$$

where the sum extends over places w' of F'_∞ which are ramified in F'_∞/F_∞. If V is associated to a cuspform f and F' is an abelian extension of $\mathbf{Q}$, then the same results hold for the analytic Iwasawa invariants of f.

Here $m(F'_{\infty,w'}/F_{\infty,w}, V)$ is a certain difference of local multiplicities defined in Section 2.1. In the case of Galois representations associated to Hilbert modular forms, these local factors can be made quite explicit; see Section 4.1 for details. It follows from Theorem 1 and work of Kato that if the p-adic main conjecture holds for a modular form f over $\mathbf{Q}$, then it holds for f over all abelian p-extensions of $\mathbf{Q}$; see Section 4.2 for details.

These Riemann-Hurwitz type formulas were first discovered by Kida [5] in the context of λ-invariants of CM fields. More precisely, when F'/F is a p-extension of CM fields and $\mu^-(F_\infty/F) = 0$, Kida gave a precise formula for $\lambda^-(F'_\infty/F')$ in terms of $\lambda^-(F_\infty/F)$ and local data involving the primes that ramify in F'/F. (See also [4] for a representation theoretic interpretation of Kida's result.) A similar formula in a somewhat different setting was given for elliptic curves with complex multiplication at ordinary primes by Wingberg [12]; Hachimori–Matsuno [3] established the cyclotomic version in general. The analytic analogue was first established for ideal class groups by Sinnott [10] and for elliptic curves by Matsuno [7].

Our proof is most closely related to the arguments in [10] and [7] where congruences implicitly played a large role in their study of analytic λ-invariants. In this paper, we make the role of congruences more explicit and apply these methods to study both algebraic and analytic λ-invariants.

As is usual, we first reduce to the case where F'/F is abelian. (Some care is required to show that our local factors are well behaved in towers of fields; this is discussed in Section 2.1.) In this case, the λ-invariant of V over F' can be expressed as the sum of the λ-invariants of twists of V by characters of $\mathrm{Gal}(F'/F)$. The key observation (already visible in both [10] and [7]) is that since $\mathrm{Gal}(F'/F)$ is a p-group, all of its characters are trivial modulo a prime over p and, thus, the twisted Galois representations are all congruent to V modulo a prime over p. The algebraic case of Theorem 1 then follows from the results of [11] which gives a precise local formula for the difference between λ-invariants of congruent Galois representations. The analytic case is handled similarly using the results of [1].

The basic principle behind this argument is that a formula relating the Iwasawa invariants of congruent Galois representations should imply of a transition formula for these invariants in p-extensions. As an example of this, in Section 4.3, we use results of [2] to prove a Kida formula for the Iwasawa invariants (in the sense of [8, 6, 9]) of weight 2 modular forms at supersingular primes.

Acknowledgments: We would like to thank the anonymous referee for several helpful comments and for pointing out some errors in an earlier draft of this paper.

2. Algebraic invariants

2.1. Local preliminaries. We begin by studying the local terms that appear in our results. Fix distinct primes ℓ and p and let L denote a finite extension of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}_\ell$. Fix a field K of characteristic zero and a finite-dimensional K-vector space V endowed with a continuous K-linear action of the absolute Galois group G_L of L. Set

$$m_L(V) := \dim_K \left(V_{I_L}\right)^{G_L},$$

the multiplicity of the trivial representation in the I_L-coinvariants of V. Note that this multiplicity is invariant under extension of scalars, so that we can enlarge K as necessary.

Let L' be a finite Galois p-extension of L. Note that L' must be cyclic and totally ramified since L contains the $\mathbf{Z}_p$-extension of $\mathbf{Q}_\ell$. Let G denote the Galois group of L'/L. Assuming that K contains all $[L':L]^{\text{th}}$ roots of unity, for a character $\chi : G \to K^\times$ of G, we set $V_\chi = V \otimes_K K(\chi)$ with $K(\chi)$ a one-dimensional K-vector space on which G acts via χ. We define

$$m(L'/L, V) := \sum_{\chi \in G^\vee} m_L(V) - m_L(V_\chi)$$

where $G^\vee$ denotes the K-dual of G.

The next result shows how these invariants behave in towers of fields.

Lemma 2.1. *Let L'' be a finite Galois p-extension of L and let L' be a Galois extension of L contained in L''. Assume that K contains all $[L'':L]^{th}$ roots of unity. Then*

$$m(L''/L, V) = [L'':L'] \cdot m(L'/L, V) + m(L''/L', V).$$

Proof. Set $G = \mathrm{Gal}(L''/L)$ and $H = \mathrm{Gal}(L''/L')$. Consider the Galois group $G_L/I_{L''}$ over L of the maximal unramified extension of L''. It sits in an exact sequence

$$0 \to G_{L''}/I_{L''} \to G_L/I_{L''} \to G \to 0 \tag{1}$$

which is in fact split since the maximal unramified extensions of both L and L'' are obtained by adjoining all prime-to-p roots of unity.

Fix a character $\chi \in G^\vee$. We compute

$$\begin{aligned} m_L(V_\chi) &= \dim_K \big((V_\chi)_{I_L}\big)^{G_L} \\ &= \dim_K \Big(\big(((V_\chi)_{I_{L''}})_G\big)^{G_{L''}}\Big)^G \\ &= \dim_K \Big(\big(((V_\chi)_{I_{L''}})^{G_{L''}}\big)_G\Big)^G \quad \text{since (1) is split} \\ &= \dim_K \Big(\big((V_\chi)_{I_{L''}}\big)^{G_{L''}}\Big)^G \quad \text{since } G \text{ is finite cyclic} \\ &= \dim_K \big((V_{I_{L''}})^{G_{L''}} \otimes \chi\big)^G \quad \text{since } \chi \text{ is trivial on } G_{L''}. \end{aligned}$$

The lemma thus follows from the following purely group-theoretical statement applied with $W = (V_{I_{L''}})^{G_{L''}}$: for a finite dimensional representation W of a finite abelian group G over a field of characteristic zero containing $\mu_{\#G}$, we have

$$\sum_{\chi \in G^\vee} \big(\langle W, 1\rangle_G - \langle W, \chi\rangle_G\big) = \\ \#H \cdot \sum_{\chi \in (G/H)^\vee} \big(\langle W, 1\rangle_G - \langle W, \chi\rangle_G\big) + \sum_{\chi \in H^\vee} \big(\langle W, 1\rangle_H - \langle W, \chi\rangle_H\big)$$

for any subgroup H of G; here $\langle W, \chi\rangle_G$ (resp. $\langle W, \chi\rangle_H$) is the multiplicity of the character χ in W regarded as a representation of G (resp. H). To prove this, we compute

$$\begin{aligned} &\sum_{\chi \in G^\vee} \big(\langle W, 1\rangle_G - \langle W, \chi\rangle_G\big) \\ &= \#G \cdot \langle W, 1\rangle_G - \Big\langle W, \operatorname{Ind}_1^G 1\Big\rangle_G \\ &= \#G \cdot \langle W, 1\rangle_G - \#H \cdot \Big\langle W, \operatorname{Ind}_H^G 1\Big\rangle_G + \#H \cdot \Big\langle W, \operatorname{Ind}_H^G 1\Big\rangle_G - \Big\langle W, \operatorname{Ind}_1^G 1\Big\rangle_G \\ &= \#H \cdot \sum_{\chi \in (G/H)^\vee} \big(\langle W, 1\rangle_G - \langle W, \chi\rangle_G\big) + \sum_{\chi \in H^\vee} \Big(\Big\langle W, \operatorname{Ind}_H^G 1\Big\rangle_G - \Big\langle W, \operatorname{Ind}_H^G \chi\Big\rangle_G\Big) \\ &= \#H \cdot \sum_{\chi \in (G/H)^\vee} \big(\langle W, 1\rangle_G - \langle W, \chi\rangle_G\big) + \sum_{\chi \in H^\vee} \big(\langle W, 1\rangle_H - \langle W, \chi\rangle_H\big) \end{aligned}$$

by Frobenius reciprocity. □

2.2. Global preliminaries. Fix a number field F; for simplicity we assume that F is either totally real or totally imaginary. Fix also an odd prime p and a finite extension K of $\mathbf{Q}_p$; we write $\mathcal{O}$ for the ring of integers of K, π for a fixed choice of uniformizer of $\mathcal{O}$, and $k = \mathcal{O}/\pi$ for the residue field of $\mathcal{O}$.

Let T be a nearly ordinary Galois representation over F with coefficients in $\mathcal{O}$; that is, T is a free $\mathcal{O}$-module of some rank n endowed with an $\mathcal{O}$-linear action of the absolute Galois group G_F, together with a choice for each place v of F dividing p of a complete flag

$$0 = T_v^0 \subset T_v^1 \subset \cdots \subset T_v^n = T$$

stable under the action of the decomposition group $G_v \subseteq G_F$ of v. We make the following assumptions on T:

(1) For each place v dividing p we have
$$\left(T_v^i/T_v^{i-1}\right) \otimes k \ncong \left(T_v^j/T_v^{j-1}\right) \otimes k$$
as $k[G_v]$-modules for all $i \neq j$;

(2) If F is totally real, then $\operatorname{rank} T^{c_v=1}$ is independent of the archimedean place v (here c_v is a complex conjugation at v);

(3) If F is totally imaginary, then n is even.

Remark 2.2. The conditions above are significantly more restrictive than are actually required to apply the results of [11]. As our main interest is in abelian (and thus necessarily Galois) extensions of $\mathbf{Q}$, we have chosen to include the assumptions (2) and (3) to simplify the exposition. The assumption (1) is also stronger than necessary: all that is actually needed is that the centralizer of $T \otimes k$ consists entirely of scalars and that $\mathfrak{gl}_n/\mathfrak{b}_v$ has trivial adjoint G_v-invariants for all places v dividing p; here $\mathfrak{gl}_n$ denotes the p-adic Lie algebra of GL_n and $\mathfrak{b}_v$ denotes the p-adic Lie algebra of the Borel subgroup associated to the complete flag at v. In particular, when T has rank 2, we may still allow the case that $T \otimes k$ has the form
$$\begin{pmatrix} \chi & * \\ 0 & \chi \end{pmatrix}$$
so long as $*$ is non-trivial. (Equivalently, if T is associated to a modular form f, the required assumption is that f is *p-distinguished.*)

Set $A = T \otimes_{\mathcal{O}} K/\mathcal{O}$; it is a cofree $\mathcal{O}$-module of corank n with an $\mathcal{O}$-linear action of G_F. Let c equal the rank of $T_v^{c_v=1}$ (resp. $n/2$) if F is totally real (resp. totally imaginary) and set
$$A_v^{\mathrm{cr}} := \operatorname{im}\left(T_v^c \otimes_{\mathcal{O}} K \hookrightarrow T \otimes_{\mathcal{O}} K \twoheadrightarrow A\right).$$
We define the Selmer group of A over the cyclotomic $\mathbf{Z}_p$-extension F_∞ of F by
$$\mathrm{Sel}(F_\infty, A) = \ker\left(H^1(F_\infty, A) \to \left(\bigoplus_{w \nmid p} H^1(F_{\infty,w}, A)\right) \times \left(\bigoplus_{w \mid p} H^1(F_{\infty,w}, A/A_v^{\mathrm{cr}})\right)\right).$$
The Selmer group $\mathrm{Sel}(F_\infty, A)$ is naturally a module for the Iwasawa algebra $\Lambda_{\mathcal{O}} := \mathcal{O}[[\mathrm{Gal}(F_\infty/F)]]$. If $\mathrm{Sel}(F_\infty, A)$ is $\Lambda_{\mathcal{O}}$-cotorsion (that is, if the dual of $\mathrm{Sel}(F_\infty, A)$ is a torsion $\Lambda_{\mathcal{O}}$-module), then we write $\mu^{\mathrm{alg}}(F_\infty, A)$ and $\lambda^{\mathrm{alg}}(F_\infty, A)$ for its Iwasawa invariants; in particular, $\mu^{\mathrm{alg}}(F_\infty, A) = 0$ if and only if $\mathrm{Sel}(F_\infty, A)$ is a cofinitely generated $\mathcal{O}$-module, while $\lambda^{\mathrm{alg}}(F_\infty, A)$ is the $\mathcal{O}$-corank of $\mathrm{Sel}(F_\infty, A)$.

Remark 2.3. In the case that T is in fact an *ordinary* Galois representation (meaning that the action of inertia on each T_v^i/T_v^{i-1} is by an integer power e_i (independent of v) of the cyclotomic character such that $e_1 > e_2 > \ldots > e_n$), then our Selmer group $\mathrm{Sel}(F_\infty, A)$ is simply the Selmer group in the sense of Greenberg of a twist of A; see [11, Section 1.3] for details.

2.3. Extensions. Let F' be a finite Galois extension of F with degree equal to a power of p. We write F'_∞ for the cyclotomic $\mathbf{Z}_p$-extension of F' and set $G = \mathrm{Gal}(F'_\infty/F_\infty)$. Note that T satisfies hypotheses (1)–(3) over F' as well, so that we may define $\mathrm{Sel}(F'_\infty, A)$ analogously to $\mathrm{Sel}(F_\infty, A)$. (For (1) this follows from the fact that G_v acts on $(T_v^i/T_v^{i-1}) \otimes k$ by a character of prime-to-p order; for (2) and (3) it follows from the fact that p is assumed to be odd.)

Lemma 2.4. *The restriction map*

$$\mathrm{Sel}(F_\infty, A) \to \mathrm{Sel}(F'_\infty, A)^G \tag{2}$$

has finite kernel and cokernel.

Proof. This is straightforward from the definitions and the fact that G is finite and A is cofinitely generated; see [3, Lemma 3.3] for details. □

We can use Lemma 2.4 to relate the μ-invariants of A over F_∞ and F'_∞.

Corollary 2.5. *If* $\mathrm{Sel}(F_\infty, A)$ *is* Λ*-cotorsion with* $\mu^{\mathrm{alg}}(F_\infty, A) = 0$*, then* $\mathrm{Sel}(F'_\infty, A)$ *is* Λ*-cotorsion with* $\mu^{\mathrm{alg}}(F'_\infty, A) = 0$.

Proof. This is a straightforward argument using Lemma 2.4 and Nakayama's lemma for compact local rings; see [3, Corollary 3.4] for details. □

Fix a finite extension K' of K containing all $[F' : F]^{\mathrm{th}}$ roots of unity. Consider a character $\chi : G \to \mathcal{O}'^\times$ taking values in the ring of integers $\mathcal{O}'$ of K'; note that χ is necessarily even since $[F' : F]$ is odd. We set

$$A_\chi = A \otimes_{\mathcal{O}} \mathcal{O}'(\chi)$$

where $\mathcal{O}'(\chi)$ is a free $\mathcal{O}'$-module of rank one with G_{F_∞}-action given by χ. If we give A_χ the induced complete flags at places dividing p, then A_χ satisfies hypotheses (1)–(3) and we have

$$A^{\mathrm{cr}}_{\chi,v} = A^{\mathrm{cr}}_v \otimes_{\mathcal{O}} \mathcal{O}'(\chi) \subseteq A_\chi$$

for each place v dividing p. We write $\mathrm{Sel}(F_\infty, A_\chi)$ for the corresponding Selmer group, regarded as a $\Lambda_{\mathcal{O}'}$-module; in particular, by $\lambda^{\mathrm{alg}}(F_\infty, A_\chi)$ we mean the $\mathcal{O}'$-corank of $\mathrm{Sel}(F_\infty, A_\chi)$, rather than the $\mathcal{O}$-corank. We write $G^\vee$ for the set of all characters $\chi : G \to \mathcal{O}'^\times$.

Proposition 2.6. *Assume that* $\mathrm{Sel}(F_\infty, A)$ *is* Λ*-cotorsion with* $\mu^{\mathrm{alg}}(F_\infty, A) = 0$*. If G is an abelian group, then there is a natural map*

$$\bigoplus_{\chi \in G^\vee} \mathrm{Sel}(F_\infty, A_\chi) \to \mathrm{Sel}(F'_\infty, A) \otimes_{\mathcal{O}} \mathcal{O}'$$

with finite kernel and cokernel.

Proof. First note that as $\mathcal{O}'[[G_{F'}]]$-modules we have

$$A \otimes_{\mathcal{O}} \mathcal{O}' \cong A_\chi$$

from which it easily follows that

$$\left(\mathrm{Sel}(F'_\infty, A) \otimes_{\mathcal{O}} \mathcal{O}'(\chi)\right)^G = \mathrm{Sel}(F'_\infty, A_\chi)^G. \tag{3}$$

Also, for any cofinitely generated $\mathcal{O}[G]$-module S, the natural map

$$\bigoplus_{\chi \in G^\vee} (S \otimes \mathcal{O}'(\chi))^G \to S \otimes \mathcal{O}' \tag{4}$$

has finite kernel and cokernel. Since we are assuming that $\mu^{\mathrm{alg}}(F_\infty, A) = 0$, we may take $S = \mathrm{Sel}(F'_\infty, A)$ in (4); combining this with (3) yields a map

$$\bigoplus_{\chi \in G^\vee} (\mathrm{Sel}(F'_\infty, A_\chi))^G \to \mathrm{Sel}(F'_\infty, A_\chi) \otimes \mathcal{O}'$$

with finite kernel and cokernel. Now applying Lemma 2.4 for each twist A_χ, we obtain our proposition. □

As an immediate corollary, we have the following.

Corollary 2.7. *If* $\mathrm{Sel}(F_\infty, A)$ *is* Λ*-cotorsion with* $\mu^{\mathrm{alg}}(F_\infty, A) = 0$*, then each group* $\mathrm{Sel}(F_\infty, A_\chi)$ *is* $\Lambda_{\mathcal{O}'}$*-cotorsion with* $\mu^{\mathrm{alg}}(F_\infty, A_\chi) = 0$*. Moreover, if* G *is abelian, then*

$$\lambda^{\mathrm{alg}}(F'_\infty, A) = \sum_{\chi \in G^\vee} \lambda^{\mathrm{alg}}(F_\infty, A_\chi).$$

2.4. Algebraic transition formula.

We continue with the notation of the previous section. We write $R(F'_\infty/F_\infty)$ for the set of prime-to-p places of F'_∞ which are ramified in F'_∞/F_∞. For a place $w' \in R(F'_\infty/F_\infty)$, we write w for its restriction to F_∞.

Theorem 2.8. *Let* F'/F *be a finite Galois* p*-extension with Galois group* G *which is unramified at all places dividing* p*. Let* T *be a nearly ordinary Galois representation over* F *with coefficients in* $\mathcal{O}$ *satisfying (1)–(3). Set* $A = T \otimes K/\mathcal{O}$ *and assume that:*

(4) $H^0(F, A[\pi]) = H^0\big(F, \mathrm{Hom}(A[\pi], \mu_p)\big) = 0$*;*

(5) $H^0(I_v, A/A_v^{cr})$ *is* $\mathcal{O}$*-divisible for all* v *dividing* p*.*

If $\mathrm{Sel}(F_\infty, A)$ *is* Λ*-cotorsion with* $\mu^{\mathrm{alg}}(F_\infty, A) = 0$*, then* $\mathrm{Sel}(F'_\infty, A)$ *is* Λ*-cotorsion with* $\mu^{\mathrm{alg}}(F'_\infty, A) = 0$*. Moreover, in this case,*

$$\lambda^{\mathrm{alg}}(F'_\infty, A) = [F'_\infty : F_\infty] \cdot \lambda^{\mathrm{alg}}(F_\infty, A) + \sum_{w' \in R(F'_\infty/F_\infty)} m(F'_{\infty,w'}/F_{\infty,w}, V)$$

with $V = T \otimes K$ *and* $m(F'_{\infty,w'}/F_{\infty,w}, V)$ *as in Section 2.1.*

Note that $m(F'_{\infty,w'}/F_{\infty,w}, V)$ in fact depends only on w and not on w'. The hypotheses (4) and (5) are needed to apply the results of [11]; they will not otherwise appear in the proof below. We note that the assumption that F'/F is unramified at p is primarily needed to assure that the condition (5) holds for twists of A as well.

Since p-groups are solvable and the only simple p-group is cyclic, the next lemma shows that it suffices to consider the case of $\mathbf{Z}/p\mathbf{Z}$-extensions.

Lemma 2.9. *Let* F''/F *be a Galois* p*-extension of number fields and let* F' *be an intermediate extension which is Galois over* F*. Let* T *be as above. If*

Theorem 2.8 holds for T with respect to any two of the three field extensions F''/F', F'/F and F''/F, then it holds for T with respect to the third extension.

Proof. This is clear from Corollary 2.5 except for the λ-invariant formula. Substituting the formula for $\lambda(F'_\infty, A)$ in terms of $\lambda(F_\infty, A)$ into the formula for $\lambda(F''_\infty, A)$ in terms of $\lambda(F'_\infty, A)$, one finds that it suffices to show that

$$\begin{aligned}\sum_{w''\in R(F''_\infty/F_\infty)} m(F''_{\infty,w''}/F_{\infty,w}, V) = \\ [F''_\infty : F'_\infty]\cdot \sum_{w'\in R(F'_\infty/F_\infty)} m(F'_{\infty,w'}/F_{\infty,w}, V) \\ + \sum_{w''\in R(F''_\infty/F'_\infty)} m(F''_{\infty,w''}/F'_{\infty,w'}, V).\end{aligned}$$

This formula follows upon summing the formula of Lemma 2.1 over all $w'' \in R(F''_\infty/F_\infty)$ and using the two facts:

- $[F''_\infty : F'_\infty]/[F''_{\infty,w''} : F'_{\infty,w'}]$ equals the number of places of F''_∞ lying over w' (since the residue field of $F_{\infty,w}$ has no p-extensions);
- $m(F''_{\infty,w''}/F'_{\infty,w'}, V) = 0$ for any $w'' \in R(F''_\infty/F_\infty) - R(F''_\infty/F'_\infty)$.

□

Proof of Theorem 2.8. By Lemma 2.9 and the preceding remark, we may assume that F'_∞/F_∞ is a cyclic extension of degree p. The fact that $\mathrm{Sel}(F'_\infty, A)$ is cotorsion with trivial μ-invariant is simply Corollary 2.5. Furthermore, by Corollary 2.7, we have

$$\lambda^{\mathrm{alg}}(F'_\infty, A) = \sum_{\chi\in G^\vee} \lambda^{\mathrm{alg}}(F_\infty, A_\chi).$$

For $\chi \in G^\vee$, note that χ is trivial modulo a uniformizer π' of $\mathcal{O}'$ as it takes values in μ_p. In particular, the residual representations $A_\chi[\pi']$ and $A[\pi]$ are isomorphic. Under the hypotheses (1)–(5), the result [11, Theorem 1] gives a precise formula for the relation between λ-invariants of congruent Galois representations. In the present case it takes the form:

$$\lambda^{\mathrm{alg}}(F_\infty, A_\chi) = \lambda^{\mathrm{alg}}(F_\infty, A) + \sum_{w'\nmid p}\big(m_{F_{\infty,w}}(V\otimes\omega^{-1}) - m_{F_{\infty,w}}(V_\chi\otimes\omega^{-1})\big)$$

where the sum is over all prime-to-p places w' of F'_∞, w denotes the place of F_∞ lying under w' and ω is the mod p cyclotomic character. The only non-zero terms in this sum are those for which w' is ramified in F'_∞/F_∞. For any such w', we have $\mu_p \subseteq F_{\infty,w}$ by local class field theory so that ω is in fact trivial at w; thus

$$\lambda^{\mathrm{alg}}(F_\infty, A_\chi) = \lambda^{\mathrm{alg}}(F_\infty, A) + \sum_{w'\in R(F'_\infty/F_\infty)}\big(m_{F_{\infty,w}}(V) - m_{F_{\infty,w}}(V_\chi)\big).$$

Summing over all $\chi \in G^\vee$ then yields

$$\lambda^{\mathrm{alg}}(F'_\infty, A) = [F'_\infty : F_\infty] \cdot \lambda^{\mathrm{alg}}(F_\infty, A) + \sum_{w' \in R(F'_\infty/F_\infty)} m(F'_{\infty,w'}/F_{\infty,w}, V)$$

which completes the proof. □

3. Analytic invariants

3.1. Definitions. Let $f = \sum a_n q^n$ be a modular eigenform of weight $k \geq 2$, level N and character ε. Let K denote the finite extension of $\mathbf{Q}_p$ generated by the Fourier coefficients of f (under some fixed embedding $\bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$), let $\mathcal{O}$ denote the ring of integers of K and let k denote the residue field of $\mathcal{O}$. Let V_f denote a two-dimensional K-vector space with Galois action associated to f in the usual way; thus the characteristic polynomial of a Frobenius element at a prime $\ell \nmid Np$ is

$$x^2 - a_\ell x + \ell^{k-1}\varepsilon(\ell).$$

Fix a Galois stable $\mathcal{O}$-lattice T_f in V_f. We assume that $T_f \otimes k$ is an irreducible Galois representation; in this case T_f is uniquely determined up to scaling. Set $A_f = T_f \otimes K/\mathcal{O}$.

Assuming that f is p-ordinary (in the sense that a_p is relatively prime to p) and fixing a canonical period for f, one can associate to f a p-adic L-function $L_p(\mathbf{Q}_\infty/\mathbf{Q}, f)$ which lies in $\Lambda_{\mathcal{O}}$. This is well-defined up to a p-adic unit (depending upon the choice of a canonical period) and thus has well-defined Iwasawa invariants.

Let $F/\mathbf{Q}$ be a finite abelian extension and let F_∞ denote the cyclotomic $\mathbf{Z}_p$-extension of F. For a character χ of $\mathrm{Gal}(F/\mathbf{Q})$, we denote by f_χ the modular eigenform $\sum a_n \chi(n) q^n$ obtained from f by twisting by χ (viewed as a Dirichlet character). If f is p-ordinary and $F/\mathbf{Q}$ is unramified at p, then f_χ is again p-ordinary and we define

$$L_p(F_\infty/F, f) = \prod_{\chi \in \mathrm{Gal}(F/\mathbf{Q})^\vee} L_p(\mathbf{Q}_\infty/\mathbf{Q}, f_\chi).$$

If $F/\mathbf{Q}$ is ramified at p, it is still possible to define $L_p(F_\infty/F, f)$; see [7, pg. 5], for example.

If F_1 and F_2 are two distinct number fields whose cyclotomic $\mathbf{Z}_p$-extensions agree, the corresponding p-adic L-functions of f over F_1 and F_2 need not agree. However, it is easy to check that the λ-invariants of these two power series are equal while their μ-invariants differ by a factor of a power of p. As we are only interested in the case of vanishing μ-invariants, we will abuse notation somewhat and simply denote the Iwasawa invariants of $L_p(F_\infty/F, f)$ by $\mu^{\mathrm{an}}(F_\infty, f)$ and $\lambda^{\mathrm{an}}(F_\infty, f)$.

3.2. Analytic transition formula. Let $F/\mathbf{Q}$ be a finite abelian extension of $\mathbf{Q}$ and let F' be a finite p-extension of F such that $F'/\mathbf{Q}$ is abelian. As always, let F_∞ and F'_∞ denote the cyclotomic $\mathbf{Z}_p$-extensions of F and F'. As before, we write $R(F'_\infty/F_\infty)$ for the set of prime-to-p places of F'_∞ which are ramified in F'_∞/F_∞.

Theorem 3.1. *Let f be a p-ordinary modular form such that $T_f \otimes k$ is irreducible and p-distinguished. If $\mu^{\mathrm{an}}(F_\infty, f) = 0$, then $\mu^{\mathrm{an}}(F'_\infty, f) = 0$. Moreover, if this is the case, then*

$$\lambda^{\mathrm{an}}(F'_\infty, f) = [F'_\infty : F_\infty] \cdot \lambda^{\mathrm{an}}(F_\infty, f) + \sum_{w' \in R(F'_\infty/F_\infty)} m(F'_{\infty,w'}/F_{\infty,w}, V_f).$$

Proof. By Lemma 2.9, we may assume $[F : \mathbf{Q}]$ is prime-to-p. Indeed, let F_0 be the maximal subfield of F of prime-to-p degree over $\mathbf{Q}$. By Lemma 2.9, knowledge of the theorem for the two extensions F'/F_0 and F/F_0 would then imply it for F'/F as well. Furthermore, replacing F (resp. F') by the maximal tamely ramified subextension of F_∞ (resp. F'_∞), we may assume that every character of $\mathrm{Gal}(F/\mathbf{Q})$ and $\mathrm{Gal}(F'/\mathbf{Q})$ is the product of a power of the mod p cyclotomic character and a character unramified at p.

After making these reductions, we let M denote the (unique) p-extension of $\mathbf{Q}$ inside of F' such that $MF = F'$. Set $G = \mathrm{Gal}(F/\mathbf{Q})$ and $H = \mathrm{Gal}(M/\mathbf{Q})$, so that $\mathrm{Gal}(F'/\mathbf{Q}) \cong G \times H$. We have

$$\mu^{\mathrm{an}}(F_\infty, f) = \sum_{\psi \in \mathrm{Gal}(F/\mathbf{Q})^\vee} \mu^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi) \tag{5}$$

and

$$\mu^{\mathrm{an}}(F'_\infty, f) = \sum_{\psi \in \mathrm{Gal}(F'/\mathbf{Q})^\vee} \mu^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi) = \sum_{\psi \in G^\vee} \sum_{\chi \in H^\vee} \mu^{\mathrm{an}}(\mathbf{Q}_\infty, f_{\psi\chi}). \tag{6}$$

Since we are assuming that $\mu^{\mathrm{an}}(F_\infty, f) = 0$ and since these μ-invariants are non-negative, from (5) it follows that $\mu^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi) = 0$ for each $\psi \in \mathrm{Gal}(F/\mathbf{Q})^\vee$. Fix $\psi \in G^\vee$. For any $\chi \in H^\vee$, $\psi\chi$ is congruent to ψ modulo any prime over p and thus f_χ and $f_{\psi\chi}$ are congruent modulo any prime over p. Then, since $\mu^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi) = 0$, by [1, Theorem 3.7.5] it follows that $\mu^{\mathrm{an}}(\mathbf{Q}_\infty, f_{\psi\chi}) = 0$ for each $\chi \in H^\vee$. (Note that the results of [1] apply to twists of p-ordinary forms by powers of the mod p cyclotomic character; this is why the reduction to the tamely ramified case is necessary for this argument.) Therefore, by (6) we have that $\mu^{\mathrm{an}}(F'_\infty, f) = 0$ proving the first part of the theorem.

For λ-invariants, we again have

$$\lambda^{\mathrm{an}}(F_\infty, f) = \sum_{\psi \in \mathrm{Gal}(F/\mathbf{Q})^\vee} \lambda^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi).$$

and

$$\lambda^{\mathrm{an}}(F'_\infty, f) = \sum_{\psi \in G^\vee} \sum_{\chi \in H^\vee} \lambda^{\mathrm{an}}(\mathbf{Q}_\infty, f_{\psi\chi}). \tag{7}$$

By [1, Theorem 3.7.7] the congruence between f_χ and $f_{\psi\chi}$ implies that

$$\lambda^{\mathrm{an}}(\mathbf{Q}_\infty, f_{\psi\chi}) - \lambda^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi) = \sum_v \big(m_{\mathbf{Q}_{\infty,v}}(V_{f_{\psi\chi}} \otimes \omega^{-1}) - m_{\mathbf{Q}_{\infty,v}}(V_{f_\psi} \otimes \omega^{-1})\big)$$

where the sum is over all places v of $\mathbf{Q}_\infty$ at which χ is ramified. (Note that in [1] the sum extends over all prime-to-p places; however, the terms are trivial unless χ is ramified at v. Also note that the mod p cyclotomic characters that appear are actually trivial since if $\mathbf{Q}_{\infty,v}$ has a ramified Galois p-extensions for $v \nmid p$, then $\mu_p \subseteq \mathbf{Q}_{\infty,v}$.)

Combining this with (7) and the definition of $m(M_{\infty,v'}/\mathbf{Q}_{\infty,v}, V_{f_\psi})$, we conclude that

$$\begin{aligned}\lambda^{\mathrm{an}}(F'_\infty, f) &= \sum_{\psi\in G^\vee} \Big([F'_\infty : F_\infty]\cdot\lambda^{\mathrm{an}}(\mathbf{Q}_\infty, f_\psi) + \\ &\qquad \sum_{v'\in R(M_\infty/\mathbf{Q}_\infty)} m(M_{\infty,v'}/\mathbf{Q}_{\infty,v}, V_{f_\psi})\Big) \\ &= [F'_\infty : F_\infty]\cdot\lambda^{\mathrm{an}}(F_\infty, f) + \\ &\qquad \sum_{v'\in R(M_\infty/\mathbf{Q}_\infty)} \sum_{\psi\in G^\vee} m(M_{\infty,v'}/\mathbf{Q}_{\infty,v}, V_{f_\psi}) \\ &= [F'_\infty : F_\infty]\cdot\lambda^{\mathrm{an}}(F_\infty, f) + \sum_{v'\in R(M_\infty/\mathbf{Q}_\infty)} g_{v'}(F'_\infty/M_\infty)\cdot \\ &\qquad m(M_{\infty,v'}/\mathbf{Q}_{\infty,v}, \mathbf{Z}[\mathrm{Gal}(F_{\infty,w}/\mathbf{Q}_{\infty,v})]\otimes V_f)\end{aligned}$$

where $g_{v'}(F'_\infty/M_\infty)$ denotes the number of places of F'_∞ above the place v' of M_∞. By Frobenius reciprocity,

$$m(M_{\infty,v'}/\mathbf{Q}_{\infty,v}, \mathbf{Z}[\mathrm{Gal}(F_{\infty,w}/\mathbf{Q}_{\infty,v})]\otimes V_f) = m(F'_{\infty,w'}/F_{\infty,w}, V_f)$$

where w' is the unique place of F'_∞ above v' and w. It follows that

$$\lambda(F'_\infty, f) = [F'_\infty : F_\infty]\cdot\lambda^{\mathrm{an}}(F_\infty, f) + \sum_{w'\in R(F'_\infty/F_\infty)} m(F'_{\infty,w'}/F_{\infty,w}, V_f)$$

as desired. □

4. Additional Results

4.1. Hilbert modular forms. We illustrate our results in the case of the two-dimensional representation V_f associated to a Hilbert modular eigenform f over a totally real field F. Although in principle our analytic results should remain true in this context, we focus on the less conjectural algebraic picture. Fix a G_F-stable lattice $T_f \subseteq V_f$ and let $A_f = T_f \otimes K/\mathcal{O}$.

Let F' be a finite Galois p-extension of F unramified at all places dividing p; for simplicity we assume also that F' is linearly disjoint from F_∞. Let v be a place of F not dividing p and fix a place v' of F' lying over v. For a character φ of G_v, we define

$$h(\varphi) = \begin{cases} -1 & \varphi \text{ ramified, } \varphi|_{G_{v'}} \text{ unramified, and } \varphi \equiv 1 \bmod \pi; \\ 0 & \varphi \not\equiv 1 \bmod \pi \text{ or } \varphi|_{G_{v'}} \text{ ramified;} \\ e_v(F'/F) - 1 & \varphi \text{ unramified and } \varphi \equiv 1 \bmod \pi \end{cases}$$

where $e_v(F'/F)$ denotes the ramification index of v in F'/F and $G_{v'}$ is the decomposition group at v'. Set

$$h_v(f) = \begin{cases} h(\varphi_1) + h(\varphi_2) & f \text{ principal series with characters } \varphi_1, \varphi_2 \text{ at } v; \\ h(\varphi) & f \text{ special with character } \varphi \text{ at } v; \\ 0 & f \text{ supercuspidal or extraordinary at } v. \end{cases}$$

For example, if f is unramified principal series at v with Frobenius characteristic polynomial

$$x^2 - a_v x + c_v,$$

then

$$h_v(f) = \begin{cases} 2(e_v(F'/F) - 1) & a_v \equiv 2, c_v \equiv 1 \bmod \pi \\ e_v(F'/F) - 1 & a_v \equiv c_v + 1 \not\equiv 2 \bmod \pi \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.1. *Assume that f is ordinary (in the sense that for each place v dividing p the Galois representation V_f has a unique one-dimensional quotient unramified at v) and that*

$$H^0(F, A_f[\pi]) = H^0\big(F, \operatorname{Hom}(A_f[\pi], \mu_p)\big) = 0.$$

If $\operatorname{Sel}(F_\infty, A_f)$ is Λ-cotorsion with $\mu^{\mathrm{alg}}(F_\infty, A_f) = 0$, then also $\operatorname{Sel}(F'_\infty, A_f)$ is Λ-cotorsion with $\mu^{\mathrm{alg}}(F'_\infty, A_f) = 0$ and

$$\lambda^{\mathrm{alg}}(F'_\infty, A) = [F'_\infty : F_\infty] \cdot \lambda^{\mathrm{alg}}(F_\infty, A) + \sum_v g_v(F'_\infty/F) \cdot h_v(f);$$

here the sum is over the prime-to-p places of F ramified in F'_∞ and $g_v(F'_\infty/F)$ denotes the number of places of F'_∞ lying over such a v.

Proof. Fix a place v of F not dividing p and let w denote a place of F_∞ lying over v. Since there are exactly $g_v(F_\infty/F)$ such places, by Theorem 2.8 it suffices to prove that

$$(8) \quad h_v(f) = m(F'_{\infty,w'}/F_{\infty,w}, V_f) := \sum_{\chi \in \operatorname{Gal}(F'_{\infty,w'}/F_{\infty,w})^\vee} \big(m_{F_{\infty,w}}(V_f) - m_{F_{\infty,w}}(V_{f,\chi})\big).$$

This is a straightforward case analysis. We will discuss the case that V_f is special associated to a character φ at v; the other cases are similar. In the special case, we have

$$V_{f,\chi}|_{I_{F_{\infty,w}}} = \begin{cases} K'(\chi\varphi) & \chi\varphi|_{G_{F_{\infty,w}}} \text{ unramified;} \\ 0 & \chi\varphi|_{G_{F_{\infty,w}}} \text{ ramified.} \end{cases}$$

Since an unramified character has trivial restriction to $G_{F_{\infty,w}}$ if and only if it has trivial reduction modulo π, it follows that

$$m_{F_{\infty,w}}(V_{f,\chi}) = \begin{cases} 1 & \varphi \equiv 1 \bmod \pi \text{ and } \chi\varphi|_{G_{F_{\infty,w}}} \text{ unramified;} \\ 0 & \text{otherwise.} \end{cases}$$

In particular, the sum in (8) is zero if $\varphi \not\equiv 1 \bmod \pi$ or if φ is ramified when restricted to $G_{F'_{\infty,w'}}$ (as then $\chi\varphi$ is ramified for all $\chi \in G_v^\vee$). If $\varphi \equiv 1 \bmod \pi$ and φ itself is unramified, then $m_{F_{\infty,w}}(V_f) = 1$ while $m_{F_{\infty,w}}(V_{f,\chi}) = 0$ for $\chi \neq 1$, so that the sum in (8) is $[F'_{\infty,w'} : F_{\infty,w}] - 1 = e_v(F'/F) - 1$, as desired. Finally, if $\varphi \equiv 1 \bmod \pi$ and φ is ramified but becomes unramified when restricted to $G_{v'}$, then $m_{F_{\infty,w}}(V_f) = 0$, while $m_{F_{\infty,w}}(V_{f,\chi}) = 1$ for a unique χ, so that the sum is -1. □

Suppose finally that f is in fact the Hilbert modular form associated to an elliptic curve E over F. The only principal series which occur are unramified and we have $c_v \equiv 1 \pmod{\pi}$ (since the determinant of V_f is cyclotomic and F_∞ has a p-extension (namely, F'_∞) ramified at v), so that

$$h_v(f) \neq 0 \quad \Leftrightarrow \quad a_v \equiv 2 \quad \Leftrightarrow \quad E(F_v) \text{ has a point of order } p$$

in which case $h_v(f) = 2(e_v(F'/F) - 1)$. The only characters which may occur in a special constituent are trivial or unramified quadratic, and we have $h_v(f) = e_v(F'/F) - 1$ or 0 respectively. Thus Theorem 4.1 recovers [3, Theorem 3.1] in this case.

4.2. The main conjecture. Let f be a p-ordinary elliptic modular eigenform of weight at least two and arbitrary level with associated Galois representation V_f. Let F be a finite abelian extension of $\mathbf{Q}$ with cyclotomic $\mathbf{Z}_p$-extension F_∞. Recall that the p-adic Iwasawa main conjecture for f over F asserts that the Selmer group $\mathrm{Sel}(F_\infty, A_f)$ is Λ-cotorsion and that the characteristic ideal of its dual is generated by the p-adic L-function $L_p(F_\infty, f)$. In fact, when the residual representation of V_f is absolutely irreducible, it is known by work of Kato that $\mathrm{Sel}(F_\infty, A_f)$ is indeed Λ-cotorsion and that $L_p(F_\infty, f)$ is an element of the characteristic ideal of $\mathrm{Sel}(F_\infty, A_f)$. In particular, this reduces the verification of the main conjecture for f over F to the equality of the algebraic and analytic Iwasawa invariants of f over F. The identical transition formulae in Theorems 2.8 and 3.1 thus yield the following immediate application to the main conjecture.

Theorem 4.2. *Let F'/F be a finite p-extension with F' abelian over $\mathbf{Q}$. If the residual representation of V_f is absolutely irreducible and p-distinguished, then the main conjecture holds for f over F with $\mu(F_\infty, f) = 0$ if and only if it holds for f over F' with $\mu(F'_\infty, f) = 0$.*

For an example of Theorem 4.2, consider the eigenform

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$$

of weight 12 and level 1. We take $p = 11$. It is well known that Δ is congruent modulo 11 to the newform associated to the elliptic curve $X_0(11)$. The 11-adic main conjecture is known for $X_0(11)$ over $\mathbf{Q}$; it has trivial μ-invariant and λ-invariant equal to 1 (see, for instance, [1, Example 5.3.1]. We should be clear here that the non-triviality of λ in this case corresponds to a trivial zero of the p-adic L-function; we are using the Greenberg Selmer group which does account for the trivial zero.) It follows from [1] that the 11-adic main conjecture also holds for Δ over $\mathbf{Q}$, again with trivial μ-invariant and λ-invariant equal to 1. Theorem 4.2 thus allows us to conclude that the main conjecture holds for Δ over any abelian 11-extension of $\mathbf{Q}$.

For a specific example, consider $F = \mathbf{Q}(\zeta_{23})^+$; it is a cyclic 11-extension of $\mathbf{Q}$. We can easily use Theorem 4.1 to compute its λ-invariant: using that $\tau(23) = 18643272$ one finds that $h_{23}(\Delta) = 0$, so that $\lambda(\mathbf{Q}(\zeta_{23})^+, \Delta) = 11$.

For a more interesting example, take F to be the unique subfield of $\mathbf{Q}(\zeta_{1123})$ which is cyclic of order 11 over $\mathbf{Q}$. In this case we have

$$\tau(1123) \equiv 2 \pmod{11}$$

so that we have $h_{1123}(\Delta) = 20$. Thus, in this case, Theorem 4.1 shows that $\lambda(F, \Delta) = 31$.

4.3. The supersingular case. As mentioned in the introduction, the underlying principle of this paper is that the existence of a formula relating the λ-invariants of congruent Galois representations should imply a Kida-type formula for these invariants. We illustrate this now in the case of modular forms of weight two that are supersingular at p.

Let f be an eigenform of weight 2 and level N with Fourier coefficients in K some finite extension of $\mathbf{Q}_p$. Assume further than $p \nmid N$ and that $a_p(f)$ is not a p-adic unit. In [8], Perrin-Riou associates to f a pair of algebraic and analytic μ-invariants over $\mathbf{Q}_\infty$ which we denote by $\mu^\star_\pm(\mathbf{Q}_\infty, f)$. (Here $\star$ denotes either "alg" or "an" for algebraic and analytic respectively.) Moreover, when $\mu^\star_+(\mathbf{Q}_\infty, f) = \mu^\star_-(\mathbf{Q}_\infty, f)$ or when $a_p(f) = 0$, she also defines corresponding λ-invariants $\lambda^\star_\pm(\mathbf{Q}_\infty, f)$. When $a_p(f) = 0$ these invariants coincide with the Iwasawa invariants of [6] and [9]. We also note that in [8] only the case of elliptic curves is treated, but the methods used there generalize to weight two modular forms.

We extend the definition of these invariants to the cyclotomic $\mathbf{Z}_p$-extension of an unramified abelian extension F of $\mathbf{Q}$. We define

$$\mu^\star_\pm(F_\infty, f) = \sum_{\psi \in \mathrm{Gal}(F/\mathbf{Q})^\vee} \mu^\star_\pm(\mathbf{Q}_\infty, f_\psi) \quad \text{and} \quad \lambda^\star_\pm(F_\infty, f) = \sum_{\psi \in \mathrm{Gal}(F/\mathbf{Q})^\vee} \lambda^\star_\pm(\mathbf{Q}_\infty, f_\psi)$$

for $\star \in \{\mathrm{alg}, \mathrm{an}\}$.

The following transition formula follows from the congruence results of [2].

Theorem 4.3. *Let f be as above and consider a p-extension of number fields F'/F with $F'/\mathbf{Q}$ unramified at p. If $\mu_{\pm}^{\star}(F_\infty, f) = 0$, then $\mu_{\pm}^{\star}(F'_\infty, f) = 0$. Moreover, if this is the case, then*

$$\lambda_{\pm}^{\star}(F'_\infty, f) = [F'_\infty : F_\infty] \cdot \lambda_{\pm}^{\star}(F_\infty, f) + \sum_{w' \in R(F'_\infty/F_\infty)} m(F'_{\infty,w'}/F_{\infty,w}, V_f).$$

In particular, if the main conjecture is true for f over F (with $\mu_{\pm}^{\star}(F_\infty, f) = 0$), then the main conjecture is true for f over F' (with $\mu_{\pm}^{\star}(F'_\infty, f) = 0$).

Proof. The proof of this theorem proceeds along the lines of the proof of Theorem 3.1 replacing the appeals to the results of [1, 11] to the results of [2]. The main result of [2] is a formula relating the $\lambda_{\pm}^{\star}$-invariants of congruent supersingular weight two modular forms. This formula has the same shape as the formulas that appear in [1] and [11] which allows for the proof to proceed nearly verbatim. □

References

[1] M. Emerton, R. Pollack and T. Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. 163, (2006) no. 3, 523–580.

[2] R. Greenberg, A. Iovita and R. Pollack, *Iwasawa invariants of supersingular modular forms*, preprint.

[3] Y. Hachimori and K. Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom. 8 (1999), no. 3, 581–601.

[4] K. Iwasawa, *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. 33 (1981), 263–288.

[5] Y. Kida, *ℓ-extensions of CM-fields and cyclotomic invariants*, J. Number Theory 12 (1980), 519–528.

[6] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. 152 (2003), 1–36.

[7] K. Matsuno, *An analogue of Kida's formula for the p-adic L-functions of modular elliptic curves*, J. Number Theory 84 (2000), 80–92.

[8] B. Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. 12 (2003), no. 2, 155–186.

[9] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. 118 (2003), no. 3, 523–558.

[10] W. Sinnott, *On p-adic L-functions and the Riemann–Hurwitz genus formula*, Comp. Math. 53 (1984), 3–17.

[11] T. Weston, *Iwasawa invariants of Galois deformations*, Manuscripta Math. 118 (2005) no. 2, 161–180.

[12] K. Wingberg, *A Riemann–Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication*, Comment. Math. Helv. 63 (1988), 587–592.

Robert Pollack
Department of Mathematics
Boston University,
Boston, MA
USA
rpollack@math.bu.edu

Tom Weston
Dept. of Mathematics,
University of Massachusetts,
Amherst, MA
USA
weston@math.umass.edu

Banach-Hecke Algebras and p-Adic Galois Representations

P. Schneider, J. Teitelbaum

Received: October 31, 2005
Revised: December 28, 2005

Wir lassen vom Geheimnis uns erheben
Der magischen Formelschrift, in deren Bann
Das Uferlose, Stürmende, das Leben
Zu klaren Gleichnissen gerann.
Hermann Hesse

Dedicated to John Coates

Abstract. In this paper, we take some initial steps towards illuminating the (hypothetical) p-adic local Langlands functoriality principle relating Galois representations of a p-adic field L and admissible unitary Banach space representations of $G(L)$ when G is a split reductive group over L.

2000 Mathematics Subject Classification: 11F80, 11S37, 22E50
Keywords and Phrases: Satake isomorphism, Iwahori-Hecke algebra, Banach-Hecke algebra, filtered isocrystal, crystalline Galois representation, p-adic local Langlands correspondence

In this paper, we take some initial steps towards illuminating the (hypothetical) p-adic local Langlands functoriality principle relating Galois representations of a p-adic field L and admissible unitary Banach space representations of $G(L)$ when G is a split reductive group over L. The outline of our work is derived from Breuil's remarkable insights into the nature of the correspondence between 2-dimensional crystalline Galois representations of the Galois group of $\mathbb{Q}_p$ and Banach space representations of $GL_2(\mathbb{Q}_p)$.

In the first part of the paper, we study the p-adic completion $\mathcal{B}(G,\rho)$ of the Hecke algebra $\mathcal{H}(G,\rho)$ of bi-equivariant compactly supported $\mathrm{End}(\rho)$-valued functions on a totally disconnected, locally compact group G derived from a finite dimensional continuous representation ρ of a compact open subgroup U of G. (These are the "Banach-Hecke algebras" of the title). After describing some general features of such algebras we study in particular the case where G is split reductive and $U = U_0$ is a special maximal compact or $U = U_1$ is an Iwahori subgroup of G and ρ is the restriction of a finite dimensional algebraic representation of G to U_0 or U_1.

In the smooth theory for trivial $\rho = 1_U$, by work of Bernstein, the maximal commutative subalgebra of the Iwahori-Hecke algebra is isomorphic to the group ring $K[\Lambda]$ where Λ is the cocharacter group of a maximal split torus T of G, and the spherical Hecke algebra is isomorphic by the Satake isomorphism to the ring $K[\Lambda]^W$ of Weyl group invariants. At the same time the algebra $K[\Lambda]$ may be viewed as the ring of algebraic functions on the dual maximal torus T' in the dual group G'. Together, these isomorphisms allow the identification of characters of the spherical Hecke algebra with semisimple conjugacy classes in G'. On the one hand, the Hecke character corresponds to a certain parabolically induced smooth representation; on the other, the conjugacy class in G' determines the Frobenius in an unramified Weil group representation of the field L. This is the unramified local Langlands correspondence (the Satake parametrization) in the classical case.

With these principles in mind, we show that the completed maximal commutative subalgebra of the Iwahori-Hecke algebra for ρ is isomorphic to the affinoid algebra of a certain explicitly given rational subdomain T'_ρ in the dual torus T'. The spectrum of this algebra therefore corresponds to certain points of T'. We also show that the quotient of this subdomain by the Weyl group action is isomorphic to the corresponding completion of the spherical Hecke algebra; this algebra, for most groups G, turns out to be a Tate algebra. These results may be viewed as giving a p-adic completion of the Satake isomorphism, though our situation is somewhat complicated by our reluctance to introduce a square root of q as is done routinely in the classical case. These computations take up the first four sections of the paper.

In the second part of the paper, we let $G = GL_{d+1}(L)$. We relate the subdomain of T' determined by the completion $\mathcal{B}(G,\rho)$ to isomorphism classes of a certain kind of crystalline Dieudonne module. This relationship follows Breuil's theory, which puts a 2-dimensional irreducible crystalline representation V of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ with coefficients in a field K into correspondence with a topologically irreducible admissible unitary representation of $GL_2(\mathbb{Q}_p)$ in a K-Banach space. Furthermore, this Banach space representation is a completion of a locally algebraic representation whose smooth factor comes from $D_{cris}(V)$ viewed as a Weil group representation and whose algebraic part is determined by the Hodge-Tate weights of V.

To state our relationship, let V be a $d+1$-dimensional crystalline representation of $\mathrm{Gal}(\overline{L}/L)$ in a K-vector space, where L and K are finite extensions of $\mathbb{Q}_p$. In this situation, $D_{cris}(V)$ has a K-vector space structure. Suppose further that:

i. L is embeddable into K, and fix once and for all such an embedding $L \subseteq K$;

ii. the eigenvalues of the Frobenius on $D_{cris}(V)$ lie in K;

iii. the (negatives of) the Hodge-Tate weights of $D_{cris}(V)$ are multiplicity free and are separated from one another by at least $[L : \mathbb{Q}_p]$;

iv. V is *special*, meaning that the kernel of the natural map

$$\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \to \mathbb{C}_p \otimes_L V$$

is generated by its $\mathrm{Gal}(\overline{L}/L)$ invariants.

It follows from the Colmez-Fontaine theory that the category of such special representations is equivalent to a category of "K-isocrystals", which are K-vector spaces with a K-linear Frobenius and a filtration that is admissible in a sense very close to the usual meaning.

Given such a representation, we extract from the associated K-isocrystal its Frobenius, which we view as an element of the dual group $G'(K)$ determined up to conjugacy. The semi-simple part ζ of this element determines a point of $T'(K)$ up to the Weyl group action. From the Hodge-Tate weights, we extract a dominant cocharacter of G' and hence a highest weight ξ determining an algebraic representation $\rho = \rho_\xi$ for G. (In fact, the highest weight is a modification of the Hodge-Tate weights, but we avoid this complication in this introduction). Put together, this data yields a completion of the Iwahori-Hecke algebra, determined by the highest weight, and a character of its maximal commutative subalgebra, determined up to the Weyl group action. In other words, we obtain a simple module K_ζ for the completed spherical Hecke algebra $\mathcal{B}(G, \rho_\xi | U_0)$.

Our main result is that the existence of an admissible filtration on $D_{cris}(V)$ translates into the condition that the point of T' determined by the Frobenius lives in the subdomain T'_ρ. Conversely, we show how to reverse this procedure and, from a point of $T'_\rho(K)$ (up to Weyl action), make an isocrystal that admits an admissible filtration of Hodge-Tate type determined by ρ. See Section 5 (esp. Proposition 5.2) for the details.

It is crucial to realize that the correspondence between points of T'_ρ and isocrystals outlined above does not determine a specific filtration on the isocrystal. Except when $d = 1$ there are infinitely many choices of filtration compatible with the given data. Consequently the "correspondence" we describe is a very coarse version of a p-adic local Langlands correspondence.

To better understand this coarseness on the "representation-theoretic" side, recall that to a Galois representation V of the type described above we associate a simple module K_ζ for the completion $\mathcal{B}(G, \rho|U_0)$ of the spherical Hecke algebra. There is an easily described sup-norm on the smooth compactly induced representation $\mathrm{ind}_{U_0}^G(\rho|U_0)$; let $B_{U_0}^G(\rho|U_0)$ be the completion of this representation. We show that the completed Hecke algebra acts continuously on this space. By analogy with the Borel-Matsumoto theory constructing parabolically induced representations from compactly induced ones, and following also Breuil's approach for $GL_2(\mathbb{Q}_p)$, it is natural to consider the completed tensor product

$$B_{\xi,\zeta} := K_\zeta \,\widehat{\otimes}_{\mathcal{B}(G,\rho_\xi|U_0)}\, B^G_{U_0}(\rho_\xi|U_0)\ .$$

A deep theorem of Breuil-Berger ([BB]) says that, in the $GL_2(\mathbb{Q}_p)$-case, this representation in most cases is nonzero, admissible, and irreducible, and under Breuil's correspondence it is the Banach representation associated to V. In our more general situation, we do not know even that $B_{\xi,\zeta}$ is nonzero. Accepting, for the moment, that it is nonzero, we do not expect it to be admissible or irreducible, because it is associated to the entire infinite family of representations having the same Frobenius and Hodge-Tate weights as V but different admissible filtrations. We propose that $B_{\xi,\zeta}$ maps, with dense image, to each of the Banach spaces coming from this family of Galois representations. We discuss this further in Section 5.

In the last section of this paper (Section 6) we consider the shape of a p-adic local Langlands functoriality for a general L-split reductive group G over L, with Langlands dual group G' also defined over L. Here we rely on ideas from the work of Kottwitz, Rapoport-Zink, and Fontaine-Rapoport. Recall that a cocharacter ν of the dual group G' defined over K allows one to put a filtration $Fil^{\cdot}_{\rho'\circ\nu} E$ on every K-rational representation space (ρ', E) of G'. Using (a modified version of) a notion of Rapoport-Zink, we say that a pair (ν, b) consisting of an element b of $G'(K)$ and a K-rational cocharacter ν of G' is an "admissible pair" if, for any K-rational representation (ρ', E) of G', the K-isocrystal $(E, \rho'(b), Fil^{\cdot}_{\rho'\circ\nu} E)$ is admissible. Such an admissible pair defines a faithful tensor functor from the neutral Tannakian category of K-rational representations of G' to that of admissible filtered K-isocrystals. Composing this with the Fontaine functor one obtains a tensor functor to the category of "special" $\mathrm{Gal}(\overline{L}/L)$ representations of the type described earlier. The Tannakian formalism therefore constructs from an admissible pair an isomorphism class of representations of the Galois group of L in $G'(\overline{K})$.

Now suppose given an irreducible algebraic representation ρ of G. Its highest weight may be viewed as a cocharacter of G'. Under a certain technical condition, we prove in this section that there is an admissible pair (ν, b) where ν is conjugate by $G'(K)$ to a (modification of) the highest weight, and b is an element of $G'(K)$, if and only if the semisimple part of b is conjugate to an element of the affinoid domain $T'_\rho(K)$ (See Proposition 6.1). Thus in some sense this domain is functorial in the group G'.

Our work in this section relies on a technical hypothesis on G. Suppose that η is half the sum of the positive roots of G. We need $[L:\mathbb{Q}_p]\eta$ to be an integral weight of G. This happens, for example, if L has even degree over $\mathbb{Q}_p$, and in general for many groups, but not, for example, when $G = PGL_2(\mathbb{Q}_p)$. This complication has its origin in the normalization of the Langlands correspondence. Because of the square root of q issue the p-adic case seems to force the use of the "Hecke" or the "Tate" correspondence rather than the traditional unitary correspondence; but even for smooth representations this is not functorial (cf. [Del] (3.2.4-6)). It turns out that without the above integrality hypothesis one even has to introduce a square root of a specific continuous Galois character (for $L = \mathbb{Q}_p$ it is the cyclotomic character). This leads to isocrystals with a filtration indexed by half-integers. Although it seems possible to relate these to Galois representations this has not been done yet in the literature. We hope to come back to this in the future.

The authors thank Matthew Emerton for pointing out that the conditions which define our affinoid domains T'_ρ are compatible with the structure of his Jacquet functor on locally algebraic representations ([Em1] Prop. 3.4.9 and Lemma 4.4.2, [Em2] Lemma 1.6). We thank Laurent Berger, Christophe Breuil, and especially Jean-Marc Fontaine for their very helpful conversations about these results. We also want to stress that our computations in Section 4 rely in an essential way on the results of Marie-France Vigneras in [Vig]. The first author gratefully acknowledges support from UIC and CMI. During the final stages of this paper he was employed by the Clay Mathematics Institute as a Research Scholar. The second author was supported by National Science Foundation Grant DMS-0245410.

We dedicate this paper to John Coates on the occasion of his sixtieth birthday. His constant support and unrelenting enthusiasm was and is an essential source of energy and inspiration for us over all these years.

Throughout this paper K is a fixed complete extension field of $\mathbb{Q}_p$ with absolute value $|\ |$.

Added in proof: In a forthcoming joint paper by C. Breuil and P. Schneider the technical restrictions of the present paper – that $L \subseteq K$, that the crystalline Galois representations V have to be special, and that $[L : \mathbb{Q}_p]\eta$ has to be an integral weight for the split group G – will be removed. In fact, this forces a renormalization of the picture in the present paper.

1. Banach-Hecke algebras

In this section G denotes a totally disconnected and locally compact group, and $U \subseteq G$ is a fixed compact open subgroup. We let (ρ, E) be a continuous representation of U on a finite dimensional K-vector space E, and we fix a U-invariant norm $\|\ \|$ on E.

The Hecke algebra $\mathcal{H}(G, \rho)$ is the K-vector space of all compactly supported functions $\psi : G \longrightarrow \mathrm{End}_K(E)$ satisfying

$$\psi(u_1 g u_2) = \rho(u_1) \circ \psi(g) \circ \rho(u_2) \qquad \text{for any } u_1, u_2 \in U \text{ and } g \in G\ .$$

It is a unital associative K-algebra via the convolution

$$\psi_1 * \psi_2(h) := \sum_{g \in G/U} \psi_1(g) \circ \psi_2(g^{-1}h)\ .$$

Its unit element is the function

$$\psi_e(h) := \begin{cases} \rho(h) & \text{if } h \in U, \\ 0 & \text{otherwise.} \end{cases}$$

We note that any function ψ in $\mathcal{H}(G,\rho)$ necessarily is continuous. We now introduce the norm

$$\|\psi\| := \sup_{g\in G} \|\psi(g)\|$$

on $\mathcal{H}(G,\rho)$ where on the right hand side $\|\ \|$ refers to the operator norm on $\mathrm{End}_K(E)$ with respect to the original norm $\|\ \|$ on E. This norm on $\mathcal{H}(G,\rho)$ evidently is submultiplicative. By completion we therefore obtain a unital K-Banach algebra $\mathcal{B}(G,\rho)$, called in the following the Banach-Hecke algebra, with submultiplicative norm. As a Banach space $\mathcal{B}(G,\rho)$ is the space of all continuous functions $\psi : G \longrightarrow \mathrm{End}_K(E)$ vanishing at infinity and satisfying

$$\psi(u_1 g u_2) = \rho(u_1) \circ \psi(g) \circ \rho(u_2) \qquad \text{for any } u_1, u_2 \in U \text{ and } g \in G\ .$$

In the special case where $\rho = 1_U$ is the trivial representation $\mathcal{H}(G, 1_U)$, resp. $\mathcal{B}(G, 1_U)$, is the vector space of all K-valued finitely supported functions, resp. functions vanishing at infinity, on the double coset space $U\backslash G/U$.

A more intrinsic interpretation of these algebras can be given by introducing the compactly induced G-representation $\mathrm{ind}_U^G(\rho)$. This is the K-vector space of all compactly supported functions $f : G \longrightarrow E$ satisfying

$$f(gu) = \rho(u^{-1})(f(g)) \qquad \text{for any } u \in U \text{ and } g \in G$$

with G acting by left translations. Again we note that any function f in $\mathrm{ind}_U^G(\rho)$ is continuous. We equip $\mathrm{ind}_U^G(\rho)$ with the G-invariant norm

$$\|f\| := \sup_{g\in G} \|f(g)\|$$

and let $B_U^G(\rho)$ denote the corresponding completion. The G-action extends isometrically to the K-Banach space $B_U^G(\rho)$, which consists of all continuous functions $f : G \longrightarrow E$ vanishing at infinity and satisfying

$$f(gu) = \rho(u^{-1})(f(g)) \qquad \text{for any } u \in U \text{ and } g \in G\ .$$

Lemma 1.1: *The G-action on $B_U^G(\rho)$ is continuous.*

Proof: Since G acts isometrically it remains to show that the orbit maps

$$\begin{array}{rcl} c_f : G & \longrightarrow & B_U^G(\rho) \\ g & \longmapsto & gf\ , \end{array}$$

for any $f \in B_U^G(\rho)$, are continuous. In case $f \in \mathrm{ind}_U^G(\rho)$ the map c_f even is locally constant. In general we write $f = \lim\limits_{i\to\infty}$ as the limit of a sequence $(f_i)_{i\in\mathbb{N}}$ in $\mathrm{ind}_U^G(\rho)$. Because of

$$\|(c_f - c_{f_i})(g)\| = \|g(f - f_i)\| = \|f - f_i\|$$

the map c_f is the uniform limit of the locally constant maps c_{f_i} and hence is continuous.

One easily checks that the pairing

$$(1) \qquad \begin{array}{rcl} \mathcal{H}(G,\rho) \times \mathrm{ind}_U^G(\rho) & \longrightarrow & \mathrm{ind}_U^G(\rho) \\ (\psi, f) & \longmapsto & (\psi * f)(g) := \sum_{h\in G/U} \psi(g^{-1}h)(f(h)) \end{array}$$

makes $\mathrm{ind}_U^G(\rho)$ into a unital left $\mathcal{H}(G,\rho)$-module and that this module structure commutes with the G-action.

Lemma 1.2: *The map*

$$\begin{array}{rcl} \mathcal{H}(G,\rho) & \xrightarrow{\cong} & \mathrm{End}_G(\mathrm{ind}_U^G(\rho)) \\ \psi & \longmapsto & A_\psi(f) := \psi * f \end{array}$$

is an isomorphism of K-algebras.

Proof: For a smooth representation ρ this can be found in [Kut]. Our more general case follows by the same argument. But since we will need the notations anyway we recall the proof. The map in question certainly is a homomorphism of K-algebras. We now introduce, for any $w \in E$, the function

$$f_w(g) := \begin{cases} \rho(g^{-1})(w) & \text{if } g \in U, \\ 0 & \text{otherwise} \end{cases}$$

in $\mathrm{ind}_U^G(\rho)$. We have

$$(2) \qquad A_\psi(f_w)(g) = (\psi * f_w)(g) = \psi(g^{-1})(w) \quad \text{for any } \psi \in \mathcal{H}(G,\rho) \ .$$

This shows that the map in question is injective. To see its surjectivity we fix an operator $A_0 \in \mathrm{End}_G(\mathrm{ind}_U^G(\rho))$ and consider the function

$$\begin{array}{rcl} \psi_0 : G & \longrightarrow & \mathrm{End}_K(E) \\ g & \longmapsto & [w \mapsto A_0(f_w)(g^{-1})] \ . \end{array}$$

It clearly has compact support. Furthermore, for $u_1, u_2 \in U$, we compute

$$\begin{aligned} \psi_0(u_1 g u_2)(w) &= A_0(f_w)(u_2^{-1} g^{-1} u_1^{-1}) = \rho(u_1)[A_0(f_w)(u_2^{-1} g^{-1})] \\ &= \rho(u_1)[(u_2(A_0(f_w)))(g^{-1})] = \rho(u_1)[A_0(u_2(f_w))(g^{-1})] \\ &= \rho(u_1)[A_0(f_{\rho(u_2)(w)})(g^{-1})] = \rho(u_1)[\psi_0(\rho(u_2)(w))] \\ &= [\rho(u_1) \circ \psi_0 \circ \rho(u_2)](w) \ . \end{aligned}$$

Hence $\psi_0 \in \mathcal{H}(G,\rho)$. Moreover, for any $f \in \operatorname{ind}_U^G(\rho)$ we have

$$f = \sum_{h \in G/U} h(f_{f(h)})$$

and therefore

$$\begin{aligned} A_{\psi_0}(f)(g) = (\psi_0 * f)(g) &= \sum_{h \in G/U} \psi_0(g^{-1}h)(f(h)) \\ &= \sum_{h \in G/U} A_0(f_{f(h)})(h^{-1}g) = A_0(\sum_{h \in G/U} h(f_{f(h)}))(g) \\ &= A_0(f)(g) \ . \end{aligned}$$

Hence $A_{\psi_0} = A_0$.

We evidently have $\|\psi * f\| \leq \|\psi\| \cdot \|f\|$. By continuity we therefore obtain a continuous left action of the Banach algebra $\mathcal{B}(G,\rho)$ on the Banach space $B_U^G(\rho)$ which is submultiplicative in the corresponding norms and which commutes with the G-action. This action is described by the same formula (1), and we therefore continue to denote it by $*$.

Lemma 1.3: *The map*

$$\begin{array}{ccc} \mathcal{B}(G,\rho) & \xrightarrow{\cong} & \operatorname{End}_G^{cont}(B_U^G(\rho)) \\ \psi & \longmapsto & A_\psi(f) := \psi * f \end{array}$$

is an isomorphism of K-algebras and is an isometry with respect to the operator norm on the right hand side.

Proof: (The superscript "cont" refers to the continuous endomorphisms.) By the previous discussion the map $\psi \longmapsto A_\psi$ is well defined, is a homomorphism of K-algebras, and is norm decreasing. Using the notations from the proof of Lemma 1.2 the formula (2), by continuity, holds for any $\psi \in \mathcal{B}(G,\rho)$. Using that $\|f_w\| = \|w\|$ we now compute

$$\begin{aligned} \|A_\psi\| &\geq \sup_{w \neq 0} \frac{\|\psi * f_w\|}{\|f_w\|} = \sup_{w \neq 0} \sup_g \frac{\|\psi(g^{-1})(w)\|}{\|w\|} = \sup_g \|\psi(g^{-1})\| \\ &= \|\psi\| \geq \|A_\psi\| \ . \end{aligned}$$

It follows that the map in the assertion is an isometry and in particular is injective. To see its surjectivity we fix an $A_0 \in \operatorname{End}_G^{cont}(B_U^G(\rho))$ and define

$$\begin{array}{rcl} \psi_0 : G & \longrightarrow & \operatorname{End}_K(E) \\ g & \longmapsto & [w \mapsto A_0(f_w)(g^{-1})] \ . \end{array}$$

Since each $A_0(f_w)$ is continuous and vanishing at infinity on G it follows that ψ_0 is continuous and vanishing at infinity. By exactly the same computations as in the proof of Lemma 1.2 one then shows that in fact $\psi_0 \in \mathcal{B}(G,\rho)$ and that $A_{\psi_0} = A_0$.

We end this section by considering the special case where (ρ, E) is the restriction to U of a continuous representation ρ of G on a finite dimensional K-vector space E. It is easy to check that then the map

$$\begin{array}{rcl} \iota_\rho : \mathcal{H}(G, 1_U) & \longrightarrow & \mathcal{H}(G,\rho) \\ \psi & \longmapsto & (\psi \cdot \rho)(g) := \psi(g)\rho(g) \end{array}$$

is an injective homomorphism of K-algebras. There are interesting situations where this map in fact is an isomorphism. We let L be a finite extension of $\mathbb{Q}_p$ contained in K, and we assume that G as well as (ρ, E) are locally L-analytic.

Lemma 1.4: *Suppose that, for the derived action of the Lie algebra $\mathfrak{g}$ of G, the $K \otimes_L \mathfrak{g}$-module E is absolutely irreducible; then the homomorphism ι_ρ is bijective.*

Proof: Using Lemma 1.2 and Frobenius reciprocity we have

$$\begin{aligned} \mathcal{H}(G,\rho) &= \mathrm{End}_G(\mathrm{ind}_U^G(\rho)) = \mathrm{Hom}_U(E, \mathrm{ind}_U^G(\rho)) \\ &= \mathrm{Hom}_U(E, \mathrm{ind}_U^G(1) \otimes_K E) \\ &= [\mathrm{ind}_U^G(1) \otimes_K E^* \otimes_K E]^U \end{aligned}$$

where the last term denotes the U-fixed vectors in the tensor product with respect to the diagonal action. This diagonal action makes the tensor product equipped with the finest locally convex topology into a locally analytic G-representation. Its U-fixed vectors certainly are contained in the vectors annihilated by the derived action of $\mathfrak{g}$. Since G acts smoothly on $\mathrm{ind}_U^G(1)$ we have

$$\begin{aligned} (\mathrm{ind}_U^G(1) \otimes_K E^* \otimes_K E)^{\mathfrak{g}=0} &= \mathrm{ind}_U^G(1) \otimes_K (E^* \otimes_K E)^{\mathfrak{g}=0} \\ &= \mathrm{ind}_U^G(1) \otimes_K \mathrm{End}_{K\otimes_L \mathfrak{g}}(E) \ . \end{aligned}$$

Our assumption on absolute irreducibility implies that $\mathrm{End}_{K\otimes_L\mathfrak{g}}(E) = K$. We therefore see that

$$\mathcal{H}(G,\rho) = [\mathrm{ind}_U^G(1) \otimes_K E^* \otimes_K E]^U = \mathrm{ind}_U^G(1)^U = \mathcal{H}(G, 1_U) \ .$$

2. Weights and affinoid algebras

For the rest of this paper $L/\mathbb{Q}_p$ is a finite extension contained in K, and G denotes the group of L-valued points of an L-split connected reductive group over L. Let $|\ |_L$ be the normalized absolute value of L, $\mathrm{val}_L : K^\times \longrightarrow \mathbb{R}$

the unique additive valuation such that $\mathrm{val}_L(L^\times) = \mathbb{Z}$, and q the number of elements in the residue class field of L. We fix a maximal L-split torus T in G and a Borel subgroup $P = TN$ of G with Levi component T and unipotent radical N. The Weyl group of G is the quotient $W = N(T)/T$ of the normalizer $N(T)$ of T in G by T. We also fix a maximal compact subgroup $U_0 \subseteq G$ which is special with respect to T (i.e., is the stabilizer of a special vertex x_0 in the apartment corresponding to T, cf. [Car]§3.5). We put $T_0 := U_0 \cap T$ and $N_0 := U_0 \cap N$. The quotient $\Lambda := T/T_0$ is a free abelian group of rank equal to the dimension of T and can naturally be identified with the cocharacter group of T. Let $\lambda : T \longrightarrow \Lambda$ denote the projection map. The conjugation action of $N(T)$ on T induces W-actions on T and Λ which we denote by $t \longmapsto {}^w t$ and $\lambda \longmapsto {}^w\lambda$, respectively. We also need the L-torus T' dual to T. Its K-valued points are given by

$$T'(K) := \mathrm{Hom}(\Lambda, K^\times) \ .$$

The group ring $K[\Lambda]$ of Λ over K naturally identifies with the ring of algebraic functions on the torus T'. We introduce the "valuation map"

$$val : \ T'(K) = \mathrm{Hom}(\Lambda, K^\times) \xrightarrow{\mathrm{val}_L \circ} \mathrm{Hom}(\Lambda, \mathbb{R}) =: V_{\mathbb{R}} \ .$$

If $X^*(T)$ denotes the algebraic character group of the torus T then, as $|\chi(T_0)| = \{1\}$, we have the embedding

$$\begin{array}{ccc} X^*(T) & \longrightarrow & \mathrm{Hom}(\Lambda, \mathbb{R}) \\ \chi & \longmapsto & \mathrm{val}_L \circ \chi \end{array}$$

which induces an isomorphism

$$X^*(T) \otimes \mathbb{R} \xrightarrow{\cong} V_{\mathbb{R}} \ .$$

We therefore may view $V_{\mathbb{R}}$ as the real vector space underlying the root datum of G with respect to T. Evidently any $\lambda \in \Lambda$ defines a linear form in the dual vector space $V_{\mathbb{R}}^*$ also denoted by λ. Let Φ denote the set of roots of T in G and let $\Phi^+ \subseteq \Phi$ be the subset of those roots which are positive with respect to P. As usual, $\check{\alpha} \in \Lambda$ denotes the coroot corresponding to the root $\alpha \in \Phi$. The subset $\Lambda^{--} \subseteq \Lambda$ of antidominant cocharacters is defined to be the image $\Lambda^{--} := \lambda(T^{--})$ of

$$T^{--} := \{t \in T : |\alpha(t)|_L \geq 1 \text{ for any } \alpha \in \Phi^+\} \ .$$

Hence

$$\Lambda^{--} = \{\lambda \in \Lambda : \mathrm{val}_L \circ \alpha(\lambda) \leq 0 \text{ for any } \alpha \in \Phi^+\} \ .$$

We finally recall that Λ^{--} carries the partial order $\leq$ given by

$$\mu \leq \lambda \quad \text{if} \quad \lambda - \mu \in \sum_{\alpha \in \Phi^+} \mathbb{R}_{\geq 0} \cdot (-\check{\alpha}) \subseteq \Lambda \otimes \mathbb{R} \ .$$

In this section we will investigate certain Banach algebra completions of the group ring $K[\Lambda]$ together with certain twisted W-actions on them. We will proceed in an axiomatic way and will give ourselves a cocycle on W with values in $T'(K)$, i.e., a map

$$\gamma : W \times \Lambda \longrightarrow K^\times$$

such that

$$(a) \qquad \gamma(w, \lambda\mu) = \gamma(w,\lambda)\gamma(w,\mu) \qquad \text{for any } w \in W \text{ and } \lambda, \mu \in \Lambda$$

and

$$(b) \qquad \gamma(vw, \lambda) = \gamma(v, {}^w\lambda)\gamma(w,\lambda) \qquad \text{for any } v, w \in W \text{ and } \lambda \in \Lambda\ .$$

Moreover we impose the positivity condition

$$(c) \qquad |\gamma(w,\lambda)| \leq 1 \qquad \text{for any } w \in W \text{ and } \lambda \in \Lambda^{--}$$

as well as the partial triviality condition

$$(d) \qquad \gamma(w,\lambda) = 1 \qquad \text{for any } w \in W \text{ and } \lambda \in \Lambda \text{ such that } {}^w\lambda = \lambda\ .$$

The twisted action of W on $K[\Lambda]$ then is defined by

$$\begin{array}{rcl} W \times K[\Lambda] & \longrightarrow & K[\Lambda] \\ (w, \sum_\lambda c_\lambda \lambda) & \longmapsto & w \cdot (\sum_\lambda c_\lambda \lambda) := \sum_\lambda \gamma(w,\lambda) c_\lambda {}^w\lambda\ . \end{array}$$

By (a), each $w \in W$ acts as an algebra automorphism, and the cocycle condition (b) guarantees the associativity of this W-action. The invariants with respect to this action will be denoted by $K[\Lambda]^{W,\gamma}$. Since Λ^{--} is a fundamental domain for the W-action on Λ it follows that $K[\Lambda]^{W,\gamma}$ has the K-basis $\{\sigma_\lambda\}_{\lambda \in \Lambda^{--}}$ defined by

$$\sigma_\lambda := \sum_{w \in W/W(\lambda)} w \cdot \lambda = \sum_{w \in W/W(\lambda)} \gamma(w,\lambda) {}^w\lambda$$

where $W(\lambda) \subseteq W$ denotes the stabilizer of λ and where the sums are well defined because of (d). Next, again using (d), we define the map

$$\begin{array}{rcl} \gamma^{dom} : \Lambda & \longrightarrow & K^\times \\ \lambda & \longmapsto & \gamma(w,\lambda) \quad \text{if } {}^w\lambda \in \Lambda^{--}\ , \end{array}$$

and we equip $K[\Lambda]$ with the norm

$$\| \sum_\lambda c_\lambda \lambda \|_\gamma := \sup_{\lambda \in \Lambda} |\gamma^{dom}(\lambda) c_\lambda|\ .$$

The cocycle condition (b) implies the identity

$$(1) \qquad \gamma^{dom}({}^w\lambda)\gamma(w,\lambda) = \gamma^{dom}(\lambda)$$

from which one deduces that the twisted W-action on $K[\Lambda]$ is isometric in the norm $\| \ \|_\gamma$ and hence extends by continuity to a W-action on the completion $K\langle\Lambda;\gamma\rangle$ of $K[\Lambda]$ with respect to $\| \ \|_\gamma$. Again we denote the corresponding W-invariants by $K\langle\Lambda;\gamma\rangle^{W,\gamma}$. One easily checks that $\{\sigma_\lambda\}_{\lambda\in\Lambda^{--}}$ is an orthonormal basis of the Banach space $(K\langle\Lambda;\gamma\rangle^{W,\gamma}, \| \ \|_\gamma)$.

Lemma 2.1: *i.* $|\gamma^{dom}(\lambda)| \geq 1$ *for any* $\lambda \in \Lambda$*;*

ii. $|\gamma^{dom}(\lambda\mu)| \leq |\gamma^{dom}(\lambda)||\gamma^{dom}(\mu)|$ *for any* $\lambda,\mu \in \Lambda$.

Proof: i. If ${}^w\lambda \in \Lambda^{--}$ then $\gamma^{dom}(\lambda) = \gamma(w,\lambda) = \gamma(w^{-1}, {}^w\lambda)^{-1}$. The claim therefore is a consequence of the positivity condition (c). ii. If ${}^w(\lambda\mu) \in \Lambda^{--}$ then, using (1), we have

$$\gamma^{dom}(\lambda\mu) = \gamma^{dom}({}^w\lambda)^{-1}\gamma^{dom}({}^w\mu)^{-1}\gamma^{dom}(\lambda)\gamma^{dom}(\mu) \ .$$

Hence the claim follows from the first assertion.

It is immediate from Lemma 2.1.i that the norm $\| \ \|_\gamma$ is submultiplicative. Hence $K\langle\Lambda;\gamma\rangle$ is a K-Banach algebra containing $K[\Lambda]$ as a dense subalgebra. Moreover, since the twisted W-action on $K\langle\Lambda;\gamma\rangle$ is by algebra automorphisms, $K\langle\Lambda;\gamma\rangle^{W,\gamma}$ is a Banach subalgebra of $K\langle\Lambda;\gamma\rangle$.

In order to compute the Banach algebra $K\langle\Lambda;\gamma\rangle$ we introduce the subset

$$T'_\gamma(K) := \{\zeta \in T'(K) : |\zeta(\lambda)| \leq |\gamma^{dom}(\lambda)| \text{ for any } \lambda \in \Lambda\}$$

of $T'(K)$. We obviously have

$$T'_\gamma(K) = val^{-1}(V^\gamma_{\mathbb{R}})$$

with

$$V^\gamma_{\mathbb{R}} := \{z \in V_{\mathbb{R}} : \lambda(z) \geq \mathrm{val}_L(\gamma^{dom}(\lambda)) \text{ for any } \lambda \in \Lambda\} \ .$$

By (a), our cocycle γ defines the finitely many points

$$z_w := -val(\gamma(w^{-1},.)) \qquad \text{for } w \in W$$

in $V_{\mathbb{R}}$. The cocycle condition (b) implies that

$$z_{vw} = {}^v z_w + z_v \qquad \text{for any } v,w \in W \tag{2}$$

and the positivity condition (c) that

$$\lambda(z_w) \leq 0 \qquad \text{for any } w \in W \text{ and } \lambda \in \Lambda^{--} \ . \tag{3}$$

Remark 2.2: $\{z \in V_{\mathbb{R}} : \lambda(z) \leq 0 \text{ for any } \lambda \in \Lambda^{--}\} = \sum_{\alpha\in\Phi^+} \mathbb{R}_{\geq 0} \cdot \mathrm{val}_L \circ\alpha$.

Proof: This reduces to the claim that the (closed) convex hull of Λ^{--} in $V^*_{\mathbb{R}}$ is equal to the antidominant cone

$$(V^*_{\mathbb{R}})^{--} = \{z^* \in V^*_{\mathbb{R}} : z^*(z) \leq 0 \text{ for any } z \in \sum_{\alpha \in \Phi^+} \mathbb{R}_{\geq 0} \cdot \mathrm{val}_L \circ \alpha\} \ .$$

Let $Z \subseteq G$ denote the connected component of the center of G. Then G/Z is semisimple and the sequence

$$0 \longrightarrow Z/Z_0 \longrightarrow T/T_0 \longrightarrow (T/Z)/(T/Z)_0 \longrightarrow 0$$

is exact. Hence the fundamental antidominant coweights for the semisimple group G/Z can be lifted to elements $\omega_1, \ldots, \omega_d \in V^*_{\mathbb{R}}$ in such a way that, for some $m \in \mathbb{N}$, we have $m\omega_1, \ldots, m\omega_d \in \Lambda^{--}$. It follows that

$$(V^*_{\mathbb{R}})^{--} = (Z/Z_0) \otimes \mathbb{R} + \sum_{i=1}^{d} \mathbb{R}_{\geq 0} \cdot \omega_i$$

and

$$\Lambda^{--} \supseteq Z/Z_0 + m \cdot \sum_{i=1}^{d} \mathbb{Z}_{\geq 0} \cdot \omega_i \ .$$

We therefore obtain from (3) that

$$z_w \in \sum_{\alpha \in \Phi^+} \mathbb{R}_{\geq 0} \cdot \mathrm{val}_L \circ \alpha \qquad \text{for any } w \in W \ . \tag{4}$$

In terms of these points z_w the set $V^\gamma_{\mathbb{R}}$ is given as

$$\begin{aligned}
&\{z \in V_{\mathbb{R}} : \lambda(z) \geq \lambda(-z_{w^{-1}}) \text{ for any } \lambda \in \Lambda,\ w \in W \text{ such that } {}^w\lambda \in \Lambda^{--}\} \\
&= \{z \in V_{\mathbb{R}} : {}^{w^{-1}}\lambda(z) \geq {}^{w^{-1}}\lambda(-z_{w^{-1}}) \text{ for any } w \in W \text{ and } \lambda \in \Lambda^{--}\} \\
&= \{z \in V_{\mathbb{R}} : \lambda({}^w z) \geq \lambda(z_w) \text{ for any } w \in W \text{ and } \lambda \in \Lambda^{--}\}
\end{aligned}$$

where the last identity uses (2). Obviously $V^\gamma_{\mathbb{R}}$ is a convex subset of $V_{\mathbb{R}}$. Using the partial order $\leq$ on $V_{\mathbb{R}}$ defined by Φ^+ (cf. [B-GAL] Chap. VI §1.6) we obtain from Remark 2.2 that

$$V^\gamma_{\mathbb{R}} = \{z \in V_{\mathbb{R}} : {}^w z \leq z_w \text{ for any } w \in W\} \ .$$

Lemma 2.3: *$V^\gamma_{\mathbb{R}}$ is the convex hull in $V_{\mathbb{R}}$ of the finitely many points $-z_w$ for $w \in W$.*

Proof: From (2) and (4) we deduce that

$${}^w z_v + z_w = z_{wv} \geq 0 \quad \text{and hence} \quad {}^w(-z_v) \leq z_w$$

for any $v, w \in W$. It follows that all $-z_v$ and therefore their convex hull is contained in $V_{\mathbb{R}}^{\gamma}$. For the reverse inclusion suppose that there is a point $z \in V_{\mathbb{R}}^{\gamma}$ which does not lie in the convex hull of the $-z_w$. We then find a linear form $\ell \in V_{\mathbb{R}}^{*}$ such that $\ell(z) < \ell(-z_w)$ for any $w \in W$. Choose $v \in W$ such that $\ell_0 := {}^{v}\ell$ is antidominant. It follows that ${}^{v^{-1}}\ell_0(z) < {}^{v^{-1}}\ell_0(-z_w)$ and hence, using (2), that

$$\ell_0({}^{v}z) < \ell_0(-{}^{v}z_w) = \ell_0(z_v) - \ell_0(z_{vw})$$

for any $w \in W$. For $w := v^{-1}$ we in particular obtain

$$\ell_0({}^{v}z) < \ell_0(z_v) \ .$$

On the other hand, since $z \in V_{\mathbb{R}}^{\gamma}$, we have

$$\lambda({}^{v}z) \geq \lambda(z_v)$$

for any $\lambda \in \Lambda^{--}$ and hence for any λ in the convex hull of Λ^{--}. But as we have seen in the proof of Remark 2.2 the antidominant ℓ_0 belongs to this convex hull which leads to a contradiction.

Proposition 2.4: *i. $T'_{\gamma}(K)$ is the set of K-valued points of an open K-affinoid subdomain T'_{γ} in the torus T';*

ii. the Banach algebra $K\langle\Lambda;\gamma\rangle$ is naturally isomorphic to the ring of analytic functions on the affinoid domain T'_{γ};

iii. the affinoid domain T'_{γ} is the preimage, under the map "val", of the convex hull of the finitely many points $-z_w \in V_{\mathbb{R}}$ for $w \in W$;

iv. $K\langle\Lambda;\gamma\rangle^{W,\gamma}$ is an affinoid K-algebra.

Proof: It follows from Gordan's lemma ([KKMS] p. 7) that the monoid Λ^{--} is finitely generated. Choose a finite set of generators F^{--}, and let

$$F := \{{}^{w}\lambda : \lambda \in F^{--}\} \ .$$

Using the fact that, by construction, the function γ^{dom} is multiplicative within Weyl chambers we see that the infinitely many inequalities implicit in the definition of $T'_{\gamma}(K)$ can in fact be replaced by finitely many:

$$T'_{\gamma}(K) = \{\zeta \in T'(K) : |\zeta(\lambda)| \leq |\gamma^{dom}(\lambda)| \text{ for any } \lambda \in F\}.$$

We therefore define T'_{γ} to be the rational subset in T' given by the finitely many inequalities $|\gamma^{dom}(\lambda)^{-1}\lambda(\zeta)| \leq 1$ for $\lambda \in F$ and obtain point i. of our assertion.

Now choose indeterminates T_λ for $\lambda \in F$ and consider the commutative diagram of algebra homomorphisms

$$\begin{tikzcd}
o_K[T_\lambda : \lambda \in F] \arrow[r] \arrow[d, "\subseteq"'] & K[\Lambda]^0 \arrow[d, "\subseteq"] \\
K[T_\lambda : \lambda \in F] \arrow[r] \arrow[d, "\subseteq"'] & K[\Lambda] \arrow[d, "\subseteq"] \\
K\langle T_\lambda : \lambda \in F\rangle \arrow[r] & K\langle\Lambda;\gamma\rangle
\end{tikzcd}$$

where the horizontal arrows send T_λ to $\gamma^{dom}(\lambda)^{-1}\lambda$, where o_K is the ring of integers of K, and where $K[\Lambda]^0$ denotes the unit ball with respect to $\| \ \|_\gamma$ in $K[\Lambda]$. Again, the multiplicativity of γ^{dom} within Weyl chambers shows that all three horizontal maps are surjective. The lower arrow gives a presentation of $K\langle\Lambda;\gamma\rangle$ as an affinoid algebra. The middle arrow realizes the dual torus T' as a closed algebraic subvariety

$$\begin{array}{rcl} \iota : T' & \longrightarrow & \mathbb{A}^f \\ \zeta & \longmapsto & (\zeta(\lambda))_{\lambda\in F} \end{array}$$

in the affine space $\mathbb{A}^f$ where f denotes the cardinality of the set F. The surjectivity of the upper arrow shows that the norm $\| \ \|_\gamma$ on $K[\Lambda]$ is the quotient norm of the usual Gauss norm on the polynomial ring $K[T_\lambda : \lambda \in F]$. Hence the kernel of the lower arrow is the norm completion of the kernel I of the middle arrow. Since any ideal in the Tate algebra $K\langle T_\lambda : \lambda \in F\rangle$ is closed we obtain

$$K\langle\Lambda;\gamma\rangle = K\langle T_\lambda : \lambda \in F\rangle / I K\langle T_\lambda : \lambda \in F\rangle \ .$$

This means that the affinoid variety $Sp(K\langle\Lambda;\gamma\rangle)$ is the preimage under ι of the affinoid unit polydisk in $\mathbb{A}^f$. In particular, $Sp(K\langle\Lambda;\gamma\rangle)$ is an open subdomain in T' which is reduced and coincides with the rational subset T'_γ (cf. [FvP] Prop. 4.6.1(4)). This establishes point ii. of the assertion. The point iii. is Lemma 2.3. For point iv., as the invariants in an affinoid algebra with respect to a finite group action, $K\langle\Lambda;\gamma\rangle^{W,\gamma}$ is again affinoid (cf. [BGR] 6.3.3 Prop. 3).

Suppose that the group G is semisimple and adjoint. Then the structure of the affinoid algebra $K\langle\Lambda;\gamma\rangle^{W,\gamma}$ is rather simple. The reason is that for such a group the set Λ^{--} is the free commutative monoid over the fundamental antidominant cocharacters $\lambda_1, \ldots, \lambda_d$. As usual we let $K\langle X_1, \ldots, X_d\rangle$ denote the Tate algebra in d variables over K. Obviously we have a unique continuous algebra homomorphism

$$K\langle X_1, \ldots, X_d\rangle \longrightarrow K\langle\Lambda;\gamma\rangle^{W,\gamma}$$

sending the variable X_i to σ_{λ_i}.

We also need a general lemma about orthogonal bases in normed vector spaces. Let $(Y, \| \ \|)$ be a normed K-vector space and suppose that Y has an orthogonal basis of the form $\{x_\ell\}_{\ell \in I}$. Recall that the latter means that

$$\| \sum_\ell c_\ell x_\ell \| = \sup_\ell |c_\ell| \cdot \|x_\ell\|$$

for any vector $\sum_\ell c_\ell x_\ell \in Y$. We suppose moreover that there is given a partial order $\leq$ on the index set I such that:

– Any nonempty subset of I has a minimal element;

– for any $k \in I$ the set $\{\ell \in I : \ell \leq k\}$ is finite.

(Note that the partial order $\leq$ on Λ^{--} has these properties.)

Lemma 2.5: *Suppose that $\|x_\ell\| \leq \|x_k\|$ whenever $\ell \leq k$; furthermore, let elements $c_{\ell k} \in K$ be given, for any $\ell \leq k$ in I, such that $|c_{\ell k}| \leq 1$; then the vectors*

$$y_k := x_k + \sum_{\ell < k} c_{\ell k} x_\ell$$

form another orthogonal basis of Y, and $\|y_k\| = \|x_k\|$.

Proof: We have

$$\|y_k\| = \max(\|x_k\|, \max_{\ell < k} |c_{\ell k}| \cdot \|x_\ell\|) = \|x_k\|$$

as an immediate consequence of our assumptions. We also have

$$x_k = y_k + \sum_{\ell < k} b_{\ell k} y_\ell$$

where $(b_{\ell k})$ is the matrix inverse to $(c_{\ell k})$ (over the ring of integers in K; cf. [B-GAL] Chap. VI §3.4 Lemma 4). Let now $x = \sum_k c_k x_k$ be an arbitrary vector in Y. We obtain

$$x = \sum_k c_k x_k = \sum_k c_k (\sum_{\ell \leq k} b_{\ell k} y_\ell) = \sum_\ell (\sum_{\ell \leq k} c_k b_{\ell k}) y_\ell \ .$$

Clearly $\|x\| \leq \sup_\ell |\sum_{\ell \leq k} c_k b_{\ell k}| \cdot \|y_\ell\|$. On the other hand we compute

$$\begin{aligned} \sup_\ell |\textstyle\sum_{\ell \leq k} c_k b_{\ell k}| \cdot \|y_\ell\| &\leq \sup_\ell \sup_{\ell \leq k} |c_k| \cdot \|y_\ell\| = \sup_\ell \sup_{\ell \leq k} |c_k| \cdot \|x_\ell\| \\ &\leq \sup_k |c_k| \cdot \|x_k\| = \|x\| \ . \end{aligned}$$

Proposition 2.6: *If the group G is semisimple and adjoint then the above map is an isometric isomorphism $K\langle X_1, \ldots, X_d\rangle \xrightarrow{\cong} K\langle \Lambda; \gamma\rangle^{W,\gamma}$.*

Proof: We write a given $\lambda \in \Lambda^{--}$ as $\lambda = \lambda_1^{m_1} \dots \lambda_d^{m_d}$ and put

$$\widetilde{\sigma}_\lambda := \sigma_{\lambda_1}^{m_1} \cdot \ldots \cdot \sigma_{\lambda_d}^{m_d} \ .$$

It suffices to show that these $\{\widetilde{\sigma}_\lambda\}_{\lambda \in \Lambda^{--}}$ form another orthonormal basis of $K\langle \Lambda; \gamma \rangle^{W,\gamma}$. One checks that the arguments in [B-GAL] Chap. VI §§3.2 and 3.4 work, over the ring of integers in K, equally well for our twisted W-action and show that we have

$$\widetilde{\sigma}_\lambda = \sigma_\lambda + \sum_{\mu < \lambda} c_{\mu\lambda} \sigma_\mu$$

with $|c_{\mu\lambda}| \leq 1$. So we may apply Lemma 2.5.

We finish this section with a discussion of those examples of a cocycle γ which will be relevant later on.

Example 1: We fix a prime element π_L of L. Let $\xi \in X^*(T)$ be a dominant integral weight and put

$$\gamma(w, \lambda(t)) := \pi_L^{\mathrm{val}_L(\xi({}^w t)) - \mathrm{val}_L(\xi(t))} \qquad \text{for } t \in T \ .$$

This map γ obviously has the properties (a),(b), and (d). For $t \in T^{--}$ we have $\lambda({}^w t) \leq \lambda(t)$ by [B-GAL] Chap. VI §1.6 Prop. 18; since ξ is dominant we obtain

$$\mathrm{val}_L \circ \xi(\frac{t}{{}^w t}) \leq 0 \ .$$

This means that $|\gamma(w, \lambda)| \leq 1$ for $\lambda \in \Lambda^{--}$ which is condition (c). We leave it as an exercise to the reader to check that the resulting Banach algebra $K\langle \Lambda; \gamma \rangle$ together with the twisted W-action, up to isomorphism, is independent of the choice of the prime element π_L.

Example 2: A particular case of a dominant integral weight is the determinant of the adjoint action of T on the Lie algebra $\mathrm{Lie}(N)$ of the unipotent radical N

$$\Delta(t) := \det(\mathrm{ad}(t); \mathrm{Lie}(N)) \ .$$

Its absolute value satisfies

$$\delta(t) = |\Delta(t)|_L^{-1}$$

where $\delta : P \longrightarrow \mathbb{Q}^\times \subseteq K^\times$ is the modulus character of the Borel subgroup P. We let K_q/K denote the splitting field of the polynomial $X^2 - q$ and we fix a root $q^{1/2} \in K_q^\times$. Then the square root $\delta^{1/2} : \Lambda \longrightarrow K_q^\times$ of the character δ is well defined. For a completely analogous reason as in the first example the cocycle

$$\gamma(w, \lambda) := \frac{\delta^{1/2}({}^w\lambda)}{\delta^{1/2}(\lambda)}$$

has the properties $(a) - (d)$. Moreover, using the root space decomposition of $\mathrm{Lie}(N)$ one easily shows that

$$\gamma(w, \lambda(t)) = \prod_{\alpha \in \Phi^+ \setminus {}^{w^{-1}}\Phi^+} |\alpha(t)|_L \ .$$

Hence the values of this cocycle γ are integral powers of q and therefore lie in K.

Example 3: Obviously the properties $(a) - (d)$ are preserved by the product of two cocycles. For any dominant integral weight $\xi \in X^*(T)$ therefore the cocycle

$$\gamma_\xi(w, \lambda(t)) := \frac{\delta^{1/2}({}^w\lambda)}{\delta^{1/2}(\lambda)} \cdot \pi_L^{\mathrm{val}_L(\xi({}^w t)) - \mathrm{val}_L(\xi(t))}$$

is K-valued and satisfies $(a) - (d)$. We write

$$V_{\mathbb{R}}^\xi := V_{\mathbb{R}}^{\gamma_\xi} \qquad \text{and} \qquad T'_\xi := T'_{\gamma_\xi} \ .$$

Let $\eta \in V_{\mathbb{R}}$ denote half the sum of the positive roots in Φ^+ and put

$$\eta_L := [L : \mathbb{Q}_p] \cdot \eta \ .$$

Let

$$\xi_L := \mathrm{val}_L \circ \xi \in V_{\mathbb{R}} \ .$$

For the points $z_w \in V_{\mathbb{R}}$ corresponding to the cocycle γ_ξ we then have

$$z_w = (\eta_L + \xi_L) - {}^w(\eta_L + \xi_L) \ .$$

In particular, $V_{\mathbb{R}}^\xi$ is the convex hull of the points ${}^w(\eta_L + \xi_L) - (\eta_L + \xi_L)$ for $w \in W$. Note that, since γ_ξ has values in $L^\times$, the affinoid variety T'_ξ is naturally defined over L. Given any point $z \in V_{\mathbb{R}}$, we will write z^{dom} for the unique dominant point in the W-orbit of z.

Lemma 2.7: $V_{\mathbb{R}}^\xi = \{z \in V_{\mathbb{R}} : (z + \eta_L + \xi_L)^{dom} \leq \eta_L + \xi_L\}$.

Proof: Using the formula before Lemma 2.3 we have

$$\begin{aligned} V_{\mathbb{R}}^\xi &= \{z \in V_{\mathbb{R}} : {}^w z \leq (\eta_L + \xi_L) - {}^w(\eta_L + \xi_L) \text{ for any } w \in W\} \\ &= \{z \in V_{\mathbb{R}} : {}^w(z + \eta_L + \xi_L) \leq \eta_L + \xi_L \text{ for any } w \in W\} \ . \end{aligned}$$

It remains to recall ([B-GAL] Chap. VI §1.6 Prop. 18) that for any $z \in V_{\mathbb{R}}$ and any $w \in W$ one has ${}^w z \leq z^{dom}$.

The γ_ξ in Example 3 are the cocycles which will appear in our further investigation of specific Banach-Hecke algebras. In the following we explicitly compute the affinoid domain T'_ξ in case of the group $G := GL_{d+1}(L)$. (In case $\xi = 1$ compare also [Vig] Chap. 3.) We let $P \subseteq G$ be the lower triangular Borel subgroup and $T \subseteq P$ be the torus of diagonal matrices. We take $U_0 := GL_{d+1}(o_L)$ where o_L is the ring of integers of L. If $\pi_L \in o_L$ denotes a prime element then

$$\Lambda^{--} = \{ \begin{pmatrix} \pi_L^{m_1} & & 0 \\ & \ddots & \\ 0 & & \pi_L^{m_{d+1}} \end{pmatrix} T_0 : m_1 \geq \ldots \geq m_{d+1} \} .$$

For $1 \leq i \leq d+1$ define the diagonal matrix

$$t_i := \begin{pmatrix} \pi_L & & & & & 0 \\ & \ddots & & & & \\ & & \pi_L & & & \\ & & & 1 & & \\ & & & & \ddots & \\ 0 & & & & & 1 \end{pmatrix} \quad \text{with } i \text{ diagonal entries equal to } \pi_L \ .$$

As a monoid Λ^{--} is generated by the elements $\lambda_1, \ldots, \lambda_{d+1}, \lambda_{d+1}^{-1}$ where $\lambda_i := \lambda(t_i)$. For any nonempty subset $I = \{i_1, \ldots, i_s\} \subseteq \{1, \ldots, d+1\}$ let $\lambda_I \in \Lambda$ be the cocharacter corresponding to the diagonal matrix having π_L at the places $i_1, \ldots, i_s$ and 1 elsewhere. Moreover let, as usual, $|I| := s$ be the cardinality of I and put $ht(I) := i_1 + \ldots + i_s$. These λ_I together with $\lambda_{\{1,\ldots,d+1\}}^{-1}$ form the W-orbit of the above monoid generators. From the proof of Prop. 2.4 we therefore know that T'_ξ as a rational subdomain of T' is described by the conditions

$$|\zeta(\lambda_I)| \leq |\gamma_\xi^{dom}(\lambda_I)|$$

for any I and

$$|\zeta(\lambda_{\{1,\ldots,d+1\}})| = |\gamma_\xi^{dom}(\lambda_{\{1,\ldots,d+1\}})| \ .$$

One checks that

$$|\gamma_1^{dom}(\lambda_I)| = |q|^{|I|(|I|+1)/2 - ht(I)} \ .$$

If the dominant integral weight $\xi \in X^*(T)$ is given by

$$\begin{pmatrix} g_1 & & 0 \\ & \ddots & \\ 0 & & g_{d+1} \end{pmatrix} \longmapsto \prod_{i=1}^{d+1} g_i^{a_i}$$

with $(a_1, \ldots, a_{d+1}) \in \mathbb{Z}^{d+1}$ then

$$|\gamma_\xi^{dom}(\lambda_I)| = |q|^{|I|(|I|+1)/2 - ht(I)} |\pi_L|^{\sum_{j=1}^{|I|} a_j - \sum_{i \in I} a_i} \ .$$

We now use the coordinates

$$\begin{array}{ccl} T'(K) & \longrightarrow & (K^\times)^{d+1} \\ \zeta & \longmapsto & (\zeta_1, \ldots, \zeta_{d+1}) \text{ with } \zeta_i := q^{i-1}\pi_L^{a_i}\zeta(\lambda_{\{i\}}) \end{array}$$

on the dual torus. In these coordinates T'_ξ is the rational subdomain of all $(\zeta_1, \ldots, \zeta_{d+1}) \in (K^\times)^{d+1}$ such that

$$\prod_{i \in I} |\zeta_i| \leq |q|^{|I|(|I|-1)/2} |\pi_L|^{\sum_{i=1}^{|I|} a_i}$$

for any proper nonempty subset $I \subseteq \{1, \ldots, d+1\}$ and

$$\prod_{i=1}^{d+1} |\zeta_i| = |q|^{d(d+1)/2} |\pi_L|^{\sum_{i=1}^{d+1} a_i} .$$

The advantage of these variables is the following. As usual we identify the Weyl group W with the symmetric group on the set $\{1, \ldots, d+1\}$. One checks that

$$\gamma_\xi(w, \lambda_{\{i\}}) = q^{w(i)-i} \pi_L^{a_{w(i)} - a_i}$$

for any $w \in W$ and $1 \leq i \leq d+1$. This implies that the twisted W-action on the affinoid algebra $K\langle\Lambda; \gamma_\xi\rangle$ is induced by the permutation action on the coordinates $\zeta_1, \ldots, \zeta_{d+1}$ of the affinoid domain T'_ξ. In fact, the above identity means that the cocycle γ_ξ can be written as the coboundary of an element in $T'(K)$. This is more generally possible for any group G whose derived group is simply connected (cf. [Gro] §8). We do not pursue this point of view systematically, though, since it is not compatible with general Langlands functoriality. But the problem of "splitting" the cocycle and the difficulty of reconciling the normalization of the Satake isomorphism will reappear as a technical complication in our attempt, in section 6, to treat Langlands functoriality.

3. The p-adic Satake isomorphism

Keeping the notations and assumptions introduced in the previous section we now consider a locally L-analytic representation (ρ, E) of G of the form

$$E = K_\chi \otimes_L E_L$$

where

– K_χ is a one dimensional representation of G given by a locally L-analytic character $\chi : G \longrightarrow K^\times$, and

– E_L is an L-rational irreducible representation ρ_L of G of highest weight ξ.

Let

$$E_L = \oplus_{\beta \in X^*(T)} E_{L,\beta}$$

be the decomposition into weight spaces for T. According to [BT] II.4.6.22 and Prop. II.4.6.28(ii) the reductive group G has a smooth connected affine model $\mathcal{G}$ over the ring of integers o_L in L such that $\mathcal{G}(o_L) = U_0$. We fix once and for all a U_0-invariant o_L-lattice M in E_L ([Jan] I.10.4) and let $\| \ \|$ be the corresponding U_0-invariant norm on E. The following fact is well-known.

Lemma 3.1: *We have* $M = \underset{\beta \in X^*(T)}{\oplus} M_\beta$ *with* $M_\beta := M \cap E_{L,\beta}$.

Proof: For the convenience of the reader we sketch the argument. Fix a weight $\beta \in X^*(T)$. It suffices to construct an element Π_β in the algebra of distributions $\mathrm{Dist}(\mathcal{G})$ which acts as a projector

$$\Pi_\beta : E_L \longrightarrow E_{L,\beta} \ .$$

Let B be the finite set of weights $\neq \beta$ which occur in E_L. Also we need the Lie algebra elements

$$H_i := (d\mu_i)(1) \in \mathrm{Lie}(\mathcal{G})$$

where $\mu_1, \ldots, \mu_r$ is a basis of the cocharacter group of T. We have

$$\underline{\gamma} := (d\gamma(H_1), \ldots, d\gamma(H_r)) \in \mathbb{Z}^r \quad \text{for any } \gamma \in X^*(T) \ .$$

According to [Hum] Lemma 27.1 we therefore find a polynomial $\Pi \in \mathbb{Q}[y_1,\ldots,y_r]$ such that $\Pi(\mathbb{Z}^r) \subseteq \mathbb{Z}$, $\Pi(\underline{\beta}) = 1$, and $\Pi(\underline{\gamma}) = 0$ for any $\gamma \in B$. Moreover [Hum] Lemma 26.1 says that the polynomial Π is a $\mathbb{Z}$-linear combination of polynomials of the form

$$\binom{y_1}{b_1} \cdot \ldots \cdot \binom{y_r}{b_r} \quad \text{with integers } b_1, \ldots, b_r \geq 0 \ .$$

Then [Jan] II.1.12 implies that

$$\Pi_\beta := \Pi(H_1, \ldots, H_r)$$

lies in $\mathrm{Dist}(\mathcal{G})$. By construction Π_β induces a projector from E_L onto $E_{L,\beta}$.

It follows that, for any $t \in T$, the operator norm of $\rho_L(t)$ on E_L is equal to

$$\|\rho_L(t)\| = \max\{|\beta(t)| : \beta \in X^*(T) \text{ such that } E_{L,\beta} \neq 0\}.$$

Lemma 3.2: *For any* $t \in T$ *we have* $\|\rho(t)\| = |\chi(t)| \cdot |\xi({}^w t)|$ *with* $w \in W$ *such that* ${}^w t \in T^{--}$.

Proof: Consider first the case $t \in T^{--}$ with $w = 1$. For any weight β occurring in E_L one has $\xi = \alpha\beta$ where α is an appropriate product of simple roots. But by definition of T^{--} we have $|\alpha(t)|_L \geq 1$ for any simple root α. For general $t \in T$ and $w \in W$ as in the assertion we then obtain

$$\begin{aligned}|\xi({}^w t)| &= \max\{|\beta({}^w t)| : E_{L,\beta} \neq 0\}\\ &= \max\{|\beta(t)| : E_{L,\beta} \neq 0\}\\ &= \|\rho_L(t)\| \ .\end{aligned}$$

Here the second identity is a consequence of the fact that the set of weights of E_L is W-invariant.

Collecting this information we first of all see that Lemma 1.4 applies and gives, for any open subgroup $U \subseteq U_0$, the isomorphism

$$\mathcal{H}(G, 1_U) \cong \mathcal{H}(G, \rho|U) \ .$$

But the norm $\| \ \|$ on $\mathcal{H}(G, \rho|U)$ corresponds under this isomorphism to the norm $\| \ \|_{\chi,\xi}$ on $\mathcal{H}(G, 1_U)$ defined by

$$\|\psi\|_{\chi,\xi} := \sup_{g\in G} |\psi(g)\chi(g)| \cdot \|\rho_L(g)\| \ .$$

If $|\chi|= 1$ (e.g., if the group G is semisimple) then the character χ does not affect the norm $\| \ \|_\xi := \| \ \|_{\chi,\xi}$. In general χ can be written as a product $\chi = \chi_1\chi_{un}$ of two characters where $|\chi_1| = 1$ and $\chi_{un}|U_0 = 1$. Then

$$\begin{array}{ccc}(\mathcal{H}(G, 1_U), \| \ \|_\xi) & \xrightarrow{\cong} & (\mathcal{H}(G, 1_U), \| \ \|_{\chi,\xi})\\ \psi & \longmapsto & \psi \cdot \chi_{un}^{-1}\end{array}$$

is an isometric isomorphism. We therefore have the following fact.

Lemma 3.3: *The map*

$$\begin{array}{ccc}\| \ \|_\xi\textit{-completion of } \mathcal{H}(G, 1_U) & \xrightarrow{\cong} & \mathcal{B}(G, \rho|U)\\ \psi & \longmapsto & \psi \cdot \chi_{un}^{-1}\rho\end{array}$$

is an isometric isomorphism of Banach algebras.

In this section we want to compute these Banach-Hecke algebras in the case $U = U_0$. By the Cartan decomposition G is the disjoint union of the double cosets U_0tU_0 with t running over T^{--}/T_0. Let therefore $\psi_{\lambda(t)} \in \mathcal{H}(G, 1_{U_0})$ denote the characteristic function of the double coset U_0tU_0. Then $\{\psi_\lambda\}_{\lambda\in\Lambda^{--}}$ is a K-basis of $\mathcal{H}(G, 1_{U_0})$. According to Lemma 3.2 the norm $\| \ \|_\xi$ on $\mathcal{H}(G, 1_{U_0})$ is given by

$$\|\psi\|_\xi := \sup_{t\in T^{--}} |\psi(t)\xi(t)| \ .$$

The $\{\psi_\lambda\}_{\lambda\in\Lambda^{--}}$ form a $\|\ \|_\xi$-orthogonal basis of $\mathcal{H}(G,1_{U_0})$ and hence of its $\|\ \|_\xi$-completion.

The Satake isomorphism computes the Hecke algebra $\mathcal{H}(G,1_{U_0})$. For our purposes it is important to consider the renormalized version of the Satake map given by

$$\begin{array}{rcl} S_\xi : \mathcal{H}(G,1_{U_0}) & \longrightarrow & K[\Lambda] \\ \psi & \longmapsto & \sum\limits_{t\in T/T_0} \pi_L^{\mathrm{val}_L(\xi(t))}(\sum\limits_{n\in N/N_0} \psi(tn))\lambda(t) \ . \end{array}$$

On the other hand we again let K_q/K be the splitting field of the polynomial X^2-q and we temporarily fix a root $q^{1/2}\in K_q$. Satake's theorem says (cf. [Car]§4.2) that the map

$$\begin{array}{rcl} S^{norm} : \mathcal{H}(G,1_{U_0})\otimes_K K_q & \longrightarrow & K_q[\Lambda] \\ \psi & \longmapsto & \sum\limits_{t\in T/T_0} \delta^{-1/2}(t)(\sum\limits_{n\in N/N_0} \psi(tn))\lambda(t) \end{array}$$

induces an isomorphism of K_q-algebras

$$\mathcal{H}(G,1_{U_0})\otimes_K K_q \xrightarrow{\cong} K_q[\Lambda]^W \ .$$

Here the W-invariants on the group ring $K_q[\Lambda]$ are formed with respect to the W-action induced by the conjugation action of $N(T)$ on T. Since $\pi_L^{\mathrm{val}_L\circ\xi}\delta^{1/2}$ defines a character of Λ it is clear that S_ξ is a homomorphism of algebras as well and a simple Galois descent argument shows that S_ξ induces an isomorphism of K-algebras

$$\mathcal{H}(G,1_{U_0}) \xrightarrow{\cong} K[\Lambda]^{W,\gamma_\xi}$$

where γ_ξ is the cocycle from Example 3 in section 2. The left hand side has the $\|\ \|_\xi$-orthogonal basis $\{\psi_\lambda\}_{\lambda\in\Lambda^{--}}$ with

$$\|\psi_{\lambda(t)}\|_\xi = |\xi(t)| \ .$$

The right hand side has the $\|\ \|_{\gamma_\xi}$-orthonormal basis $\{\sigma_\lambda\}_{\lambda\in\Lambda^{--}}$ where

$$\sigma_\lambda = \sum_{w\in W/W(\lambda)} \gamma_\xi(w,\lambda)\,{}^w\lambda$$

(cf. section 2). Since the maps

$$\begin{array}{rcl} N/N_0 & \xrightarrow{\simeq} & NtU_0/U_0 \\ nN_0 & \longmapsto & tnU_0 \end{array}$$

are bijections we have

$$\sum_{n\in N/N_0} \psi_{\lambda(s)}(tn) = |(NtU_0\cap U_0sU_0)/U_0| =: c(\lambda(t),\lambda(s)) \qquad \text{for any } s,t\in T \ .$$

It follows that

$$\begin{aligned} S_\xi(\psi_\mu) &= \sum_{t\in T/T_0} \pi_L^{\mathrm{val}_L(\xi(t))} c(\lambda(t),\mu)\lambda(t) \\ &= \sum_{\lambda\in\Lambda^{--}} \pi_L^{\mathrm{val}_L\circ\xi(\lambda)} c(\lambda,\mu)\sigma_\lambda \qquad \text{for any } \mu\in\Lambda^{--} \ . \end{aligned}$$

and

$$\pi_L^{\mathrm{val}_L\circ\xi({}^w\lambda)} c({}^w\lambda,\mu) = \gamma_\xi(w,\lambda)\pi_L^{\mathrm{val}_L\circ\xi(\lambda)} c(\lambda,\mu)$$

for any $\lambda\in\Lambda^{--}$, $\mu\in\Lambda$, and $w\in W$.

The reason for the validity of Satake's theorem lies in the following properties of the coefficients $c(\lambda,\mu)$.

Lemma 3.4: *For $\lambda,\mu\in\Lambda^{--}$ we have:*

i. $c(\mu,\mu)=1$;

ii. $c(\lambda,\mu)=0$ unless $\lambda\leq\mu$.

Proof: [BT] Prop. I.4.4.4.

Proposition 3.5: *The map S_ξ extends by continuity to an isometric isomorphism of K-Banach algebras*

$$\|\ \|_\xi\text{-completion of } \mathcal{H}(G,1_{U_0}) \xrightarrow{\cong} K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi} \ .$$

Proof: Define

$$\widetilde{\psi}_\lambda := \pi_L^{-\,\mathrm{val}_L\circ\xi(\lambda)}\psi_\lambda$$

for $\lambda\in\Lambda^{--}$. The left, resp. right, hand side has the $\|\ \|_\xi$-orthonormal, resp. $\|\ \|_{\gamma_\xi}$-orthonormal, basis $\{\widetilde{\psi}_\lambda\}_{\lambda\in\Lambda^{--}}$, resp. $\{\sigma_\lambda\}_{\lambda\in\Lambda^{--}}$. We want to apply Lemma 2.5 to the normed vector space $(K[\Lambda]^{W,\gamma_\xi},\|\ \|_{\gamma_\xi})$, its orthonormal basis $\{\sigma_\lambda\}$, and the elements

$$S_\xi(\widetilde{\psi}_\mu) = \sigma_\mu + \sum_{\lambda<\mu} \pi_L^{\mathrm{val}_L\circ\xi(\lambda)-\mathrm{val}_L\circ\xi(\mu)} c(\lambda,\mu)\sigma_\lambda$$

(cf. Lemma 3.4). The coefficients $c(\lambda,\mu)$ are integers and therefore satisfy $|c(\lambda,\mu)|\leq 1$. Moreover, $\lambda<\mu$ implies, since ξ is dominant, that $\mathrm{val}_L\circ\xi(\mu)\leq \mathrm{val}_L\circ\xi(\lambda)$. Hence the assumptions of Lemma 2.5 indeed are satisfied and we obtain that $\{S_\xi(\widetilde{\psi}_\lambda)\}$ is another orthonormal basis for $(K[\Lambda]^{W,\gamma_\xi},\|\ \|_{\gamma_\xi})$.

Corollary 3.6: *The Banach algebras $\mathcal{B}(G,\rho|U_0)$ and $K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi}$ are isometrically isomorphic.*

If $\xi = 1$ then, in view of Lemma 2.7, the reader should note the striking analogy between the above result and the computation in [Mac] Thm. (4.7.1) of the spectrum of the algebra of integrable complex valued functions on $U_0\backslash G/U_0$. The methods of proof are totally different, though. In fact, in our case the spherical function on $U_0\backslash G/U_0$ corresponding to a point in T_1' in general is not bounded.

Suppose that the group G is semisimple and adjoint. We fix elements $t_1, \ldots, t_d \in T^{--}$ such that $\lambda_i := \lambda(t_i)$ are the fundamental antidominant cocharacters. In Prop. 2.6 we have seen that then $K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi}$ is a Tate algebra in the variables $\sigma_{\lambda_1} \ldots, \sigma_{\lambda_d}$. Hence $\mathcal{B}(G, \rho|U_0)$ is a Tate algebra as well. But it seems complicated to compute explicitly the variables corresponding to the σ_{λ_i}. Instead we may repeat our previous reasoning in a modified way.

Proposition 3.7: *Suppose that G is semisimple and adjoint; then $\mathcal{B}(G, \rho|U_0)$ is a Tate algebra over K in the variables $\frac{\psi_{\lambda_1}\cdot\rho}{\xi(t_1)}, \ldots, \frac{\psi_{\lambda_d}\cdot\rho}{\xi(t_d)}$.*

Proof: By Lemma 3.3 and Prop. 3.5 it suffices to show that $K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi}$ is a Tate algebra in the variables $\xi(t_i)^{-1}S_\xi(\psi_{\lambda_i})$. We write a given $\lambda \in \Lambda^{--}$ as $\lambda = \lambda_1^{m_1} \ldots \lambda_d^{m_d}$ and put

$$\widetilde{\sigma}_\lambda := S_\xi(\widetilde{\psi}_{\lambda_1})^{m_1} \cdot \ldots \cdot S_\xi(\widetilde{\psi}_{\lambda_d})^{m_d} = S_\xi(\widetilde{\psi}_{\lambda_1}^{m_1} * \ldots * \widetilde{\psi}_{\lambda_d}^{m_d})$$

using notation from the proof of Prop. 3.5. Similarly as in the proof of Prop. 2.7 one checks that the arguments in [B-GAL] Chap. VI §§3.2 and 3.4 work, over the ring of integers in K, equally well for our twisted W-action (note that, in the language of loc. cit. and due to Lemma 3.4, the unique maximal term in $S_\xi(\widetilde{\psi}_{\lambda_i})$ is λ_i) and show that we have

$$\widetilde{\sigma}_\lambda = \sigma_\lambda + \sum_{\mu<\lambda} c_{\mu\lambda}\sigma_\mu$$

with $|c_{\mu\lambda}| \leq 1$. So we may apply again Lemma 2.5 and obtain that $\{\widetilde{\sigma}_\lambda\}$ is another orthonormal basis for $K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi}$. It remains to note that $\xi(t_i)$ and $\pi_L^{\mathrm{val}_L(\xi(t))}$ only differ by a unit.

Example: Consider the group $G := GL_{d+1}(L)$. Cor. 3.6 applies to G but Prop. 3.7 does not. Nevertheless, with the same notations as at the end of section 2 a simple modification of the argument gives

$$\mathcal{B}(G, \rho|U_0) = K\Big\langle \frac{\psi_{\lambda_1}\cdot\chi_{un}^{-1}\rho}{\xi(t_1)}, \ldots, \frac{\psi_{\lambda_d}\cdot\chi_{un}^{-1}\rho}{\xi(t_d)}, \big(\frac{\psi_{\lambda_{d+1}}\cdot\chi_{un}^{-1}\rho}{\xi(t_{d+1})}\big)^{\pm1}\Big\rangle .$$

Moreover in this case the λ_i are minimal with respect to the partial order $\leq$ so that we do have

$$\xi(t_i)^{-1}S_\xi(\psi_{\lambda_i}) = \sigma_{\lambda_i} .$$

Hence the above representation of $\mathcal{B}(G,\rho|U_0)$ as an affinoid algebra corresponds to the representation

$$K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi} = K\langle\sigma_{\lambda_1}\ldots,\sigma_{\lambda_d},\sigma_{\lambda_{d+1}}^{\pm1}\rangle \ .$$

On affinoid domains this corresponds to a map

$$T'_\xi \longrightarrow \{(\omega_1,\ldots,\omega_{d+1})\in K^{d+1} : |\omega_1|,\ldots,|\omega_d|\leq 1, |\omega_{d+1}| = 1\}$$

which, using our choice of coordinates on T' from section 2, is given by

$$(\zeta_1,\ldots,\zeta_{d+1}) \longmapsto (\ldots,q^{-\frac{(i-1)i}{2}}\xi(t_i)^{-1}\Sigma_i(\zeta_1,\ldots,\zeta_{d+1}),\ldots)$$

where

$$\Sigma_1(\zeta_1,\ldots,\zeta_{d+1}) = \zeta_1+\ldots+\zeta_{d+1},\ \ldots\ ,\Sigma_{d+1}(\zeta_1,\ldots,\zeta_{d+1}) = \zeta_1\cdot\ldots\cdot\zeta_{d+1}$$

denote the elementary symmetric polynomials.

Let us further specialize to the case $G = GL_2(L)$. Then E_L is the k-th symmetric power, for some $k\geq 0$, of the standard representation of GL_2. The highest weight of E_L is $\xi(\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix}) = t_2^k$. We obtain

$$\mathcal{B}(G,\rho|U_0) = K\big\langle X_1,(\pi_L^{-k}X_2)^{\pm1}\big\rangle \ .$$

with the variables $X_i := \psi_{\lambda_i}\cdot\chi_{un}^{-1}\rho$. The above map between affinoid domains becomes

$$(\zeta_1,\zeta_2) \longrightarrow (\zeta_1+\zeta_2, q^{-1}\pi_L^{-k}\zeta_1\zeta_2) \ .$$

4. p-adic Iwahori-Hecke algebras

With the same assumptions and notations as in the previous section we now let $U_1\subseteq U_0$ be the Iwahori subgroup such that $U_1\cap P = U_0\cap P$. In this section we will compute the Banach-Hecke algebras $\mathcal{B}(G,\rho|U_1)$. By Lemma 3.3 this means, similarly as before, computing the $\|\ \|_\xi$-completion of $\mathcal{H}(G,1_{U_1})$.

The extended affine Weyl group $\widetilde{W}$ of G is given by

$$\widetilde{W} := N(T)/T_0 \ .$$

Since the Weyl group W lifts to $U_0\cap N(T)/T_0\subseteq\widetilde{W}$ we see that $\widetilde{W}$ is the semidirect product of W and Λ. The Bruhat-Tits decomposition says that G is the disjoint union of the double cosets U_1xU_1 with x running over $\widetilde{W}$. Therefore, if we let $\tau_x\in\mathcal{H}(G,1_{U_1})$ denote the characteristic function of the double coset U_1xU_1, then $\{\tau_x\}_{x\in\widetilde{W}}$ is a K-basis of $\mathcal{H}(G,1_{U_1})$. The τ_x are known to be invertible in the algebra $\mathcal{H}(G, 1_{U_1})$. As a consequence of Lemma 3.2 the $\| \, \|_\xi$-norm is given by

$$\|\psi\|_\xi = \sup_{v,w \in W} \sup_{t \in T^{--}} |\psi(v\lambda(^w t))\xi(t)| \ .$$

In particular, $\{\tau_x\}_{x \in \widetilde{W}}$ is an $\| \, \|_\xi$-orthogonal basis of $\mathcal{H}(G, 1_{U_1})$ such that

$$\|\tau_x\|_\xi = |\xi(^w t)| \qquad \text{if } v, w \in W \text{ and } t \in T \text{ such that } x = v\lambda(t) \text{ and } {}^w t \in T^{--} \ .$$

We let $\mathcal{C}$ be the unique Weyl chamber corresponding to P in the apartment corresponding to T with vertex x_0 (cf. [Car]§3.5). The Iwahori subgroup U_1 fixes pointwise the unique chamber $C \subseteq \mathcal{C}$ with vertex x_0. The reflections at the walls of $\mathcal{C}$ generate the Weyl group W. Let $s_0, \ldots, s_e \in \widetilde{W}$ be the reflections at all the walls of C and let W_{aff} denote the subgroup of $\widetilde{W}$ generated by $s_0, \ldots, s_e$. This affine Weyl group W_{aff} with the generating set $\{s_0, \ldots, s_e\}$ is a Coxeter group. In particular we have the corresponding length function $\ell : W_{aff} \longrightarrow \mathbb{N} \cup \{0\}$ and the corresponding Bruhat order $\leq$ on W_{aff}. If $\Omega \subseteq \widetilde{W}$ is the subgroup which fixes the chamber C then $\widetilde{W}$ also is the semidirect product of Ω and W_{aff}. We extend the length function ℓ to $\widetilde{W}$ by $\ell(\omega w) := \ell(w)$ for $\omega \in \Omega$ and $w \in W_{aff}$. The Bruhat order is extended to $\widetilde{W}$ by the rule $\omega w \leq \omega' w'$, for $w, w' \in W_{aff}$ and $\omega, \omega' \in \Omega$, if and only if $\omega = \omega'$ and $w \leq w'$. One of the basic relations established by Iwahori-Matsumoto is:

(1) For any $x, y \in \widetilde{W}$ such that $\ell(xy) = \ell(x) + \ell(y)$ we have $\tau_{xy} = \tau_x * \tau_y$.

It easily implies that, for any $\lambda \in \Lambda$, the element

$$\Theta(\lambda) := \tau_{\lambda_1} * \tau_{\lambda_2}^{-1} \in \mathcal{H}(G, 1_{U_1})$$

where $\lambda = \lambda_1 \lambda_2^{-1}$ with $\lambda_i \in \Lambda^{--}$ is independent of the choice of λ_1 and λ_2. Moreover Bernstein has shown that the map

$$\begin{array}{rcl} \Theta : K[\Lambda] & \longrightarrow & \mathcal{H}(G, 1_{U_1}) \\ \lambda & \longmapsto & \Theta(\lambda) \end{array}$$

is an embedding of K-algebras.

Comment: It is more traditional (cf. [HKP] §1) to consider the embedding of K_q-algebras (with K_q/K and $q^{1/2} \in K_q$ be as before)

$$\begin{array}{rcl} \Theta^{norm} : K_q[\Lambda] & \longrightarrow & \mathcal{H}(G, 1_{U_1}) \otimes_K K_q \\ \lambda & \longmapsto & \delta^{-1/2}(\lambda)\tau_{\lambda_1} * \tau_{\lambda_2}^{-1} \end{array}$$

where $\lambda = \lambda_1 \lambda_2^{-1}$ with dominant λ_i. The modified map $\Theta^+ := \delta^{1/2} \cdot \Theta^{norm}$ already is defined over K. On $K[\Lambda]$ we have the involution ι_λ defined by $\iota_\Lambda(\lambda) := \lambda^{-1}$, and on $\mathcal{H}(G, 1_{U_1})$ there is the anti-involution ι defined by $\iota(\psi)(g) := \psi(g^{-1})$. We then have

$$\Theta = \iota \circ \Theta^+ \circ \iota_\Lambda \ .$$

In the following we consider the renormalized embedding of K-algebras

$$\begin{array}{llll}\Theta_\xi : & K[\Lambda] & \longrightarrow & \mathcal{H}(G, 1_{U_1}) \\ & \lambda & \longmapsto & \pi_L^{-\operatorname{val}_L \circ \xi(\lambda)} \Theta(\lambda) \ .\end{array}$$

In order to compute the norm induced, via Θ_ξ, by $\| \ \|_\xi$ on $K[\Lambda]$ we introduce the elements

$$\theta_x := q^{(\ell(x) - \ell(w) - \ell(\lambda_1) + \ell(\lambda_2))/2} \tau_w * \tau_{\lambda_1} * \tau_{\lambda_2}^{-1} \ .$$

for any $x \in \widetilde{W}$ written as $x = w\lambda_1\lambda_2^{-1}$ with $w \in W$ and $\lambda_i \in \Lambda^{--}$. Since $\ell(w) + \ell(\lambda_1) = \ell(w\lambda_1)$ (cf. [Vig] App.) we obtain from (1) that

$$\theta_x = q^{(\ell(w\lambda_1\lambda_2^{-1}) - \ell(w\lambda_1) + \ell(\lambda_2))/2} \tau_{w\lambda_1} * \tau_{\lambda_2}^{-1} \ .$$

On the other hand [Vig] Lemma 1.2 (compare also [Hai] Prop. 5.4) says that, for any $x, y \in \widetilde{W}$, the number

$$(\ell(xy^{-1}) - \ell(x) + \ell(y))/2$$

is an integer between 0 and $\ell(y)$ and that

$$\tau_x * \tau_y^{-1} = q^{-(\ell(xy^{-1}) - \ell(x) + \ell(y))/2} (\tau_{xy^{-1}} + Q_{x,y})$$

where $Q_{x,y}$ is a linear combination with integer coefficients of τ_z with $z < xy^{-1}$. It follows that for any $x \in \widetilde{W}$ we have

$$\theta_x = \tau_x + Q_x \tag{2}$$

where Q_x is a linear combination with integer coefficients of τ_z with $z < x$.

Lemma 4.1: *Consider two elements $x = w'\lambda$ and $y = v'\mu$ in $\widetilde{W}$ where $w', v' \in W$ and $\lambda, \mu \in \Lambda$; let $w, v \in W$ such that ${}^w\lambda, {}^v\mu \in \Lambda^{--}$; if $x \leq y$ then we have:*

i. ${}^v\mu - {}^w\lambda \in \sum_{\alpha \in \Phi^+} \mathbb{N}_0 \cdot (-\check{\alpha})$;

ii. $\|\tau_x\|_\xi \leq \|\tau_y\|_\xi$.

Proof: i. Let $w_0 \in W$ denote the longest element. We will make use of the identity

$$\{x' \in \widetilde{W} : x' \leq w_0({}^{w_0 v}\mu)\} = \bigcup_{\lambda'} W\lambda' W$$

where λ' ranges over all elements in Λ^{--} such that ${}^v\mu - \lambda' \in \sum_{\alpha \in \Phi^+} \mathbb{N}_0 \cdot (-\check{\alpha})$ (see [Ka2] (4.6) or [HKP] 7.8). Since $y \in W({}^v\mu)W$ this identity implies first that $x \leq y \leq ({}^{w_0 v}\mu)w_0$ and then that $x \in W\lambda' W$ for some $\lambda' \in \Lambda^{--}$ such that ${}^v\mu - \lambda' \in \sum_{\alpha \in \Phi^+} \mathbb{N}_0 \cdot (-\check{\alpha})$. Obviously we must have $\lambda' = {}^v\lambda$. ii. Let $\lambda = \lambda(t_1)$

and $\mu = \lambda(t_2)$. We have $\|\tau_x\|_\xi = |\xi({}^w t_1)|$ and $\|\tau_y\|_\xi = |\xi({}^v t_2)|$. Since highest weights are dominant we obtain from i. that $|\xi({}^v t_2({}^w t_1)^{-1})| \geq 1$.

It follows from Lemma 4.1.ii and formula (2) that Lemma 2.5 is applicable showing that $\{\theta_x\}_{x\in\widetilde{W}}$ is another $\| \ \|_\xi$-orthogonal basis of $\mathcal{H}(G, 1_{U_1})$ with

$$\|\theta_x\|_\xi = \|\tau_x\|_\xi \ .$$

For any $\lambda(t) = \lambda = \lambda_1\lambda_2^{-1} \in \Lambda$ with $\lambda_i \in \Lambda^{--}$ we have

$$\theta_\lambda = q^{(\ell(\lambda)-\ell(\lambda_1)+\ell(\lambda_2))/2}\pi_L^{\mathrm{val}_L(\xi(t))}\Theta_\xi(\lambda)$$

and

$$\|\theta_\lambda\|_\xi = \|\tau_\lambda\|_\xi = |\xi({}^w t)|$$

where $w \in W$ such that ${}^w t \in T^{--}$. In particular $\{\theta_\lambda\}_{\lambda\in\Lambda}$ is a $\| \ \|_\xi$-orthogonal basis of $\mathrm{im}(\Theta_\xi)$.

Lemma 4.2: *With the above notations we have*

$$q^{-(\ell(\lambda)-\ell(\lambda_1)+\ell(\lambda_2))/2} = \frac{\delta^{1/2}({}^w\lambda)}{\delta^{1/2}(\lambda)} \ .$$

Proof: Write $t = t_1t_2^{-1}$ with $\lambda(t_i) = \lambda_i$. According to the explicit formula for the length ℓ in [Vig] App. we have

$$q^{\ell(\lambda)} = \prod_{\alpha\in\Phi^+, |\alpha(t)|_L\geq 1} |\alpha(t)|_L \cdot \prod_{\alpha\in\Phi^+, |\alpha(t)|_L\leq 1} |\alpha(t)|_L^{-1}$$

and

$$q^{\ell(\lambda_i)} = \prod_{\alpha\in\Phi^+} |\alpha(t_i)|_L \ .$$

It follows that

$$q^{-(\ell(\lambda)-\ell(\lambda_1)+\ell(\lambda_2))/2} = \prod_{\alpha\in\Phi^+, |\alpha(t)|_L\leq 1} |\alpha(t)|_L$$

Since ${}^w t \in T^{--}$ we have $|{}^{w^{-1}}\alpha(t)|_L \geq 1$ for any $\alpha \in \Phi^+$. Hence $\{\alpha \in \Phi^+ : |\alpha(t)|_L < 1\} \subseteq \Phi^+ \setminus {}^{w^{-1}}\Phi^+$. By the last formula in Example 2 of section 2 the above right hand side therefore is equal to $\frac{\delta^{1/2}({}^w\lambda)}{\delta^{1/2}(\lambda)}$.

It readily follows that

$$\|\Theta_\xi(\lambda)\|_\xi = |\gamma_\xi^{dom}(\lambda)| \qquad \text{for any } \lambda \in \Lambda \ .$$

In other words

$$\Theta_\xi : (K[\Lambda], \| \ \|_{\gamma_\xi}) \longrightarrow (\mathcal{H}(G, 1_{U_1}), \| \ \|_\xi)$$

is an isometric embedding. Combining all this with Lemma 3.3 we obtain the following result.

Proposition 4.3: *i. The map*

$$\begin{array}{rcl} K\langle\Lambda;\gamma_\xi\rangle & \longrightarrow & \mathcal{B}(G,\rho|U_1) \\ \lambda & \longmapsto & \Theta_\xi(\lambda)\cdot\chi_{un}^{-1}\rho \end{array}$$

is an isometric embedding of Banach algebras;

ii. the map

$$\begin{array}{rcl} \mathcal{H}(U_0, 1_{U_1}) \otimes_K K\langle\Lambda;\gamma_\xi\rangle & \xrightarrow{\cong} & \mathcal{B}(G,\rho|U_1) \\ \tau_w \otimes \lambda & \longmapsto & (\tau_w * \Theta_\xi(\lambda))\cdot\chi_{un}^{-1}\rho \end{array}$$

is a K-linear isomorphism.

Remarks: 1) A related computation in the case $\xi = 1$ is contained in [Vig] Thm. 4(suite).

2) It is worth observing that the "twisted" W-action on $K\langle\Lambda;\gamma_\xi\rangle$ corresponds under the isomorphism Θ_ξ to the W-action on $\mathrm{im}(\Theta_\xi)$ given by

$$(w, \theta_\lambda) \longmapsto \theta_{{}^w\lambda} \ .$$

The results of this section and of the previous section are compatible in the following sense.

Proposition 4.4: *The diagram*

$$\begin{tikzcd} K\langle\Lambda;\gamma_\xi\rangle \arrow[r, "\Theta_\xi(.)\cdot\chi_{un}^{-1}\rho"] & \mathcal{B}(G,\rho|U_1) \arrow[d, "(\psi_{\lambda(1)}\cdot\chi_{un}^{-1}\rho)_*."] \\ K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi} \arrow[u, "\subseteq"] \arrow[r, "S_\xi^{-1}(.)\cdot\chi_{un}^{-1}\rho"] & \mathcal{B}(G,\rho|U_0) \end{tikzcd}$$

is commutative. Moreover, the image of $K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi}$ under the map $\Theta_\xi(.)\cdot\chi_{un}^{-1}\rho$ lies in the center of $\mathcal{B}(G,\rho|U_1)$.

Proof: We recall that the upper, resp. lower, horizontal arrow is an isometric unital monomorphism by Prop. 4.3.i, resp. by Lemma 3.3 and Prop. 3.5. The right perpendicular arrow is a continuous linear map respecting the unit elements. It suffices to treat the case of the trivial representation $\rho = 1$. By continuity we therefore are reduced to establishing the commutativity of the diagram

$$\begin{tikzcd}
K[\Lambda] \arrow[r, "\Theta"] & \mathcal{H}(G, 1_{U_1}) \arrow[d, "\psi_{\lambda(1)} * \cdot"] \\
K[\Lambda]^{W,\gamma_\xi} \arrow[u, "\subseteq"] \arrow[r, "S_1^{-1}"] & \mathcal{H}(G, 1_{U_0})
\end{tikzcd}$$

as well as the inclusion

$$\Theta(K[\Lambda]^{W,\gamma_\xi}) \subseteq \mathit{center\ of}\ \mathcal{H}(G, 1_{U_1}) \ .$$

It is known (cf. [HKP] Lemma 2.3.1, section 4.6, and Lemma 3.1.1) that:

– $\Theta^{norm}(K_q[\Lambda]^W) = \mathit{center\ of}\ \mathcal{H}(G, 1_{U_1}) \otimes_K K_q$;

– $\psi_{\lambda(1)} * \Theta^{norm} \circ S^{norm} = id$ on $\mathcal{H}(G, 1_{U_0}) \otimes_K K_q$;

– $\Theta^{norm} = \iota \circ \Theta^{norm} \circ \iota_\Lambda$ on $K_q[\Lambda]^W$.

The first identity implies the asserted inclusion. We further deduce that

$$\begin{aligned}
\Theta \circ S_1 &= \iota \circ (\delta^{1/2} \cdot \Theta^{norm}) \circ \iota_\Lambda \circ (\delta^{1/2} \cdot S^{norm}) \\
&= \iota \circ \Theta^{norm} \circ \iota_\Lambda \circ S^{norm} \\
&= \Theta^{norm} \circ S^{norm} \qquad\qquad \text{on } \mathcal{H}(G, 1_{U_0}) \otimes_K K_q
\end{aligned}$$

and hence that

$$\psi_{\lambda(1)} * (\Theta \circ S_1) = id \qquad\qquad \text{on } \mathcal{H}(G, 1_{U_0}) \ .$$

5. Crystalline Galois representations

We go back to the example of the group $G := GL_{d+1}(L)$ which we have discussed already at the end of section 3. But we now want to exploit Lemma 2.7. As before we fix a dominant integral weight $\xi \in X^*(T)$ that is given by

$$\begin{pmatrix} g_1 & & 0 \\ & \ddots & \\ 0 & & g_{d+1} \end{pmatrix} \longmapsto \prod_{i=1}^{d+1} g_i^{a_i}$$

with $(a_1, \ldots, a_{d+1}) \in \mathbb{Z}^{d+1}$. Note that the dominance means that

$$a_1 \leq \ldots \leq a_{d+1} \ .$$

Equally as before we use the coordinates

$$\begin{array}{ccl}
T'(K) & \longrightarrow & (K^\times)^{d+1} \\
\zeta & \longmapsto & (\zeta_1, \ldots, \zeta_{d+1}) \text{ with } \zeta_i := q^{i-1} \pi_L^{a_i} \zeta(\lambda_{\{i\}})
\end{array}$$

on the dual torus. Some times we view ζ as the diagonal matrix in $GL_{d+1}(K)$ with diagonal entries $(\zeta_1,\ldots,\zeta_{d+1})$. On the other hand, on the root space we use the coordinates

$$\begin{array}{rcl} V_{\mathbb{R}} = \mathrm{Hom}(\Lambda, \mathbb{R}) & \longrightarrow & \mathbb{R}^{d+1} \\ z & \longmapsto & (z_1,\ldots,z_{d+1}) \text{ with } z_i := z(\lambda_{\{i\}}) \ . \end{array}$$

In these coordinates we have:

1) The points η_L and ξ_L from Example 3 in section 2 correspond to

$$\frac{[L:\mathbb{Q}_p]}{2}(-d,-(d-2),\ldots,d-2,d) \quad \text{and} \quad (a_1,\ldots,a_{d+1}) \ ,$$

respectively.

2) The map $val : T'(K) \longrightarrow V_{\mathbb{R}}$ corresponds to the map

$$\begin{array}{ccc} (K^\times)^{d+1} & \longrightarrow & \mathbb{R}^{d+1} \\ (\zeta_1,\ldots,\zeta_{d+1}) & \longmapsto & (\mathrm{val}_L(\zeta_1),\ldots,\mathrm{val}_L(\zeta_{d+1})) - \xi_L - \widetilde{\eta}_L \ . \end{array}$$

where

$$\widetilde{\eta}_L := [L:\mathbb{Q}_p](0,1,\ldots,d) = \eta_L + \frac{[L:\mathbb{Q}_p]}{2}(d,\ldots,d) \ .$$

3) On $\mathbb{R}^{d+1}$ the partial order defined by Φ^+ is given by

$$(z_1,\ldots,z_{d+1}) \leq (z'_1,\ldots,z'_{d+1})$$

if and only if

$$z_{d+1} \leq z'_{d+1} \ , \ z_d + z_{d+1} \leq z'_d + z'_{d+1} \ , \ \ldots, \ z_2 + \ldots + z_{d+1} \leq z'_2 + \ldots + z'_{d+1}$$

and

$$z_1 + \ldots + z_{d+1} = z'_1 + \ldots + z'_{d+1} \ .$$

4) The map $z \longmapsto z^{dom}$ corresponds in $\mathbb{R}^{d+1}$ to the map which rearranges the coordinates in increasing order and which we will also denote by $(.)^{dom}$.

It now is a straightforward computation to show that Lemma 2.7 amounts to

$$T'_\xi = \{\zeta \in T' : (\mathrm{val}_L(\zeta_1),\ldots,\mathrm{val}_L(\zeta_{d+1}))^{dom} \leq \xi_L + \widetilde{\eta}_L\}.$$

Even more explicitly, T'_ξ is the domain of all $(\zeta_1,\ldots,\zeta_{d+1}) \in (K^\times)^{d+1}$ such that

$$(\mathrm{val}_L(\zeta_1),\ldots,\mathrm{val}_L(\zeta_{d+1}))^{dom} \leq (a_1, a_2 + [L:\mathbb{Q}_p],\ldots,a_{d+1} + d[L:\mathbb{Q}_p]) \ .$$

For any increasing sequence $\underline{r} = (r_1 \leq \ldots \leq r_{d+1})$ of real numbers we denote by $\mathcal{P}(\underline{r})$ the convex polygon in the plane through the points

$$(0,0), (1, r_1), (2, r_1 + r_2), \ldots, (d+1, r_1 + \ldots + r_{d+1}) \; .$$

We then may reformulate the above description of T'_ξ as follows.

Lemma 5.1: *T'_ξ is the subdomain of all $\zeta \in T'$ such that $\mathcal{P}(val(\zeta)^{dom})$ lies above $\mathcal{P}(\xi_L + \widetilde{\eta}_L)$ and both polygons have the same endpoint.*

We recall that a filtered K-isocrystal is a triple $\underline{D} = (D, \varphi, Fil^{\cdot} D)$ consisting of a finite dimensional K-vector space D, a K-linear automorphism φ of D – the "Frobenius" – , and an exhaustive and separated decreasing filtration $Fil^{\cdot} D$ on D by K-subspaces. In the following we fix the dimension of D to be equal to $d+1$ and, in fact, the vector space D to be the $d+1$-dimensional standard vector space $D = K^{d+1}$. We then may think of φ as being an element in the group $G'(K) := GL_{d+1}(K)$. The (filtration) type $type(\underline{D}) \in \mathbb{Z}^{d+1}$ is the sequence $(b_1, \ldots, b_{d+1})$, written in increasing order, of the break points b of the filtration $Fil^{\cdot} D$ each repeated $dim_K\, gr^b D$ many times. We put

$$t_H(\underline{D}) := \sum_{b \in \mathbb{Z}} b \cdot dim_K\, gr^b\, D \; .$$

Then $(d+1, t_H(\underline{D}))$ is the endpoint of the polygon $\mathcal{P}(type(\underline{D}))$. On the other hand we define the Frobenius type $s(\underline{D})$ of $\underline{D}$ to be the conjugacy class of the semisimple part of φ in $G'(K)$. We put

$$t_N^L(\underline{D}) := \mathrm{val}_L(\det_K(\varphi)) \; .$$

The filtered K-isocrystal $\underline{D}$ is called weakly L-admissible if $t_H(\underline{D}) = t_N^L(\underline{D})$ and $t_H(\underline{D}') \leq t_N^L(\underline{D}')$ for any filtered K-isocrystal $\underline{D}'$ corresponding to a φ-invariant K-subspace $D' \subseteq D$ with the induced filtration.

Proposition 5.2: *Let $\zeta \in T'(K)$ and let ξ be a dominant integral weight of G; then $\zeta \in T'_\xi(K)$ if and only if there is a weakly L-admissible filtered K-isocrystal $\underline{D}$ such that $type(\underline{D}) = \xi_L + \widetilde{\eta}_L$ and $\zeta \in s(\underline{D})$.*

Proof: Let us first suppose that there exists a filtered K-isocrystal $\underline{D}$ with the asserted properties. Then $\mathcal{P}(type(\underline{D})) = \mathcal{P}(\xi_L + \widetilde{\eta}_L)$ is the Hodge polygon of $\underline{D}$ and $\mathcal{P}(val(\zeta)^{dom})$ is its Newton polygon (relative to val_L). By [Fon] Prop. 4.3.3 (the additional assumptions imposed there on the field K are irrelevant at this point) the weak admissibility of $\underline{D}$ implies that its Newton polygon lies above its Hodge polygon with both having the same endpoint. Lemma 5.1 therefore implies that $\zeta \in T'_\xi(K)$.

We now assume vice versa that $\zeta \in T'_\xi(K)$. We let φ_{ss} be the semisimple automorphism of the standard vector space D given by the diagonal matrix with diagonal entries $(\zeta_1, \ldots, \zeta_{d+1})$. Let

$$D = D_1 + \ldots + D_m$$

be the decomposition of D into the eigenspaces of φ_{ss}. We now choose the Frobenius φ on D in such a way that φ_{ss} is the semisimple part of φ and that any D_j is φ-indecomposable. In this situation D has only finitely many φ-invariant subspaces D' and each of them is of the form

$$D' = D'_1 + \ldots + D'_m$$

with D'_j one of the finitely many φ-invariant subspaces of D_j. By construction the Newton polygon of (D, φ) is equal to $\mathcal{P}(val(\zeta)^{dom})$. To begin with consider any filtration $Fil^{\cdot} D$ of type $\xi_L + \widetilde{\eta}_L$ on D and put $\underline{D} := (D, \varphi, Fil^{\cdot} D)$. The corresponding Hodge polygon then is $\mathcal{P}(\xi_L + \widetilde{\eta}_L)$. By Lemma 5.1 the first polygon lies above the second and both have the same endpoint. The latter already says that

$$t_H(\underline{D}) = t_N^L(\underline{D}) \ .$$

It remains to be seen that we can choose the filtration $Fil^{\cdot} D$ in such a way that $t_H(\underline{D}') \leq t_N^L(\underline{D}')$ holds true for any of the above finitely many φ-invariant subspaces $D' \subseteq D$. The inequality between the two polygons which we have does imply that

$$a_1 + (a_2 + [L : \mathbb{Q}_p]) + \ldots + (a_{dim D'} + (dim\, D' - 1)[L : \mathbb{Q}_p]) \leq t_N^L(\underline{D}') \ .$$

Hence it suffices to find the filtration in such a way that we have

$$t_H(\underline{D}') \leq a_1 + (a_2 + [L : \mathbb{Q}_p]) + \ldots + (a_{dim D'} + (dim\, D' - 1)[L : \mathbb{Q}_p])$$

for any D'. But it is clear that for any filtration (of type $\xi_L + \widetilde{\eta}_L$) in general position we actually have

$$t_H(\underline{D}') = a_1 + (a_2 + [L : \mathbb{Q}_p]) + \ldots + (a_{dim D'} + (dim\, D' - 1)[L : \mathbb{Q}_p])$$

for the finitely many D'.

In order to connect this to Galois representations we have to begin with a different kind of filtered isocrystal (cf. [BM] §3.1). First of all we now suppose that K is a finite extension of $\mathbb{Q}_p$ (as always containing L). Then a filtered isocrystal over L with coefficients in K is a triple $\underline{M} = (M, \phi, Fil^{\cdot} M_L)$ consisting of a free $L_0 \otimes_{\mathbb{Q}_p} K$-module M of finite rank, a σ-linear automorphism ϕ of M – the "Frobenius" – , and an exhaustive and separated decreasing filtration $Fil^{\cdot} M_L$ on $M_L := L \otimes_{L_0} M$ by $L \otimes_{\mathbb{Q}_p} K$-submodules. Here L_0 denotes the maximal unramified subextension of L and σ its Frobenius automorphism. By abuse of notation we also write σ for the automorphism $\sigma \otimes id$ of $L_0 \otimes_{\mathbb{Q}_p} K$. We put

$$t_H(\underline{M}) := \sum_{b \in \mathbf{Z}} b \cdot dim_L\, gr^b\, M_L = [K:L] \cdot \sum_{b \in \mathbf{Z}} b \cdot dim_K\, gr^b\, M_L \ .$$

The equality is a consequence of the fact that for any finitely generated $L \otimes_{\mathbb{Q}_p} K$-module M' the identity

$$dim_L M' = [K:L] \cdot dim_K M'$$

holds true. By semisimplicity this needs to be verified only for a simple module which must be isomorphic to a field into which L and K both can be embedded and in which case this identity is obvious.

The number $t_N(\underline{M})$ is defined as $\mathrm{val}_{\mathbb{Q}_p}(\phi(x)/x)$ where x is an arbitrary nonzero element in the maximal exterior power of M as an L_0-vector space. But we have

$$\begin{aligned} t_N(\underline{M}) &= \mathrm{val}_{\mathbb{Q}_p}(\phi(x)/x) \\ &= \frac{1}{[L_0 : \mathbb{Q}_p]} \cdot \mathrm{val}_{\mathbb{Q}_p}(\det_{L_0}(\phi^{[L_0:\mathbb{Q}_p]})) \\ &= \frac{1}{[L_0 : \mathbb{Q}_p]} \cdot \mathrm{val}_{\mathbb{Q}_p}(\mathrm{Norm}_{K/L_0}(\det_K(\phi^{[L_0:\mathbb{Q}_p]}))) \\ &= \mathrm{val}_{\mathbb{Q}_p}(\mathrm{Norm}_{K/L_0}(\det_K(\phi))) \\ &= [K : L_0] \cdot \mathrm{val}_{\mathbb{Q}_p}(\det_K(\phi)) \\ &= [K : L] \cdot \mathrm{val}_L(\det_K(\phi)) \ . \end{aligned}$$

The filtered isocrystal $\underline{M}$ over L with coefficients in K is called weakly admissible (cf. [BM] Prop. 3.1.1.5) if $t_H(\underline{M}) = t_N(\underline{M})$ and $t_H(\underline{M}') \leq t_N(\underline{M}')$ for any subobject $\underline{M}'$ of $\underline{M}$ corresponding to a ϕ-invariant $L_0 \otimes_{\mathbb{Q}_p} K$-submodule $M' \subseteq M$ with the induced filtration on $L \otimes_{L_0} M'$.

By the main result of [CF] there is a natural equivalence of categories $V \longmapsto D_{cris}(V)$ between the category of K-linear crystalline representations of the absolute Galois group $\mathrm{Gal}(\overline{L}/L)$ of the field L and the category of weakly admissible filtered isocrystals over L with coefficients in K. It has the property that

$$dim_K\, V = rank_{L_0 \otimes_{\mathbb{Q}_p} K}\, D_{cris}(V) \ .$$

To avoid confusion we recall that a K-linear Galois representation is called crystalline if it is crystalline as a $\mathbb{Q}_p$-linear representation. We also recall that the jump indices of the filtration on $D_{cris}(V)_L$ are called the Hodge-Tate coweights of the crystalline Galois representation V (they are the negatives of the Hodge-Tate weights). Moreover, we will say that V is K-split if all eigenvalues of the Frobenius on $D_{cris}(V)$ are contained in K. This is a small technical condition which always can be achieved by extending the coefficient field K. More important is the following additional condition. We let $\mathbb{C}_p$ denote the completion of the algebraic closure $\overline{L}$. We may view V as an L-vector space through the inclusion $L \subseteq K$.

Definition: *A K-linear crystalline representation V of* $\mathrm{Gal}(\overline{L}/L)$ *is called special if the kernel of the natural map $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \twoheadrightarrow \mathbb{C}_p \otimes_L V$ is generated, as a $\mathbb{C}_p$-vector space, by its* $\mathrm{Gal}(\overline{L}/L)$*-invariants (for the diagonal action).*

On the full subcategory of special crystalline Galois representations we have a simplified form of the above equivalence of categories. This is well known (see [FR] Remark 0.3). But since we have not found any details in the literature we include them here for the convenience of the reader. We will speak of a K-isocrystal and an isocrystal over L with coefficients in K, respectively, if no filtration is prescribed. Suppose that (M, ϕ) is an isocrystal over L with coefficients in K. We then have the L_0-isotypic decomposition

$$M = \oplus_{\tau \in \Delta} M_\tau$$

where $\Delta := \mathrm{Gal}(L_0/\mathbb{Q}_p)$ and where M_τ is the K-subspace of M on which L_0 acts via the embedding $\tau : L_0 \hookrightarrow K$. One has

$$\phi(M_\tau) = M_{\tau\sigma^{-1}}$$

so that ϕ^f with $f := |\Delta|$ is an $L_0 \otimes_{\mathbb{Q}_p} K$-linear automorphism of M which respects the above decomposition. We see that $(M_1, \phi^f|M_1)$ is a K-isocrystal with $dim_K\, M_1 = rank_{L_0 \otimes_{\mathbb{Q}_p} K} M$.

Lemma 5.3: *The functor*

$$\begin{array}{ccc} \textit{category of isocrystals over } L & \xrightarrow{\sim} & \textit{category of } K\textit{-isocrystals} \\ \textit{with coefficients in } K & & \\ (M, \phi) & \longmapsto & (M_1, \phi^f|M_1) \end{array}$$

is an equivalence of categories.

Proof: Let $\mathcal{I}$ denote the functor in question. To define a functor $\mathcal{J}$ in the opposite direction let (D, φ) be a K-isocrystal. We put $M := L_0 \otimes_{\mathbb{Q}_p} D$ and $\phi := (\sigma \otimes 1) \circ \phi'$ with

$$\phi'|M_\tau := \begin{cases} \varphi & \text{if } \tau = 1, \\ id & \text{otherwise.} \end{cases}$$

Here we have used the K-linear composed isomorphism

$$D \longrightarrow L_0 \otimes_{\mathbb{Q}_p} D = M \overset{pr}{\twoheadrightarrow} M_1$$

to transport φ from D to M_1. At the same time it provides a natural isomorphism $id \simeq \mathcal{I} \circ \mathcal{J}$. The opposite natural isomorphism $id \simeq \mathcal{J} \circ \mathcal{I}$ is given by the composed maps

$$M_{\sigma^i} \xrightarrow{\phi^i} M_1 \xrightarrow{\cong} (L_0 \otimes_{\mathbb{Q}_p} M_1)_1 \overset{\sigma^{-i} \otimes \phi^{-f}}{\longrightarrow} (L_0 \otimes_{\mathbb{Q}_p} M_1)_{\sigma^i}$$

for $0 \leq i \leq f-1$.

Suppose now that M_L carries a filtration $Fil^\cdot M_L$ making $\underline{M} := (M, \phi, Fil^\cdot M_L)$ into a filtered isocrystal over L with coefficients in K. Let

$$M_L = \oplus_\beta M_{L,\beta}$$

where β runs over the $\mathrm{Gal}(\overline{K}/K)$-orbits in $\mathrm{Hom}_{\mathbb{Q}_p}(L, \overline{K})$ be the L-isotypic decomposition of the $L \otimes_{\mathbb{Q}_p} K$-module M_L. The filtration on M_L induces a filtration $Fil^\cdot M_{L,\beta}$ on each $M_{L,\beta}$ and by the naturality of the decomposition we have

$$Fil^\cdot M_L = \oplus_\beta Fil^\cdot M_{L,\beta} \ .$$

Moreover, let β_0 denote the orbit of the inclusion map $L \subseteq K$. Then M_{L,β_0} is the K-subspace of M_L on which L acts through the inclusion $L \subseteq K$. The composite map

$$M_1 \xrightarrow{\subseteq} M \longrightarrow L \otimes_{L_0} M = M_L \overset{pr}{\twoheadrightarrow} M_{L,\beta_0}$$

is a K-linear isomorphism which we may use to transport the filtration $Fil^\cdot M_{L,\beta_0}$ to a filtration $Fil^\cdot M_1$ on M_1. In this way we obtain the filtered K-isocrystal $\underline{D} := (M_1, \phi^f | M_1, Fil^\cdot M_1)$. Obviously the full original filtration $Fil^\cdot M_L$ can be recovered from $Fil^\cdot M_1$ if and only if it satisfies

$$(*) \qquad gr^0 M_{L,\beta} = M_{L,\beta} \qquad \text{for any } \beta \neq \beta_0 \ .$$

Let us suppose that the condition $(*)$ is satisfied. Since gr^0, by definition, does not contribute to the number $t_H(.)$ we obviously have

$$t_H(\underline{M}) = [K : L] \cdot t_H(\underline{D}) \ .$$

On the other hand, using a normal basis of L_0 over $\mathbb{Q}_p$ as well as the inverse functor in the proof of Lemma 5.3, we compute

$$\begin{aligned} t_N(\underline{M}) &= [K : L] \cdot \mathrm{val}_L(\det_K(\phi)) \\ &= [K : L] \cdot \mathrm{val}_L(\det_K((\sigma \otimes 1) \circ (\phi^f | M_1 \oplus id_{M_\sigma} \oplus \ldots \oplus id_{M_{\sigma^{f-1}}}))) \\ &= [K : L] \cdot \mathrm{val}_L(\det_K(\phi^f | M_1)) \\ &= [K : L] \cdot t_N^L(\underline{D}) \ . \end{aligned}$$

With $\underline{M}$ any of its subobjects also satisfies the condition $(*)$. Moreover, by Lemma 5.3, the subobjects of $\underline{M}$ are in one to one correspondence with the subobjects of $\underline{D}$). It follows that $\underline{M}$ is weakly admissible if and only if $\underline{D}$ is weakly L-admissible. Hence we have the induced equivalence of categories

$$\begin{array}{c}\text{category of weakly admissible}\\ \text{filtered isocrystals over } L \text{ with}\\ \text{coefficients in } K \text{ satisfying } (*)\end{array} \xrightarrow{\sim} \begin{array}{c}\text{category of weakly}\\ L\text{-admissible filtered}\\ K\text{-isocrystals.}\end{array}$$

Suppose now that $\underline{M} = D_{cris}(V)$ of some K-linear crystalline representation of $\mathrm{Gal}(\overline{L}/L)$. By the general theory of crystalline Galois representations we have the comparison isomorphism

$$ker(\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \longrightarrow\!\!\!\!\rightarrow \mathbb{C}_p \otimes_L V) \cong \underset{i\in\mathbf{Z}}{\oplus} \big(\mathbb{C}_p(-i) \otimes_L (\underset{\beta\neq\beta_0}{\oplus} gr^i M_{L,\beta})\big) \ .$$

It is Galois equivariant with $\mathrm{Gal}(\overline{L}/L)$ acting diagonally on the left and through the first factors on the right. For the Galois invariants we therefore obtain the formula

$$ker(\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \longrightarrow\!\!\!\!\rightarrow \mathbb{C}_p \otimes_L V)^{\mathrm{Gal}(\overline{L}/L)} \cong \underset{\beta\neq\beta_0}{\oplus} gr^0 M_{L,\beta} \ .$$

It follows that the isocrystal $D_{cris}(V)$ satisfies the condition $(*)$ if and only if the crystalline Galois representation V is special. Altogether we obtain that the functor $V \longmapsto D_{cris}(V)_1$ induces an equivalence of categories

$$\begin{array}{c}\text{category of } K\text{-linear special}\\ \text{crystalline representations}\\ \text{of } \mathrm{Gal}(\overline{L}/L)\end{array} \xrightarrow{\sim} \begin{array}{c}\text{category of weakly}\\ L\text{-admissible filtered}\\ K\text{-isocrystals.}\end{array}$$

It satisfies

$$dim_K V = dim_K D_{cris}(V)_1 \ .$$

Finally suppose that V is a

$$(+)\qquad \begin{array}{c}(d+1)\text{-dimensional } K\text{-linear } K\text{-split special crystalline}\\ \text{representation of } \mathrm{Gal}(\overline{L}/L) \text{ all of whose Hodge-Tate coweights have}\\ \text{multiplicity one and increase at least by } [L:\mathbb{Q}_p] \text{ in each step.}\end{array}$$

Precisely in this situation there is a dominant integral $\xi = (a_1, \ldots, a_{d+1})$ such that the Hodge-Tate coweights of V are $\xi_L + \widetilde{\eta}_L$. By Prop. 5.2 we find an up to permutation unique point $\zeta \in T'_\xi(K)$ such that $\zeta \in s(D_{cris}(V))$. This means we have constructed a surjection

$$\text{set of isomorphism classes of } V\text{'s with } (+) \longrightarrow\!\!\!\!\rightarrow \dot{\bigcup_{\xi\ dominant}} W\backslash T'_\xi(K) \ .$$

Let us again fix a dominant $\xi = (a_1, \ldots, a_{d+1})$ and let ρ_ξ denote the irreducible rational representation of G of highest weight ξ. By Prop. 2.4 and Cor. 3.6 we have an identification

$$W \backslash T'_\xi(K) \subseteq (W \backslash T'_\xi)(K) \simeq Sp(\mathcal{B}(G, \rho_\xi | U_0))(K)$$

where $Sp(\mathcal{B}(G, \rho | U_0))(K)$ the space of K-rational points of the affinoid variety $\mathcal{B}(G, \rho_\xi | U_0)$, i.e., the space of K-valued characters of the Banach-Hecke algebra $\mathcal{B}(G, \rho_\xi | U_0)$. Our map therefore becomes a map

$$\begin{array}{c} \text{set of isomorphism classes of} \\ (d+1)\text{-dimensional } K\text{-linear } K\text{-split} \\ \text{special crystalline representations of} \\ \mathrm{Gal}(\overline{L}/L) \text{ with Hodge-Tate coweights} \\ (a_1, a_2 + [L : \mathbb{Q}_p], \ldots, a_{d+1} + d[L : \mathbb{Q}_p]) \end{array} \longrightarrow Sp(\mathcal{B}(G, \rho_\xi | U_0))(K)$$

which we write as $V \longmapsto \zeta(V)$. We point out that in this form our map is canonical in the sense that it does not depend on the choice of the prime element π_L: This choice entered into our normalization of the Satake map S_ξ and into the coordinates on T' which we used; it is easy to check that the two cancel each other out. We also note that in the limit with respect to K this map is surjective.

We finish this section with a speculation in which way the map which we have constructed above might be an approximation of a true p-adic local Langlands correspondence. We view a point $\zeta \in Sp(\mathcal{B}(G, \rho_\xi | U_0))(K)$ as a character $\zeta : \mathcal{B}(G, \rho_\xi | U_0) \longrightarrow K$. Correspondingly we let K_ζ denote the one dimensional K-vector space on which $\mathcal{B}(G, \rho_\xi | U_0)$ acts through the character ζ. We may "specialize" the "universal" Banach $\mathcal{B}(G, \rho_\xi | U_0)$-module $B^G_{U_0}(\rho_\xi | U_0)$ from section 1 to ζ by forming the completed tensor product

$$B_{\xi,\zeta} := K_\zeta \,\widehat{\otimes}_{\mathcal{B}(G, \rho_\xi | U_0)}\, B^G_{U_0}(\rho_\xi | U_0) \ .$$

By construction the K-Banach space $B_{\xi,\zeta}$ still carries a continuous and isometric (for the quotient norm) action of G. A future p-adic local Langlands correspondence should provide us with a distinguished correspondence (being essentially bijective) between the fiber of our map in ζ (i.e., all V of the kind under consideration such that $\zeta(V) = \zeta$) and the isomorphism classes of all topologically irreducible "quotient" representations of $B_{\xi,\zeta}$. Unfortunately it is not even clear that the Banach spaces $B_{\xi,\zeta}$ are nonzero.

In order to describe the existing evidence for this picture we first have to recall how the characters of the Hecke algebra $\mathcal{H}(G, 1_{U_0})$ can be visualized representation theoretically. Any element $\zeta \in T'(K)$ can be viewed as a character $\zeta : T \to \Lambda \to K^\times$, and correspondingly we may form the unramified principal series representation

$$\mathrm{Ind}^G_P(\zeta)^\infty := \begin{array}{c} \text{space of all locally constant functions } F : G \longrightarrow K \text{ such that} \\ F(gtn) = \zeta(t)^{-1} F(g) \text{ for any } g \in G, t \in T, n \in N \end{array}$$

of G. The latter is a smooth G-representation of finite length. By the Iwasawa decomposition $G = U_0P$ the subspace of U_0-invariant elements in $\mathrm{Ind}_P^G(\zeta)^\infty$ is one dimensional so that the action of $\mathcal{H}(G, 1_{U_0})$ on it is given by a character ω_ζ. On the other hand ζ defines in an obvious way a character of the algebra $K[\Lambda]$ which we also denote by ζ. Using the Satake isomorphism from section 3 one then has (cf. [Ka1] Lemma 2.4(i))

$$\omega_\zeta = \zeta \circ S_1 = (\zeta \cdot \pi_L^{-\mathrm{val}_L(\xi(.))}) \circ S_\xi \ .$$

By [Ka1] Thm. 2.7 the "specialization" in ω_ζ

$$H_{1,\zeta} := K_{\omega_\zeta} \otimes_{\mathcal{H}(G,1_{U_0})} \mathrm{ind}_{U_0}^G(1_{U_0}) \ .$$

of the "universal" $\mathcal{H}(G, 1_{U_0})$-module $\mathrm{ind}_{U_0}^G(1_{U_0})$ from section 1 is an admissible smooth G-representation. Since it also is visibly finitely generated it is, in fact, of finite length. Since $\mathrm{ind}_{U_0}^G(1_{U_0})$ as a G-representation is generated by its U_0-fixed vectors the same must hold true for any of its quotient representations, in particular for any quotient of $H_{1,\zeta}$. But the subspace of U_0-invariant vectors in $H_{1,\zeta}$ is one dimensional. It follows that $H_{1,\zeta}$ possesses a single irreducible quotient representation $V_{1,\zeta}$ – the so called spherical representation for ζ. One has the G-equivariant map

$$\begin{array}{rcl} H_{1,\zeta} & \longrightarrow & \mathrm{Ind}_P^G(\zeta)^\infty \\ 1 \otimes f & \longmapsto & f * 1_\zeta := \sum_{g \in G/U_0} f(g)g(1_\zeta) \end{array}$$

where $1_\zeta \in \mathrm{Ind}_P^G(\zeta)^\infty$ denotes the unique U_0-invariant function with value one in $1 \in G$. Hence V_ζ can also be viewed as the, up to isomorphism, unique irreducible constituent of $\mathrm{Ind}_P^G(\zeta)^\infty$ with a nonzero U_0-fixed vector.

Bringing in again the dominant integral weight ξ we have the K-linear isomorphism

$$\begin{array}{rcl} \mathrm{ind}_{U_0}^G(1_{U_0}) \otimes_K \rho_\xi & \xrightarrow{\cong} & \mathrm{ind}_{U_0}^G(\rho_\xi|U_0) \\ f \otimes x & \longmapsto & f_x(g) := f(g)g^{-1}x \ . \end{array}$$

It is G-equivariant if, on the left hand side, we let G act diagonally. On the left, resp. right, hand side we also have the action of the Hecke algebra $\mathcal{H}(G, 1_{U_0})$ through the first factor, resp. the action of the Hecke algebra $\mathcal{H}(G, \rho_\xi|U_0)$. Relative to the isomorphism ι_{ρ_ξ} between these two algebras discussed in section 1 the above map is equivariant for these Hecke algebra actions as well. (Warning: But this map does not respect our norms on both sides.) By abuse of notation we will use the same symbol to denote characters of these two Hecke algebras which correspond to each other under the isomorphism ι_{ρ_ξ}. We obtain an induced G-equivariant isomorphism

$$H_{1,\zeta} \otimes_K \rho_\xi \xrightarrow{\cong} H_{\xi,\zeta} := K_{\omega_\zeta} \otimes_{\mathcal{H}(G,\rho_\xi|U_0)} \mathrm{ind}_{U_0}^G(\rho_\xi|U_0)$$

between "specializations". Since with $V_{1,\zeta}$ also

$$V_{\xi,\zeta} := V_{1,\zeta} \otimes_K \rho_\xi$$

is irreducible as a G-representation ([ST1] Prop. 3.4) we see that $V_{\xi,\zeta}$ is the unique irreducible quotient of $H_{\xi,\zeta}$ and is also the, up to isomorphism, unique irreducible constituent of $\mathrm{Ind}_P^G(\zeta)^\infty \otimes_K \rho_\xi$ which as a U_0-representation contains $\rho_\xi | U_0$.

Assuming once more that $\zeta \in T'_\xi(K)$ we, of course, have that

$$B_{\xi,\zeta} = \text{Hausdorff completion of } H_{\xi,\zeta}$$

with respect to the quotient seminorm from $\mathrm{ind}_{U_0}^G(\rho_\xi | U_0)$. We remark that the unit ball in $\mathrm{ind}_{U_0}^G(\rho_\xi | U_0)$ and a fortiori its image in $H_{\xi,\zeta}$ are finitely generated over the group ring $o_K[G]$. Hence in order to prove that the quotient topology on $H_{\xi,\zeta}$ is Hausdorff, i.e., that the canonical map $H_{\xi,\zeta} \longrightarrow B_{\xi,\zeta}$ is injective it suffices to exhibit some bounded open G-invariant o_K-submodule in $H_{\xi,\zeta}$.

Example 1: Let $G = GL_2(\mathbb{Q}_p)$, $\xi = (a_1, a_2)$ a dominant weight, and $\zeta = (\zeta_1, \zeta_2) \in (K^\times)^2$. By the discussion at the end of section 2 the defining conditions for the affinoid domain T'_ξ are

$$|\zeta_i| \leq |p|^{a_1} \quad \text{for } i = 1, 2 \quad \text{and} \quad |\zeta_1 \zeta_2| = |p|^{a_1 + a_2 + 1} \ .$$

The complete list of the weakly $\mathbb{Q}_p$-admissible filtered K-isocrystals with a Frobenius φ whose semisimple part is given by ζ is well known (cf. [BB] end of section 3.1): Up to conjugation we may assume that $|\zeta_1| \geq |\zeta_2|$.

Case 1: $|\zeta_1| = |p|^{a_1}$ and $|\zeta_2| = |p|^{a_2+1}$; then φ is semisimple, and there are (up to isomorphism) exactly two weakly $\mathbb{Q}_p$-admissible filtrations; one corresponds to a decomposable and the other to a reducible but indecomposable Galois representation.

Case 2: $\zeta_1 \neq \zeta_2$ with $|\zeta_i| < |p|^{a_1}$ for $i = 1, 2$; then φ is semisimple, and there is (up to isomorphism) exactly one weakly $\mathbb{Q}_p$-admissible filtration; it corresponds to an irreducible Galois representation.

Case 3: $\zeta_1 = \zeta_2$ with $|\zeta_i| < |p|^{a_1}$; then φ is not semisimple, and there is (up to isomorphism) exactly one weakly $\mathbb{Q}_p$-admissible filtration; it corresponds to an irreducible Galois representation.

In particular, the fiber of our above surjection consists of two elements in case 1 and of one element in cases 2 and 3.

On the other hand for $|\zeta_1| \geq |\zeta_2|$ the map $H_{\xi,\zeta} \xrightarrow{\cong} \mathrm{Ind}_P^G(\zeta)^\infty \otimes_K \rho_\xi$ always is an isomorphism. It therefore follows from [BB] Thm. 4.3.1 that our $B_{\xi,\zeta}$ coincides in Case 2 with the representation denoted by $\Pi(V)$ in loc. cit. Moreover, still in Case 2, by [BB] Cor.s 5.4.1/2/3 the representation of G in the Banach space $B_{\xi,\zeta}$ is topologically irreducible (in particular nonzero) and admissible in the sense of [ST2] §3. In Case 3 the same assertions are shown in [Bre] Thm. 1.3.3 under the restriction that $a_2 - a_1 < 2p - 1$ and $a_1 + a_2 \neq -3$ if $p \neq 2$, resp. $a_2 - a_1 < 2$ and $a_1 + a_2 \neq -1$ if $p = 2$.

We mention that in contrast to $B_{\xi,\zeta}$ the representation $\mathrm{Ind}_P^G(\zeta)^\infty \otimes_K \rho_\xi$ (or equivalently $\mathrm{Ind}_P^G(\zeta)^\infty$) is irreducible if and only if $\zeta_2 \neq p\zeta_1$. Hence reducibility can only occur for $a_1 = a_2$ in Case 1 and for $a_1 < a_2$ in Case 2.

It was Breuil's fundamental idea that the two dimensional crystalline Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with distinct Hodge-Tate weights should correspond to the Banach representations $B_{\xi,\zeta}$ of $GL_2(\mathbb{Q}_p)$. Our general speculation therefore should be seen as an attempt to extend his picture. But we warn the reader that the case of GL_2 is atypical insofar as in general, given a pair (ξ,ζ), there will be infinitely many possibilities for a weakly admissible filtration.

Example 2. The unit ball $\mathrm{ind}_{U_0}^G(1_{U_0})^0$ in the normed space $\mathrm{ind}_{U_0}^G(1_{U_0})$ is a module for the unit ball $\mathcal{H}(G,1_{U_0})^0$ in the Hecke algebra $\mathcal{H}(G,1_{U_0})$ (for the sup-norm in both cases). For the two groups $G = GL_2(L)$ and $G = GL_3(L)$ it is known that $\mathrm{ind}_{U_0}^G(1_{U_0})^0$ is free as an $\mathcal{H}(G,1_{U_0})^0$-module. For $G = GL_2(L)$ this is a rather elementary computation on the tree and for $G = GL_3(L)$ it is the main result in [BO] Thm. 3.2.4 (see also the paragraph after Thm. 1.5; we point out that the arguments in this paper actually prove freeness and not only flatness). Let $\{b_j\}_{j\in\mathbb{N}}$ be a basis. Then $\{1 \otimes b_j\}_j$ is a basis of $H_{1,\zeta}$ as a K-vector space, and $\sum_j o_K \cdot (1 \otimes b_j)$ is open in $H_{1,\zeta}$ for the quotient topology provided $\zeta \in T_1'(K)$. Hence the quotient topology on $H_{1,\zeta}$ is Hausdorff which means that the natural map $H_{1,\zeta} \longrightarrow B_{1,\zeta}$ is injective. In particular, $B_{1,\zeta}$ is nonzero.

Example 3: Let $G = GL_{d+1}(L)$ be general but assume that $\zeta \in \mathrm{Hom}(\Lambda, o_K^\times) \subseteq T'(K)$. Then, for any element $F \in \mathrm{Ind}_P^G(\zeta)^\infty$ the function $|F|(g) := |F(g)|$ is right P-invariant. Since G/P is compact we therefore may equip $\mathrm{Ind}_P^G(\zeta)^\infty$ with the G-invariant norm

$$\|F\| := \sup_{g\in G} |F|(g) \ .$$

Moreover, our above map

$$\mathrm{ind}_{U_0}^G(1_{U_0}) \longrightarrow H_{1,\zeta} \longrightarrow \mathrm{Ind}_P^G(\zeta)^\infty$$

then is continuous. Assuming in addition that $\zeta \in T_\xi'(K)$ we obtain by completion a G-equivariant continuous K-linear map

$$B_{1,\zeta} \longrightarrow \mathrm{Ind}_P^G(\zeta)^c \ .$$

The completion $\mathrm{Ind}_P^G(\zeta)^c$ of $\mathrm{Ind}_P^G(\zeta)^\infty$ is explicitly given by

$$\begin{aligned} \mathrm{Ind}_P^G(\zeta)^c := \quad & \text{space of all continuous functions } F : G \longrightarrow K \text{ such that} \\ & F(gtn) = \zeta(t)^{-1}F(g) \text{ for any } g \in G, t \in T, n \in N \end{aligned}$$

It is easy to show that $\mathrm{Ind}_P^G(\zeta)^c$ as a representation of G in a K-Banach space is admissible.

Conjecture: *If ζ is regular then the representation of G in the Banach space $\mathrm{Ind}_P^G(\zeta)^c$ is topologically irreducible.*

Suppose therefore that ζ is regular, i.e., is not fixed by any $1 \neq w \in W$ for the conjugation action of W on T'). It is then well known that:
– The smooth G-representation $\mathrm{Ind}_P^G(\zeta)^\infty$ is irreducible (for example by the Bernstein-Zelevinsky classification).
– The above map $H_{1,\zeta} \xrightarrow{\cong} \mathrm{Ind}_P^G(\zeta)^\infty$ is an isomorphism ([Ka1] Thm. 3.2 and Remark 3.3 or [Dat] Lemma 3.1).
The latter in particular implies that the quotient topology on $H_{1,\zeta}$ is Hausdorff and that the map $B_{1,\zeta} \longrightarrow \mathrm{Ind}_P^G(\zeta)^c$ has dense image. In this context we also mention, without proof, the following result.

Proposition 5.4: *For any two $\zeta, \zeta' \in \mathrm{Hom}(\Lambda, o_K^\times)$ the vector space of all G-equivariant continuous linear maps from $\mathrm{Ind}_P^G(\zeta)^c$ to $\mathrm{Ind}_P^G(\zeta')^c$ is zero if $\zeta \neq \zeta'$ and is $K \cdot id$ if $\zeta = \zeta'$.*

For $G = GL_2(\mathbb{Q}_p)$ the above conjecture follows from a combination of [ST1] §4 and [ST3] Thm. 7.1. If $\zeta = \zeta_{(1)} \otimes \ldots \otimes \zeta_{(d+1)}$ with unramified characters $\zeta_{(i)} : L^\times / o_L^\times \longrightarrow o_K^\times$ such that $\zeta_{(i)} \not\equiv \zeta_{(i+1)} \bmod \pi_K$ for any $1 \leq i \leq d$ then the above conjecture is a consequence of an irreducibility result in characteristic p in the thesis of R. Ollivier.

6. Weakly admissible pairs and functoriality

In the traditional Langlands program the irreducible smooth representations of a general group G over L are put into correspondence with continuous homomorphisms from the Galois group $\mathrm{Gal}(\overline{L}/L)$ (or rather the Weil-Deligne group of L) into the Langlands dual group G' of G. In order to do something in this spirit in our setting it is useful to slightly change our point of view which we motivate by looking once again at the GL_{d+1}-case. We started from a dominant weight $\xi \in X^*(T)$ and an element $\zeta \in T'(K)$ in the dual torus. Viewing ζ, by our particular choice of coordinates, as a diagonal matrix ζ_c in $G'(K) = GL_{d+1}(K)$ we considered the K-isocrystals (K^{d+1}, φ) such that ζ_c lies in the conjugacy class of the semisimple part of φ. The weight ξ was used to prescribe the type of the filtration which would make these isocrystals into filtered isocrystals. Our basic result then was that among all these filtered K-isocrystals there is at least one weakly L-admissible one if and only if $\zeta \in T'_\xi(K)$. Now we observe that ξ actually can be used to define a model filtration on K^{d+1}. Quite generally, for any K-rational cocharacter $\nu : \mathbb{G}_m \longrightarrow G'$ we decompose K^{d+1} into weight spaces

$$K^{d+1} = \oplus_{i \in \mathbf{Z}} (K^{d+1})_i$$

with respect to ν and put

$$Fil^i_\nu\, K^{d+1} := \oplus_{j\geq i}(K^{d+1})_j \ .$$

Because of $X^*(T) = X_*(T') \subseteq X_*(G')$ this in particular applies to $\xi\widetilde{\eta}_L$. Of course, the filtration $Fil^{\cdot}_{\xi\tilde{\eta}_L}\, K^{d+1}$ has no reason to be weakly L-admissible. But any other filtration of the same type as $Fil^{\cdot}_{\xi\tilde{\eta}_L}\, K^{d+1}$ is of the form $gFil^{\cdot}_{\xi\tilde{\eta}_L}\, K^{d+1} = Fil^{\cdot}_{g(\xi\tilde{\eta}_L)}\, K^{d+1}$ for some $g \in G'(K)$. Hence we may express our basic result also by saying that, given the pair (ξ,ζ), there is a pair $(\nu,\varphi) \in X_*(G')(K) \times G'(K)$ such that
– ν lies in the $G'(K)$-orbit of $\xi\widetilde{\eta}_L$,
– the semisimple part of φ is conjugate to ζ_c in $G'(K)$, and
– the filtered K-isocrystal $(K^{d+1}, \varphi, Fil^{\cdot}_\nu\, K^{d+1})$ is weakly L-admissible
if and only if $\zeta \in T'_\xi(K)$.

Let now G be again a general L-split reductive group. We denote by G' its Langlands dual group which we consider to be defined over L as well (cf. [Bor]). In particular, T' is a maximal L-split torus in G'. We view our dominant $\xi \in X^*(T) = X_*(T') \subseteq X_*(G')$, as above, as a K-rational cocharacter $\xi : \mathbb{G}_m \longrightarrow G'$ and $\zeta \in T'(K) \subseteq G'(K)$. For a general pair $(\nu, b) \in X_*(G')(K) \times G'(K)$ we introduce some constructions and terminology which is borrowed from [RZ] Chap. 1. Let $REP_K(G')$ denote the category of K-rational representations of G' and let FIC_K denote the category of filtered K-isocrystals. Both are additive tensor categories. The pair (ν, b) gives rise to the tensor functor

$$\begin{array}{rcl} I_{(\nu,b)} : REP_K(G') & \longrightarrow & FIC_K \\ (\rho, E) & \longmapsto & (E, \rho(b), Fil^{\cdot}_{\rho\circ\nu}\, E) \ . \end{array}$$

Definition: *The pair (ν, b) is called weakly L-admissible if the filtered K-isocrystal $I_{(\nu,b)}(\rho,E)$, for any (ρ,E) in $REP_K(G')$, is weakly L-admissible.*

Suppose that (ν, b) is weakly L-admissible. Then $I_{(\nu,b)}$ can be viewed as a functor

$$I_{(\nu,b)} : REP_K(G') \longrightarrow FIC_K^{L-adm}$$

into the full subcategory FIC_K^{L-adm} of weakly L-admissible filtered K-isocrystals which, in fact, is a Tannakian category (the shortest argument for this probably is to observe that for a Galois representation the property of being special crystalline is preserved by tensor products and to use the Colmez-Fontaine equivalence of categories). Moreover, letting $Rep_K^{con}(\mathrm{Gal}(\overline{L}/L))$ denote the category of finite dimensional K-linear continuous representations of $\mathrm{Gal}(\overline{L}/L)$ we know from the last section that the inverse of the functor $D_{cris}(.)_1$ induces a tensor functor between neutral Tannakian categories

$$FIC_K^{L-adm} \longrightarrow Rep_K^{con}(\mathrm{Gal}(\overline{L}/L)) \ .$$

By composing these two functors we therefore obtain a faithful tensor functor

$$\Gamma_{(\nu,b)} : REP_K(G') \longrightarrow Rep_K^{con}(\mathrm{Gal}(\overline{L}/L))$$

which possibly is no longer compatible with the obvious fiber functors. This is measured by a G'-torsor over K ([DM] Thm. 3.2). By Steinberg's theorem ([Ste] Thm. 1.9) that $H^1(K^{nr}, G') = 0$ over the maximal unramified extension K^{nr} of K this torsor is trivial over K^{nr}. It follows then from the general formalism of neutral Tannakian categories ([DM] Cor. 2.9, Prop. 1.13) that the functor $\Gamma_{(\nu,b)}$ gives rise to a K^{nr}-homomorphism in the opposite direction between the affine group schemes of the two categories which is unique up to conjugation in the target group. For $REP_K(G')$ this affine group scheme of course is G' ([DM] Prop. 2.8). For $Rep_K^{con}(\mathrm{Gal}(\overline{L}/L))$ we at least have that the K-rational points of this affine group scheme naturally contain the Galois group $\mathrm{Gal}(\overline{L}/L)$. Hence by restriction we obtain a continuous homomorphism of groups

$$\gamma_{\nu,b} : \mathrm{Gal}(\overline{L}/L) \longrightarrow G'(K^{nr})$$

which is determined by the functor $\Gamma_{(\nu,b)}$ up to conjugation in $G'(K^{nr})$. So we see that any weakly L-admissible pair (ν, b) determines an isomorphism class of "Galois parameters" $\gamma_{\nu,b}$. We remark that if the derived group of G' is simply connected Kneser ([Kne]) showed that $H^1(K, G') = 0$ so that in this case the Galois parameter $\gamma_{\nu,b}$ already has values in $G'(K)$. Following [RZ] p. 14 and [Win] one probably can establish an explicit formula for the cohomology class in $H^1(K, G')$ of the torsor in question.

We indicated already earlier that Langlands functoriality (for smooth representations) requires to work with the normalized Satake isomorphism S^{norm}. This forces us to assume in this section that our coefficient field K contains a square root of q and to pick one once and for all. As a consequence we also have a preferred square root $\delta^{1/2} \in T'(K)$ of $\delta \in T'(K)$. Being able to work with the normalized Satake map we do not have to consider the twisted W-action on $K[\Lambda]$. But, of course, we still have a norm in the picture which depends on ξ and which is the following. We consider the automorphism of K-algebras

$$\begin{array}{rccc} a_\xi : & K[\Lambda] & \longrightarrow & K[\Lambda] \\ & \lambda = \lambda(t) & \longmapsto & \delta^{1/2}(\lambda)\pi_L^{\mathrm{val}_L(\xi(t))}\lambda \end{array}$$

which intertwines the conjugation action by W on the source with the twisted action on the target. Pulling back along a_ξ the norm $\| \ \|_{\gamma_\xi}$ gives the norm

$$\| \sum_{\lambda\in\Lambda} c_\lambda \lambda \|_\xi^{norm} := \sup_{\lambda=\lambda(t)} |\delta^{1/2}({}^w\lambda)\pi_L^{\mathrm{val}_L(\xi({}^w t))} c_\lambda|$$

on $K[\Lambda]$ with $w \in W$ for each λ being chosen in such a way that ${}^w\lambda \in \Lambda^{--}$. Let $K\langle\Lambda;\xi\rangle$ denote the corresponding Banach algebra completion of $K[\Lambda]$. It follows from Prop. 2.4 that $K\langle\Lambda;\xi\rangle$ is the affinoid algebra of the affinoid subdomain $T'_{\xi,norm}$ obtained by pulling back T'_ξ along a_ξ. Since a_ξ induces on T' the map $\zeta \longmapsto \delta^{1/2}\pi_L^{\mathrm{val}_L \circ \xi}\zeta$ we deduce from Lemma 2.7 that

$$T'_{\xi,norm}(K) = val^{-1}(V_{\mathbb{R}}^{\xi,norm})$$

with

$$V_{\mathbb{R}}^{\xi,norm} := \{z \in V_{\mathbb{R}} : z^{dom} \leq \eta_L + \xi_L\} \ .$$

We have the commutative diagram

$$\begin{tikzcd}
 & \mathcal{B}(G,\rho_\xi|U_0) \arrow[d] & \\
 & \|\ \|_\xi\text{-completion of } \mathcal{H}(G,1_{U_0}) \arrow[dl, "S^{norm}"'] \arrow[dr, "S_\xi"] & \\
K\langle\Lambda;\xi\rangle^W \arrow[rr, "a_\xi"] & & K\langle\Lambda;\gamma_\xi\rangle^{W,\gamma_\xi}
\end{tikzcd}$$

in which, as a consequence of Lemma 3.3 and Prop. 3.5, all maps are isomorphisms of Banach algebras. In this section we use the left hand sequence of arrows to identify $\mathcal{B}(G,\rho_\xi|U_0)$ with the algebra of analytic functions on the affinoid space $W\backslash T'_{\xi,norm}$. In particular, this identifies $(W\backslash T'_{\xi,norm})(K)$ with the set of K-valued (continuous) characters of the Banach-Hecke algebra $\mathcal{B}(G,\rho_\xi|U_0)$.

Remark: *Using that $\delta(\lambda_{\{i\}}) = q^{-d+2(i-1)}$ the statement of Prop. 5.2 for the group $G = GL_{d+1}(L)$ becomes: $\zeta \in T'_{\xi,norm}(K)$ if and only if there is a weakly L-admissible filtered K-isocrystal $\underline{D}$ such that type$(\underline{D}) = \xi_L + \widetilde{\eta}_L$ and the semisimple part of its Frobenius is given by the diagonal matrix with entries $q^{d/2}\zeta(\lambda_{\{i\}})$.*

We note that in the case where η_L happens to be integral (i.e., if $d[L:\mathbb{Q}_p]$ is even) we can go one step further, can remove completely normalizations accidental to the group $GL_{d+1}(L)$, and can restate the above remark equivalently as follows. We have $\zeta \in T'_{\xi,norm}(K)$ if and only if there is a weakly L-admissible filtered K-isocrystal $\underline{D}$ such that *type*$(\underline{D}) = \xi_L + \eta_L$ and the semisimple part of its Frobenius is given by the diagonal matrix with entries $\zeta(\lambda_{\{i\}})$. Passing now to a general G this unfortunately forces us at present to work under the technical hypothesis that $\eta_L \in X^*(T) = X_*(T')$. This, for example, is the case if $[L:\mathbb{Q}_p]$ is even or if the group G is semisimple and simply connected. To emphasize that η_L then will be considered primarily as a rational cocharacter of T' we will use multiplicative notation and write $\xi\eta_L$ for the product of the rational cocharacters ξ and η_L. In this setting and for general G the analog of Prop. 5.2 is the following.

Proposition 6.1: *Suppose that η_L is integral, let $\xi \in X^*(T)$ be dominant, and let $\zeta \in T'(K)$; then there exists a weakly L-admissible pair (ν, b) (and hence a Galois parameter $\gamma_{\nu,b}$) such that ν lies in the $G'(K)$-orbit of $\xi\eta_L$ and b has semisimple part ζ if and only if $\zeta \in T'_{\xi,norm}(K)$.*

Proof: First let (ν, b) be a weakly L-admissible pair as in the assertion. Further let $\rho : G' \longrightarrow GL(E)$ be any K-rational representation. We then have the weakly L-admissible filtered K-isocrystal $(E, \rho(b), Fil^{\cdot}_{\rho\circ\nu} E)$. Furthermore $\rho\circ\nu$ is conjugate to $\rho \circ (\xi\eta_L)$ in $GL(E)(K)$ and $\rho(\zeta)$ is the semisimple part of $\rho(b)$. We fix a K-rational Borel subgroup $P_E \subseteq GL(E)$ and a maximal K-split torus $T_E \subseteq P_E$ such that $\rho(\zeta) \in T_E(K)$. There is a unique K-rational cocharacter $(\rho \circ \nu)^{dom} : \mathbb{G}_m \longrightarrow T_E$ which is dominant with respect to P_E and which is conjugate to $\rho\circ\nu$ in $GL(E)(K)$. Then $(\rho\circ\nu)^{dom} = (\rho\circ(\xi\eta_L))^{dom}$ corresponds to the type of the filtration $Fil^{\cdot}_{\rho\circ\nu} E$ in the sense of section 5. As in the first part of the proof of Prop. 5.2 we know from [Fon] Prop. 4.3.3 that the weak L-admissibility of our filtered isocrystal implies that the Newton polygon $\mathcal{P}((\rho(val(\zeta)))^{dom})$ lies above the Hodge polygon $\mathcal{P}((\rho \circ (\xi\eta_L))^{dom})$ with both having the same endpoint. But, as discussed before Lemma 5.1, this means that

$$(\rho(val(\zeta)))^{dom} \leq (\rho \circ (\xi\eta_L))^{dom} \ .$$

According to [FR] Lemma 2.1 the latter implies that

$$val(\zeta)^{dom} \leq (\xi\eta_L)^{dom} = \xi\eta_L \quad \text{, i.e., that} \quad \zeta \in T'_{\xi,norm}(K) \ .$$

For the reverse implication we first recall that, given any pair (ν, b) and any K-rational representation $\rho : G' \longrightarrow GL(E)$, the associated filtered K-isocrystal $(E, \rho(b), Fil^{\cdot}_{\rho\circ\nu} E)$ carries the canonical HN-filtration by subobjects (cf. [RZ] Prop. 1.4). The latter is stabilized by a unique parabolic subgroup $P^{\rho}_{(\nu,b)} \subseteq GL(E)$. We obviously have

$$\rho(b) \in P^{\rho}_{(\nu,b)}(K) \ .$$

The HN-filtrations, being functorial, equip our functor $I_{(\nu,b)}$ in fact with the structure of an exact $\otimes$-filtration in the sense of [Saa] IV.2.1.1. The exactness is trivial since the category $REP_K(G')$ is semisimple. The compatibility with the tensor product is a theorem of Faltings and Totaro (independently). It then follows from [Saa] Prop. IV.2.2.5 and Thm. IV.2.4 that

$$P_{(\nu,b)} := \bigcap_{\rho} \rho^{-1}(P^{\rho}_{(\nu,b)})$$

is a K-rational parabolic subgroup of G'. Since [Saa] only considers filtrations indexed by integers this requires the following additional observation. The category $REP_K(G')$ has a generator ([Saa] II.4.3.2) and is semisimple. From this one deduces that the jump indices in the HN-filtrations on all the values of our functor can be written with a common denominator. Hence all these HN-filtrations can be reindexed simultaneously in such a way that they become integral, and [Saa] applies. We emphasize that, denoting by $\mathbb{D}$ the protorus with character group $\mathbb{Q}$, one actually has a (not unique) K-rational homomorphism $\iota_{(\nu,b)} : \mathbb{D} \longrightarrow G'$ whose weight spaces define the HN-filtration on the functor $I_{(\nu,b)}$. Its centralizer in G' is a Levi subgroup of $P_{(\nu,b)}$.

Note that we have

$$b \in P_{(\nu,b)}(K) \ .$$

After these preliminaries we make our choice of the element b.

Lemma 6.2: *There is a regular element $b \in G'(K)$ with semisimple part ζ.*

Proof: Let $M' \subseteq G'$ denote the connected component of the centralizer of ζ in G'. We have:
– M' is connected reductive ([Ste] 2.7.a);
– M' is K-split of the same rank as G' (since $T' \subseteq M'$);
– $\zeta \in T'(K) \subseteq M'(K)$; in fact, ζ lies in the center of M'.
The regular unipotent conjugacy class in M', by its unicity ([Ste] Thm. 3.3), is defined over K. Since M' is K-split it therefore contains a point $u \in M'(K)$ ([Kot] Thm. 4.2). We put $b := \zeta u \in G'(K)$. The centralizer of b in G' contains with finite index the centralizer of u in M'. Hence b is regular in G' with semisimple part ζ.

We now fix $b \in G'(K)$ to be regular with semisimple part ζ.

Lemma 6.3: *There are only finitely many K-rational parabolic subgroups $Q \subseteq G'$ such that $b \in Q(K)$.*

Proof: Obviously it suffices to prove the corresponding statement over the algebraic closure $\overline{K}$ of K. By [Ste] Thm. 1.1 there are only finitely many Borel subgroups $Q_0 \subseteq G'$ such that $b \in Q_0(\overline{K})$. Let $Q \subseteq G'$ be any parabolic subgroup with $b \in Q(\overline{K})$. It suffices to find a Borel subgroup $Q_0 \subseteq Q$ such that $b \in Q_0(\overline{K})$. Consider the Levi quotient $\overline{M}$ of Q and the image $\overline{b} \in \overline{M}(\overline{K})$ of b. Then $\overline{b}$ is contained in some Borel subgroup $\overline{Q}_0 \subseteq \overline{M}$ (cf. [Hu1] Thm. 22.2) and we can take for Q_0 the preimage of $\overline{Q}_0$ in Q.

It follows that with ν varying over the $G'(K)$-orbit $\Xi \subseteq X_*(G')$ of $\xi\eta_L$ the family of parabolic subgroups $P_{(\nu,b)}$ actually is finite. Let $P_1, \ldots, P_m$ denote these finitely many parabolic subgroups and write

$$\Xi = \Xi_1 \cup \ldots \cup \Xi_m \qquad \text{with } \Xi_i := \{\nu \in \Xi : P_{(\nu,b)} = P_i\} \ .$$

We want to show that $\nu \in \Xi$ can be chosen in such a way that $P_{(\nu,b)} = G'$. Because then the homomorphism $\iota_{(\nu,b)} : \mathbb{D} \longrightarrow G'$ factorizes through the center of G'. Since by Schur's lemma the center of G' acts through scalars on any irreducible K-rational representation ρ of G' it follows that the HN-filtration on the filtered isocrystal $(E, \rho(b), Fil^{\cdot}_{\rho\circ\nu} E)$ for irreducible ρ has only one step. On the other hand, our assumption that $\zeta \in T'_{\xi,norm}(K)$ together with [FR] Lemma 2.1 imply that this filtered isocrystal, for any ρ, has HN-slope zero. Hence it is weakly L-admissible, first for irreducible ρ and then by passing to direct sums also for arbitrary ρ. This proves that the pair (ν, b) is weakly L-admissible.

We argue by contradiction and assume that all $P_1, \ldots, P_m \neq G'$ are proper parabolic subgroups. By [FR] Lemma 2.2.i we then find, for any $1 \leq i \leq m$, an irreducible K-rational representation $\rho_i : G' \longrightarrow GL(E_i)$ and a K-line $\ell_i \subseteq E_i$ such that

$$P_i = \text{stabilizer in } G' \text{ of } \ell_i$$

(in particular, $\ell_i \neq E_i$). We claim that $P^{\rho_i}_{(\nu,b)}$, for each $\nu \in \Xi_i$, stabilizes the line ℓ_i. To see this we have to recall the actual construction of ρ_i in loc. cit. Fix a maximal K-split torus T_i in a Levi subgroup M_i of P_i and fix a Borel subgroup $T_i \subseteq B_i \subseteq P_i$. By conjugation we may assume that all the homomorphisms $\iota_{(\nu,b)}$, for $\nu \in \Xi_i$, factorize through the center of M_i. Recall that M_i then is equal to the centralizer of $\iota_{(\nu,b)}$ in G'. Hence we may view these $\iota_{(\nu,b)}$ as elements in $X_*(T_i) \otimes \mathbb{Q}$ which lie in the interior of the facet defined by P_i (the latter follows from [Saa] Prop. IV.2.2.5.1)). Pick on the other hand a B_i-dominant character $\lambda_i \in X^*(T_i)$ which lies in the interior of the facet corresponding to P_i and let ρ_i be the rational representation of highest weight λ_i. Then, according to [FR], the highest weight space $\ell_i \subseteq E_i$ has the required property that P_i is its stabilizer in G'. Let $\lambda \in X^*(T_i)$ be any weight in E_i different from λ_i. Then $\lambda_i - \lambda$ is a nonzero linear combination with nonnegative integral coefficients of B_i-simple roots.

Claim: $(\lambda_i - \lambda)(\iota_{(\nu,b)}) > 0$

Proof: Let $\{\alpha_j : j \in \Delta\} \subseteq X^*(T_i)$ be the set of B_i-simple roots and let $J \subseteq \Delta$ denote the subset corresponding to P_i. The highest weight λ_i then satisfies

$$\lambda_i(\check{\alpha}_j) \begin{cases} = 0 & \text{if } j \in J, \\ > 0 & \text{if } j \notin J \end{cases}$$

where the $\check{\alpha}_j \in X_*(T_i)$ denote the simple coroots. On the other hand the connected center of M_i is equal to $(\bigcap_{j \in J} ker(\alpha_j))^\circ$, and we have

$$\alpha_j(\iota_{(\nu,b)}) \begin{cases} = 0 & \text{if } j \in J, \\ > 0 & \text{if } j \notin J. \end{cases}$$

We may write

$$\lambda_i - \lambda = \sum_{j \in \Delta} c_j \alpha_j \quad \text{with } c_j \in \mathbb{Z}_{\geq 0} \ .$$

Hence

$$(+)\qquad (\lambda_i - \lambda)(\iota_{(\nu,b)}) = \sum_{j\notin J} c_j\alpha_j(\iota_{(\nu,b)}) \geq 0$$

and we have to show that c_j, for at least one $j \notin J$, is nonzero. Let $\lambda' \in X^*(T_i)$ denote the unique dominant element in the orbit of λ under the Weyl group of T_i. Then λ' also is a weight occurring in E_i and we have

$$\lambda_i - \lambda' = \sum_{j\in\Delta} d_j\alpha_j \quad \text{and} \quad \lambda' - \lambda = \sum_{j\in\Delta} e_j\alpha_j \quad \text{with } d_j, e_j \in \mathbb{Z}_{\geq 0} \ .$$

In particular, $d_j + e_j = c_j$. Suppose first that $\lambda_i \neq \lambda'$. Then it suffices to find a $j \notin J$ such that $d_j > 0$. By the proof of [Hum] 13.4 Lemma B we obtain λ' from λ_i by successively subtracting simple roots while remaining inside the weights occurring in E_i in each step. But because of $\lambda_i(\check{\alpha}_j) = 0$ if $j \in J$ we know ([Hum] 21.3) that $\lambda_i - \alpha_j$ cannot be a weight occurring in E_i for any $j \in J$. This means of course that we have to have $d_j > 0$ for some $j \notin J$. Now assume that $\lambda_i = \lambda'$ so that $\lambda = {}^\sigma\lambda_i$ for some σ in the Weyl group of T_i. According to the proof of [Hum] 10.3 Lemma B we obtain λ from λ_i in the following way: Let σ_j be the reflection in the Weyl group corresponding to the simple root α_j. Write $\sigma = \sigma_{j_1}\ldots\sigma_{j_t}$ in reduced form. Then

$$\lambda_i - \lambda = \sum_{1\leq s\leq t} \sigma_{j_{s+1}}\ldots\sigma_{j_t}(\lambda_i)(\check{\alpha}_{j_s})\alpha_{j_s}$$

with all coefficients being nonnegative integers. Since the σ_j for $j \in J$ fix λ_i we may assume that $j_t \notin J$. Then the last term in the above sum is $\lambda_i(\check{\alpha}_{j_t})\alpha_{j_t}$ whose coefficient is positive.

This claim means that ℓ_i is a full weight space of $\rho_i \circ \iota_{(\nu,b)}$. But it follows from (+) also that the weight of $\mathbb{D}$ on ℓ_i is maximal with respect to the natural order on the character group $\mathbb{Q}$ of $\mathbb{D}$ among all weights of $\mathbb{D}$ occurring in E_i. Hence ℓ_i must be the bottom step in the HN-filtration of the filtered K-isocrystal $\underline{E}_{i,\nu} := (E_i, \rho_i(b), Fil^{\cdot}_{\rho_i\circ\nu} E_i)$ for each $\nu \in \Xi_i$. As such it carries the structure of a subobject $\underline{\ell}_{i,\nu} \subseteq \underline{E}_{i,\nu}$. As noted already, due to $\zeta \in T'_{\xi,norm}$, the HN-slope of $\underline{E}_{i,\nu}$ is zero. By the fundamental property of the HN-filtration (cf. [RZ] Prop. 1.4) the HN-slope of $\underline{\ell}_{i,\nu}$ then must be strictly positive which means that

$$t_H(\underline{\ell}_{i,\nu}) > t_N^L(\underline{\ell}_{i,\nu}) \ .$$

Suppose that we find an $1 \leq i \leq m$ and a $\nu \in \Xi_i$ such that ℓ_i is transversal to the filtration $Fil^{\cdot}_{\rho_i\circ\nu} E_i$. Let $(a_1,\ldots,a_r)$, resp. $(z_1,\ldots,z_r)$, denote the filtration type (in the sense of section 5), resp. the slopes written in increasing order, of the corresponding $\underline{E}_{i,\nu}$. The transversality means that $t_H(\underline{\ell}_{i,\nu}) = a_1$. On the other hand, since ℓ_i is a line we must have $t_N^L(\underline{\ell}_{i,\nu}) = z_j \geq z_1$. But because of

$\zeta \in T'_{\xi,norm}(K)$, once more [FR] Lemma 2.1, and Lemma 5.1 we have $z_1 \geq a_1$ which leads to the contradictory inequality

$$t_H(\underline{\ell}_{i,\nu}) \leq t_N^L(\underline{\ell}_{i,\nu}) \ .$$

It finally remains to justify our choice of ν. Since the filtration $Fil^{\cdot}_{\rho_i \circ \nu} E_i$ is well defined for any $\nu \in \Xi$ (and not only $\nu \in \Xi_i$) it suffices to establish the existence of some $\nu \in \Xi$ such that

$$\ell_i \text{ is transversal to } Fil^{\cdot}_{\rho_i \circ \nu} E_i \text{ for any } 1 \leq i \leq m \ .$$

Let $F_i \subset E_i$ denote the top step of the filtration $Fil^{\cdot}_{\rho_i \circ \xi \eta_L} E_i$. We have to find an element $g \in G'(K)$ such that

$$\rho_i(g)(\ell_i) \not\subseteq F_i \qquad \text{for any } 1 \leq i \leq m \ .$$

For each individual i the set $U_i := \{g \in G' : \rho_i(g)(\ell_i) \not\subseteq F_i\}$ is Zariski open in G'. Since ρ_i is irreducible the set U_i is nonempty. The intersection $U := U_1 \cap \ldots \cap U_m$ therefore still is a nonempty Zariski open subset of G'. But $G'(K)$ is Zariski dense in G' (cf. [Hu1] §34.4). Hence U must contain a K-rational point $g \in U(K)$. Then the cocharacter $\nu := g^{-1}(\xi\eta_L)$ has the properties which we needed.

We summarize that, under the integrality assumption on η_L, any K-valued character of one of our Banach-Hecke algebras $\mathcal{B}(G, \rho_\xi | U_0)$ naturally gives rise to a nonempty set of Galois parameters $\mathrm{Gal}(\overline{L}/L) \longrightarrow G'(\overline{K})$. The need to pass to the algebraic closure $\overline{K}$ comes from two different sources: First the element $\zeta \in T'_{\xi,norm}$ giving rise to a K-valued character of $\mathcal{B}(G, \rho_\xi | U_0)$ in general is defined only over a finite extension of K; secondly, to make Steinberg's theorem applicable we had to pass to the maximal unramified extension. In the spirit of our general speculation at the end of the last section we view this as an approximation to a general p-adic Langlands functoriality principle.

Without the integrality assumption on η_L one can proceed at least half way as follows. Let us fix, more generally, any natural number $r \geq 1$. We introduce the category of r-filtered K-isocrystals $FIC_{K,r}$ whose objects are triples $\underline{D} = (D, \varphi, Fil^{\cdot} D)$ as before only that the filtration $Fil^{\cdot} D$ is allowed to be indexed by $r^{-1}\mathbb{Z}$ (in particular, $FIC_K = FIC_{K,1}$). The invariants $t_H(\underline{D})$ and $t_N^L(\underline{D})$ as well as the notion of weak L-admissibility are defined literally in the same way leading to the full subcategory $FIC_{K,r}^{L-adm}$ of $FIC_{K,r}$.

Proposition 6.4: *$FIC_{K,r}^{L-adm}$ is a K-linear neutral Tannakian category.*

Proof: This follows by standard arguments from [Tot].

The tensor functor

$$\begin{array}{rcl} I_{(\nu,b)} : REP_K(G') & \longrightarrow & FIC_{K,r} \\ (\rho, E) & \longmapsto & (E, \rho(b), Fil^{\cdot}_{\rho\circ\nu} E) \end{array}$$

makes sense for any pair $(\nu, b) \in (X_*(G') \otimes r^{-1}\mathbb{Z})(K) \times G'(K)$ as does the notion of weak L-admissibility of such a pair. With these generalizations Prop. 6.1 continues to hold in complete generality (involving 2-filtered K-isocrystals) with literally the same proof. What is missing at present is the connection between the categories $FIC_{K,r}^{L-adm}$ and $Rep_K^{con}(\mathrm{Gal}(\overline{L}/L))$. This might involve a certain extension of the Galois group $\mathrm{Gal}(\overline{L}/L)$. We hope to come back to this problem in the future.

References

[BO] Bellaiche J., Otwinowska A.: Platitude du module universel pour GL_3 en caractéristique non banale. Bull. SMF 131, 507-525 (2003)

[BB] Berger L., Breuil C.: Représentations cristallines irréductibles de $GL_2(\mathbb{Q}_p)$. Preprint 2005

[Bor] Borel A.: Automorphic L-functions. In Automorphic Forms, Representations and L-Functions. Proc. Symp. Pure Math. 33 (2), pp. 27-61. American Math. Soc. 1979

[BGR] Bosch S., Güntzer U., Remmert R.: Non-Archimedean Analysis. Berlin-Heidelberg-New York: Springer 1984

[B-GAL] Bourbaki, N.: Groupes et algèbres de Lie, Chap. 4-6. Paris: Masson 1981

[Bre] Breuil C.: Invariant $\mathcal{L}$ et série spéciale p-adique. Ann. Sci. ENS 37, 559-610 (2004)

[BM] Breuil C., Mézard A.: Multiplicités modulaires et représentations de $GL_2(\mathbb{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ en $\ell = p$. Duke Math. J. 115, 205-310 (2002)

[BT] Bruhat F., Tits J.: Groupes réductifs sur un corps local, I, II. Publ. Math. IHES 41, 5-252 (1972), and 60, 5-184 (1984)

[Car] Cartier P.: Representations of $\mathfrak{p}$-adic groups: a survey. In Automorphic Forms, Representations and L-Functions. Proc. Symp. Pure Math. 33 (1), pp. 111-155. American Math. Soc. 1979

[CF] Colmez P., Fontaine J.-M.: Construction des représentations semistable. Invent. math. 140, 1-43 (2000)

[Dat] Dat J.-F.: Caractères à valeurs dans le centre de Bernstein. J. reine angew. Math. 508, 61-83 (1999)

[Del] Deligne P.: Formes modulaires et representations de $GL(2)$. In Modular Functions of One Variable II (Eds. Deligne, Kuyk). Lecture Notes in Math. 349, pp. 55-105. Berlin-Heidelberg-New York: Springer 1973

[DM] Deligne P., Milne J. S.: Tannakian categories. In Hodge Cycles, Motives, and Shimura Varieties (Eds. Deligne, Milne, Ogus, Shih). Lecture Notes in Math. 900, pp. 101-228. Berlin-Heidelberg-New York: Springer 1982

[Em1] Emerton M.: Jacquet modules of locally analytic representations of p-adic reductive groups I: Definitions and first properties. To appear in Ann. Sci. ENS

[Em2] Emerton M.: p-adic L-functions and unitary completions of representations of p-adic reductive groups. Duke Math. J. 130, 353-392 (2005)

[Fon] Fontaine J.-M.: Modules galoisiens, modules filtrés et anneaux Barsotti-Tate. Astérisque 65, 3-80 (1979)

[FR] Fontaine J.-M., Rapoport M.: Existence de filtrations admissibles sur des isocristaux. Bull. SMF 133, 73-86 (2005)

[FvP] Fresnel J., van der Put M.: Rigid Analytic Geometry and Its Applications. Boston-Basel-Berlin: Birkhäuser 2004

[Hai] Haines T.: The combinatorics of Bernstein functions. Trans. AMS 353, 1251-1278 (2001)

[HKP] Haines T., Kottwitz R., Prasad A.: Iwahori-Hecke algebras. Preprint

[Gro] Gross B.H.: On the Satake isomorphism. In Galois Representations in Arithmetic Algebraic Geometry (Eds. Scholl, Taylor), London Math. Soc. Lect. Notes 254, pp. 223-237. Cambridge Univ. Press 1998

[Hum] Humphreys J.E.: Introduction to Lie Algebras and Representation Theory. Berlin-Heidelberg-New York: Springer 1972

[Hu1] Humphreys J.E.: Linear Algebraic Groups. Berlin-Heidelberg-New York: Springer 1987

[Hu2] Humphreys J.E.: Reflection groups and Coxeter Groups. Cambridge Univ. Press 1990

[Jan] Jantzen J.C.: Representations of Algebraic Groups. Orlando: Academic Press 1987

[Ka1] Kato S.: On Eigenspaces of the Hecke Algebra with Respect to a Good Maximal Compact Subgroup of a p-Adic Reductive Group. Math. Ann. 257, 1-7 (1981)

[Ka2] Kato S.: Spherical Functions and a q-Analogue of Kostant's Weight Multiplicity Formula. Invent. math. 66, 461-468 (1982)

[KKMS] Kempf G., Knudsen F., Mumford D., Saint-Donat B.: Toroidal Embeddings I. Lecture Notes in Math. 339. Berlin-Heidelberg-New York: Springer 1973

[Kne] Kneser M.: Galois-Kohomologie halbeinfacher algebraischer Gruppen über $\mathfrak{p}$-adischen Körpern. I. Math. Z. 88, 40-47 (1965)

[Kot] Kottwitz R.: Rational conjugacy classes in reductive groups. Duke Math. J. 49, 785-806 (1982)

[Kut] Kutzko P.: Mackey's Theorem for non-unitary representations. Proc. AMS 64, 173-175 (1977)

[Mac] Macdonald I.G.: Spherical Functions on a Group of p-Adic Type. Ramanujan Institute Publ. 2 (1971)

[RZ] Rapoport M., Zink T.: Period Spaces for p-divisible Groups. Annals Math. Studies 141. Princeton Univ. Press 1996

[Saa] Saavedra Rivano N.: Catégories Tannakiennes. Lecture Notes in Math. 265. Berlin-Heidelberg-New York: Springer 1972

[ST1] Schneider P., Teitelbaum J.: $U(\mathfrak{g})$-finite locally analytic representations. Representation Theory 5, 111-128 (2001)

[ST2] Schneider P., Teitelbaum J.: Banach space representations and Iwasawa theory. Israel J. Math. 127, 359-380 (2002)

[ST3] Schneider P., Teitelbaum J.: Algebras of p-adic distributions and admissible representations. Invent. math. 153, 145-196 (2003)

[Ste] Steinberg R.: Regular elements of semi-simple algebraic groups. Publ. IHES 25, 49-80 (1965)

[Tot] Totaro B.: Tensor products in p-adic Hodge theory. Duke Math. J. 83, 79-104 (1996)

[Vig] Vigneras M.-F.: Algèbres de Hecke affines génériques. Preprint 2004

[Win] Wintenberger J.-P.: Propriétés du groupe Tannakien des structures de Hodge p-adiques et torseur entre cohomologies cristalline et étale. Ann. Inst. Fourier 47, 1289-1334 (1997)

Peter Schneider
Mathematisches Institut
Westfälische Wilhelms-Universität
Münster
Einsteinstr. 62
D-48149 Münster, Germany
pschnei@math.uni-muenster.de
http://www.uni-muenster.de/
math/u/schneider

Jeremy Teitelbaum
Department of Mathematics, Statistics
and Computer Science (M/C 249)
University of Illinois at Chicago
851 S. Morgan St.
Chicago, IL 60607, USA
jeremy@uic.edu
http://raphael.math.uic.edu/~jeremy

Higher Fields of Norms and (ϕ, Γ)-Modules

Dedicated to John Coates
on the occasion of his 60th birthday

Anthony J. Scholl

Received: December 1, 2005
Revised: March 3, 2006

Abstract. We describe a generalisation of the Fontaine-Wintenberger theory of the "field of norms" functor to local fields with imperfect residue field, generalising work of Abrashkin for higher dimensional local fields. We also compute the cohomology of associated p-adic Galois representations using (ϕ, Γ)-modules.

2000 Mathematics Subject Classification: 11S15, 11S23, 11S25, 12G05
Keywords and Phrases: local fields, ramification theory, Galois representations

Introduction

Abrashkin [3] has found an analogue of the field of norms functor for higher-dimensional local fields. His construction uses the theory of ramification groups [24] for such fields. As an application of his results (include the transfer of the ramification group structure from characteristic zero to characteristic p) he obtains the analogue of Grothendieck's anabelian conjecture for higher-dimensional local fields.
In the first part of this paper we construct an analogue of the field of norms for fairly general[1] local fields with imperfect residue field. Like Abrashkin's, as a starting point it uses the alternative characterisation of the ring of integers of the (classical) field of norms as a subring of Fontaine's ring $\mathcal{R} = \widetilde{\mathbf{E}}^+$ (the perfection of $\mathfrak{o}_{\overline{K}} \otimes \mathbb{F}_p$). However we differ from him, and the original construction by Fontaine and Wintenberger [12], [13], by making no appeal to

[1] The only requirement is that the residue field has a finite p-basis.

higher ramification theory. We instead restrict to extensions which are "strictly deeply ramified" (see §1.3 and Remark 1.3.8 below) and appeal instead to the differential characterisation of deeply ramified extensions which forms the basis for Faltings's approach to p-adic Hodge theory [10] (although we only use the most elementary parts of Faltings's work). These extensions are (in the classical case) closely related to strictly APF extensions; one may hope that by using Abbès and Saito's higher ramification theory ([1], [2]) a theory for all APF extensions could be developed. We hope to clarify this relation in a subsequent paper. In any case, the theory presented here includes those extensions which arise in the theory of (ϕ, Γ)-modules. It is also perhaps worth noting that in the classical case (perfect residue field), the 2 key propositions on which the theory depends (1.2.1 and 1.2.8) are rather elementary.

In the second part of the paper we begin the study of (ϕ, Γ)-modules in this setting, and prove the natural generalisation of Herr's formula [15] for the cohomology of a p-adic Galois representation. We also describe a natural family of (non-abelian) extensions to which this theory applies. We hope to develop this further in a subsequent paper.

This work grew out of the preparation of talks given during a study group at Cambridge in winter 2004, and the author is grateful to the members of the study group, particularly John Coates and Sarah Zerbes, for their comments and encouragement, to Victor Abrashkin, Ivan Fesenko and Jan Nekovář for useful discussions, to Pierre Colmez for letting me have some of his unpublished work, and to the referee for his careful reading of the paper. He also wishes to thank Bilkent University, Ankara, for their hospitality while parts of this paper were being written.

As the referee has pointed out, the possibility of such constructions has been known to the experts for some time (see for example the remarks on page 251 of [11]). After this paper was written the author received a copy of Andreatta and Iovita's preprints [4, 5], which construct rings of norms and compute the cohomology of (ϕ, Γ)-modules for Kummer-like extensions of more general p-adic base rings.

Notation

Throughout this paper p denotes a fixed prime number.

If A is an abelian group and ξ an endomorphism of A, or more generally an ideal in a ring of endomorphisms of A, we write A/ξ for $A/\xi A$, and $A[\xi]$ for the ξ-torsion subgroup of A.

If R is a ring of characteristic p, we denote by $f = f_R \colon x \mapsto x^p$ the Frobenius endomorphism of R.

If K is any p-adically valued field and $\lambda \in \mathbb{Q}$ belongs to the value group of K, we will by abuse of notation write p^λ for the fractional ideal comprised of all $x \in K$ with $v_p(x) \geq \lambda$.

We use the sign $=$ to denote equality or canonical isomorphism, and $A := B$ to indicate that A is by definition B.

1 Fields of norms

1.1 Big local fields

By a *big local field* we mean a complete discretely-valued field, whose residue field k has characteristic p and satisfies $[k : k^p] = p^d$ for some $d \geq 0$ (we then talk of a "d-big local field"). If K is such a field we use the usual notations: $\mathfrak{o}_K$ for its valuation ring, ϖ_K for a uniformiser (not always fixed), k_K or (if no confusion is likely) simply k for its residue field, and v_K for the normalised valuation on K with $v_K(\varpi_K) = 1$. When $\operatorname{char} K = 0$, we write e_K for its absolute ramification degree, and v_p for the p-adic valuation with $v_p(p) = 1$. Of course, $d = 0$ if and only if K is a local field in the usual sense (i.e., with perfect residue field).

We recall for convenience some facts about big local fields and their extensions, and fix some notation. If L/K is a finite separable extension of d-big local fields, then $[L : K] = ef_0p^s$ where $e = e(L/K) = v_L(\varpi_K)$ is the (reduced) ramification degree, and f_0 and p^s are the separable and inseparable degrees of the extension k_L/k_K, respectively, so that $f = f_0p^s = [k_L : k_K]$.

If L/K is a finite separable extension of big local fields, the valuation ring $\mathfrak{o}_L$ is not necessarily of the form $\mathfrak{o}_K[x]$. There are two particular cases when this is true:

(i) when the residue class extension k_L/k_K is separable [21, III, §6 Lemme 4]. Then there exists $x \in \mathfrak{o}_L$ with $\mathfrak{o}_L = \mathfrak{o}_K[x]$; and if $k_L = k_K$ then $x = \varpi_L$ for any uniformiser ϖ_L will do, and its minimal polynomial is an Eisenstein polynomial.

(ii) when $\varpi_K = \varpi_L$ and the residue class extension is purely inseparable and simple[2]. Let $k_L = k_K(b)$ for some b with $b^q = a \in k_K \setminus k_K^p$, and let $u \in \mathfrak{o}_L$ be any lift of b. Then $\mathfrak{o}_L = \mathfrak{o}_K[u]$ where the minimal polynomial of u has the form $g(T) = T^q + \sum_{i=1}^{q-1} c_iT^i - v$, with $\varpi_K | c_i$ and $a = v \bmod \varpi_K$.

Conversely, let $g = T^q + \sum_{i=0}^{q-1} c_iT^i \in \mathfrak{o}_K[T]$ be any polynomial. Let us say that g is a *fake Eisenstein polynomial* if (a) its degree q is a power of p; (b) for every $i \geq 1$, $c_i \equiv 0 \pmod{\varpi_K}$; and (c) c_0 is a unit whose reduction mod ϖ_K is not a p^{th} power. Then g is irreducible (since it is irreducible mod ϖ_K) and $\mathfrak{o}_K[T]/(g)$ is a discrete valuation ring. It is the valuation ring of a totally fiercely ramified extension of K of degree q.

In particular, if L/K is Galois of prime degree then one of (i), (ii) applies, so $\mathfrak{o}_L = \mathfrak{o}_K[x]$.

For any big local field K of characteristic zero there exists a complete subfield $K_u \subset K$ which is absolutely unramified (that is, p is a uniformiser) having the same residue field as K. (This holds by the existence of Cohen subrings; see for example [EGA4, 19.8.6] or [18, pp. 211–212]). If $d = 0$ then K_u is unique; otherwise (except when $e_K = 1$) it is non-unique [EGA4, 19.8.7]. If L/K is a finite extension it is not in general possible to find such subfields $K_u \subset K$, $L_u \subset L$ satisfying $K_u \subset L_u$ (even when K itself is absolutely unramified).

[2] In the terminology of [24], L/K is totally fiercely ramified.

Let K be a big local field with residue field k, and choose $K_u \subset K$ as above. Then for any m with $0 < m \le e_K$, the quotient $\mathfrak{o}_K/(\varpi_K^m)$ contains $\mathfrak{o}_{K_u}/(p) = k$ and therefore $\mathfrak{o}_K/(\varpi_K^m) \simeq k[\varpi_K]/(\varpi_K^m)$. When k is perfect (but not in general) this isomorphism is canonical, since the projection $\mathfrak{o}_K/(\varpi_K^m) \twoheadrightarrow k$ has a unique section, whose image is the maximal perfect subring of $\mathfrak{o}_K/(\varpi_K^m)$.

If K is a big local field of characteristic p then it contains a coefficient field (non-unique if $d > 0$), so that $K \simeq k_K((\varpi_K))$. If L/K is a finite separable extension then one cannot in general find a coefficient field of L containing one of K.

From now on, unless stated explicitly to the contrary, all big local fields will be assumed to have characteristic zero. For a finite extension L/K we then write

$$\delta(L/K) = \sum \delta_i(L/K) = v_p(\mathfrak{D}_{L/K})$$

where the $\delta_i(L/K)$ are the p-adic valuations of the primary factors of $\Omega(L/K)$.

1.2 Differentials and ramification

If L/K is an extension of big local fields, we usually write $\Omega(L/K) := \Omega_{\mathfrak{o}_L/\mathfrak{o}_K}$ for the module of relative Kähler differentials, which is an $\mathfrak{o}_L$-module of finite length. Then $\Omega(L/K)$ can be generated by $\le (d+1)$ generators (for example, by equation (1.2.2) below). The Fitting ideal of $\Omega(L/K)$ (the product of its primary factors) equals the relative different $\mathfrak{D}_{L/K}$, defined in the usual way as the inverse of the $\mathfrak{o}_K$-dual of $\mathfrak{o}_L$ with respect to the trace form; see for example [10, Lemma 1.1].

Proposition 1.2.1. *Let L/K be a finite extension of d-big local fields with $[L : K] = p^{d+1}$. Assume that there exists a surjection*

$$\Omega(L/K) \twoheadrightarrow (\mathfrak{o}_L/\xi)^{d+1}$$

for some ideal $\xi \subset \mathfrak{o}_K$ with $0 < v_p(\xi) \le 1$. Then $e(L/K) = p$ and $k_L = k_K^{1/p}$, and the Frobenius endomorphism of $\mathfrak{o}_L/\xi$ has a unique factorisation

$$\begin{tikzcd}
\mathfrak{o}_L/\xi \arrow[r, "f"] \arrow[d, two heads, "\text{mod } \xi'"'] & \mathfrak{o}_L/\xi \\
\mathfrak{o}_L/\xi' \arrow[r, dashed, "\simeq"] & \mathfrak{o}_K/\xi \arrow[u, hook, "\text{inclusion}"']
\end{tikzcd}$$

where $\xi' \subset \mathfrak{o}_L$ is the ideal with valuation $p^{-1}v_p(\xi)$. In particular, Frobenius induces a surjection $f \colon \mathfrak{o}_L/\xi \twoheadrightarrow \mathfrak{o}_K/\xi$.

Proof. Let ϖ_L be a uniformiser. We have $[L : K] = p^{d+1} = ef_0p^s$, and if $p^r = [k_L : k_L^p k]$ then $\dim_{k_L} \Omega_{k_L/k} = r \le s$. We have the exact sequence of differentials

$$(\varpi_L)/(\varpi_L^2) \longrightarrow \Omega(L/K) \otimes_{\mathfrak{o}_L} k_L \longrightarrow \Omega_{k_L/k} \longrightarrow 0 \qquad (1.2.2)$$

and if $e=1$ the first map is zero (taking $\varpi_L=\varpi_k$). It follows that

$$\dim_{k_L}\big(\Omega(L/K)\otimes_{\mathfrak{o}_L}k_L\big)\begin{cases}\le 1+r & \text{in general}\\ = r & \text{if } e=1.\end{cases}$$

By definition, $d=[k_L:k_L^p]\ge r$ and by hypothesis $\dim_{k_L}\big(\Omega(L/K)\otimes_{\mathfrak{o}_L}k_L\big)\ge d+1$, so we must have $r=s=d$, $f_0=1$, $e=p$ and $k_L=k^{1/p}$.

Let $\{t_\alpha\mid 1\le\alpha\le d\}\subset\mathfrak{o}_L^*$ be a lift of a p-basis for k_L. Then $d\varpi_L,\{dt_\alpha\}$ is a basis for $\Omega(L/K)\otimes k_L$. Introduce a multi-index notation $I=(i_1,\dots,i_d)$, $t^I=\prod t_\alpha^{i_\alpha}$. Then the k-vector space $\mathfrak{o}_L/(\varpi_K)$ has as a basis the reduction mod ϖ_K of the p^{d+1} monomials $\{t^I\varpi_L^j\mid 0\le j<p,\ 0\le i_\alpha<p\}$. So by Nakayama's lemma,

$$\mathfrak{o}_L=\mathfrak{o}_K[\varpi_L,\{t_\alpha\}]=\bigoplus_{\substack{0\le j<p\\0\le i_\alpha<p}}t^I\varpi_L^j\mathfrak{o}_K. \tag{1.2.3}$$

Lemma 1.2.4. *If $x=\sum_{0\le j<p,\,0\le i_\alpha<p}x_{I,j}t^I\varpi_L^j$ with $x_{I,j}\in\mathfrak{o}_K$, then*

$$v_p(x)=\min_{I,j}\Big(v_p(x_{I,j})+\frac{j}{e_L}\Big).$$

Proof. If $y_I\in\mathfrak{o}_K$ for $0\le i_\alpha<p$, then since the elements t^I are linearly independent mod (ϖ_L), we have

$$\varpi_L\big|\sum_I y_It^I\iff\text{for all } I,\ y_I\equiv 0\ (\mathrm{mod}\ \varpi_K)\iff\varpi_K\big|\sum_I y_It^I$$

from which we see that

$$v_K\Big(\sum_I y_It^I\Big)=\min_I v_K(y_I) \tag{1.2.5}$$

and that this is an integer. Therefore

$$v_K\Big(\varpi_L^j\sum_I x_{I,j}t^I\Big)\equiv\frac{j}{p}\quad(\mathrm{mod}\ \mathbb{Z})$$

and so

$$v_p(x)=v_p\Big(\sum_{j=0}^{p-1}\varpi_L^j\sum_I x_{I,j}t^I\Big)=\min_j\Big\{v_p\big(\varpi_L^j\sum_I x_{I,j}t^I\big)\Big\}.$$

Then the lemma follows from (1.2.5). □

From (1.2.3) we obtain $(d+1)$ relations in $\mathfrak{o}_L$ of the shape:

$$\varpi_L^p=\sum_{j=0}^{p-1}A_j(t)\varpi_L^j,\qquad t_\alpha^p=\sum_{j=0}^{p-1}B_{\alpha,j}(t)\varpi_L^j\quad(1\le\alpha\le d) \tag{1.2.6}$$

where A_j, $B_{\alpha,j} \in \mathfrak{o}_K[X_1, \ldots, X_d]$ are polynomials of degree $< p$ in each variable. Write D_γ for the derivative with respect to X_γ, and $\delta_{\alpha\gamma}$ for Kronecker delta. Therefore in $\Omega(L/K)$ the following relations hold:

$$\Big(-p\varpi_L^{p-1} + \sum_{j=1}^{p-1} jA_j(t)\varpi_L^{j-1}\Big)d\varpi_L + \sum_\gamma \Big(\sum_{j=0}^{p-1} D_\gamma A_j(t)\varpi_L^j\Big)dt_\gamma = 0$$
$$\Big(\sum_{j=1}^{p-1} jB_{\alpha,j}(t)\varpi_L^{j-1}\Big)d\varpi_L - pt_\alpha^{p-1}dt_\alpha + \sum_\gamma \Big(\sum_{j=0}^{p-1} D_\gamma B_{\alpha,j}(t)\varpi_L^j\Big)dt_\gamma = 0$$

The condition on $\Omega(L/K)$ forces all the coefficients in these identities to be divisible by ξ. From (1.2.4) this implies that for all $j > 0$, $A_j(t)\varpi_L^{j-1} \equiv 0 \equiv B_{\alpha,j}(t)\varpi_L^{j-1} \pmod{\xi}$. Therefore

$$\varpi_L^p \equiv A_0(t) \quad \text{and} \quad t_\alpha^p \equiv B_{\alpha,0}(t) \pmod{\varpi_L\xi}.$$

Similarly, for every γ and every $j \geq 0$,

$$D_\gamma A_j(t) \equiv D_\gamma B_{\alpha,j}(t) \equiv 0 \pmod{\varpi_L^{-j}\xi}.$$

This last congruence implies that the nonconstant coefficients of A_j and $B_{\alpha,j}$ are divisible by $\varpi_L^{-j}\xi$, so especially

$$A_0(t) \equiv A_0(0), \quad B_{\alpha,0}(t) \equiv B_{\alpha,0}(0) \pmod{\xi}.$$

The first of these congruences, together with 1.2.4 and the first equation of (1.2.6), implies that $v_L(A_0(0)) = p$. We will therefore choose $\varpi_K = A_0(0)$ as the uniformiser of K. Then

$$\varpi_L^p \equiv \varpi_K, \quad t_\alpha^p \equiv b_\alpha \pmod{\xi}$$

where $b_\alpha = B_{\alpha,0}(0) \in \mathfrak{o}_K^*$. If $m = v_K(\xi)$ then, as noted just before the statement of this Proposition, $\mathfrak{o}_K/\xi \xrightarrow{\sim} k[\varpi_K]/(\varpi_K^m)$. We fix such an isomorphism. If $\bar{b}_\alpha \in k$ denotes the reduction of b_α mod ϖ_K, then by (1.2.3) there are compatible isomorphisms

$$\mathfrak{o}_L/\xi \xrightarrow{\sim} k[\varpi_L, \{t_\alpha\}]/(\varpi_L^{mp}, \{t_\alpha^p - \bar{b}_\alpha\})$$
$$\mathfrak{o}_L/\xi' \xrightarrow{\sim} k[\varpi_L, \{t_\alpha\}]/(\varpi_L^m, \{t_\alpha^p - \bar{b}_\alpha\})$$

such that the inclusion $\mathfrak{o}_K/\xi \hookrightarrow \mathfrak{o}_L/\xi$ induces the identity on k and maps ϖ_K to ϖ_L^p. Therefore

$$\mathfrak{o}_L/\xi' \xrightarrow[f]{\sim} (\mathfrak{o}_L/\xi)^p = \mathfrak{o}_K/\xi \subset \mathfrak{o}_L/\xi$$

as required. □

Remark 1.2.7. It is perhaps worth noting that in the case $d = 0$ the proof just given simplifies greatly; in this case L/K is totally ramified by hypothesis, so ϖ_L satisfies an Eisenstein polynomial over K, whose constant term we may take to be $-\varpi_K$. We then have *canonical* isomorphisms $\mathfrak{o}_K/\xi = k[\varpi_K]/(\varpi_K^m)$, $\mathfrak{o}_L/\xi = k[\varpi_L]/(\varpi_L^{mp})$, and the minimal polynomial of ϖ_L gives at once the congruence $\varpi_L^p \equiv \varpi_K \pmod{\xi}$ — cf. [21], Remark 1 after Proposition 13 of §III.6.

Recall now the key lemma in the theory ([9], [10], [22]) of deep ramification of local fields:

Proposition 1.2.8. *(Faltings) Let L and K' be linearly disjoint finite extensions of a d-big local field K, and set $L' = LK' \simeq L \otimes_K K'$. Assume there exists a surjection $\Omega(K'/K) \twoheadrightarrow (\mathfrak{o}_{K'}/p^\lambda)^{d+1}$ for some $\lambda \geq 0$. Then*

$$\delta(L'/K') \leq \delta(L/K) - \frac{1}{d+2}\min(\lambda, \delta(L/K)).$$

Proof. (expanded from the proof of [10, Theorem 1.2]). For simplicity of notation write:

$$R = \mathfrak{o}_K,\ S = \mathfrak{o}_L,\ R' = \mathfrak{o}_{K'},\ S' = \mathfrak{o}_{L'}$$

$$\delta = \delta(L/K),\ \delta_i = \delta_i(L/K),\ \delta' = \delta(L'/K'),\ \delta'_i = \delta_i(L'/K').$$

If M is an S'-module of finite length, write $\ell_p(M)$ for $1/e_{L'}$ times the length of M (so $\ell_p(M)$ also equals the p-adic valuation of the Fitting ideal of M). Consider the homomorphism $\gamma = \beta\alpha$, which links the two exact[3] sequences of differentials in the commutative diagram:

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & S' \otimes_S \Omega_{S/R} \arrow[d, "\alpha"'] \arrow[dr, dashed, "\gamma"] & & \\
0 \arrow[r] & S' \otimes_{R'} \Omega_{R'/R} \arrow[r] & \Omega_{S'/R} \arrow[r, "\beta"'] & \Omega_{S'/R'} \arrow[r] & 0
\end{tikzcd}$$

In this diagram, all entries are torsion S'-modules which can be generated by $\leq (d+1)$ elements. We then have the following inequalities:

(a) $\ell_p(\ker \gamma) \geq \min(\lambda, \delta)$

(b) $\ell_p(\operatorname{im} \gamma) \geq (d+2)\delta' - (d+1)\delta$

[3] See [20, p.420, footnote] or [10, Lemma 1.1]

Since $\ell_p(\operatorname{im}\gamma)+\ell_p(\ker\gamma)=\ell_p(S'\otimes\Omega_{S/R})=\delta$, combining (a) and (b) gives the desired inequality.

Proof of (a):

We have $\alpha\colon \ker\gamma \xrightarrow{\sim} \operatorname{im}\alpha\cap\ker\beta$. Therefore as there is a surjection $\Omega_{R'/R}\to(R'/p^\lambda)^{d+1}$, and as $\Omega_{S'/R}$ can be generated by $(d+1)$ elements, we have

$$\ker\beta\supset\Omega_{S'/R}[p^\lambda]\simeq(S'/p^\lambda)^{d+1}$$

and so

$$\ker\gamma\supset S'\otimes_S\Omega_{S/R}[p^\lambda]\simeq\bigoplus_{i=0}^{d}S'/p^{\min(\lambda,\delta_i)}.$$

Therefore

$$\ell_p(\ker\gamma)\geq\sum\min(\lambda,\delta_i)\geq\min(\lambda,\sum\delta_i)=\min(\lambda,\delta).$$

Proof of (b):

Evidently $\operatorname{im}\gamma=S'd(S)=S'd(R'S)$. Now since under the trace form we have $\mathfrak{D}_{L/K}^{-1}=\operatorname{Hom}_R(S,R)$, it follows that

$$R'\,\mathfrak{D}_{L/K}^{-1}=\operatorname{Hom}_{R'}(R'\otimes S,R')\supset\operatorname{Hom}_{R'}(S',R')=\mathfrak{D}_{L'/K'}^{-1}$$

and so $S'\supset R'S\supset\mathfrak{D}_{L/K}\mathfrak{D}_{L'/K'}^{-1}=\varpi^jS'$ say, where $\varpi=\varpi_{L'}$ is a uniformiser and $j=e_{L'}(\delta-\delta')$. Therefor we have inclusions

$$\operatorname{im}\gamma\supset S'd(\varpi^jS')\supset\varpi^j\Omega_{S'/R'}=p^{\delta-\delta'}\Omega_{S'/R'}\simeq\bigoplus_{i=0}^{d}S'/(p^{\max(0,\delta_i'-\delta+\delta')})$$

and therefore

$$\ell_p(\operatorname{im}\gamma)\geq\sum_{i=0}^{d}(\delta_i'-\delta+\delta')=(d+2)\delta'-(d+1)\delta.$$

□

1.3 Deep ramification and norm fields

In this section we will work with towers $K_0\subset K_1\subset\dots$ of finite extensions of d-big local fields. If $K_\bullet=\{K_n\}$ is such a tower, write $K_\infty=\bigcup K_n$. We abbreviate $\mathfrak{o}_n=\mathfrak{o}_{K_n}$, $\varpi_n=\varpi_{K_n}$ and $k_n=k_{K_n}$. Define an equivalence relation on towers by setting $K_\bullet\sim K_\bullet'$ if there exists $r\in\mathbb{Z}$ such that for every n sufficiently large, $K_n'=K_{n+r}$.

We shall say that a tower $K_\bullet$ is *strictly deeply ramified* if there exists $n_0\geq 0$ and an ideal $\xi\subset\mathfrak{o}_{n_0}$ with $0<v_p(\xi)\leq 1$, such that the following condition holds:

> For every $n\geq n_0$, the extension K_{n+1}/K_n has degree p^{d+1}, and there exists a surjection $\Omega(K_{n+1}/K_n)\twoheadrightarrow(\mathfrak{o}_{n+1}/\xi)^{d+1}$.

(1.3.1)

If $K_\bullet$ is strictly deeply ramified then so is any equivalent tower (with the same ξ and possible different n_0). See 1.3.8 below for some comments on this definition. Let $K_\bullet$ be a strictly deeply ramified tower, and (n_0, ξ) a pair for which (1.3.1) holds. Then by 1.2.1, for every $n \geq n_0$ we have $e(K_{n+1}/K_n) = p$, and Frobenius induces a surjection $f\colon \mathfrak{o}_{n+1}/\xi \longrightarrow\!\!\!\!\!\rightarrow \mathfrak{o}_n/\xi$. We can then choose uniformisers ϖ_n of K_n such that $\varpi_{n+1}^p \equiv \varpi_n \pmod{\xi}$ for every $n \geq n_0$. Define

$$X^+ = X^+(K_\bullet, \xi, n_0) := \varprojlim_{n \geq n_0} (\mathfrak{o}_n/\xi, f)$$

and wite $pr_n\colon X^+ \longrightarrow\!\!\!\!\!\rightarrow \mathfrak{o}_n/\xi$ for the n^{th} projection in the inverse limit. Set $\Pi = (\varpi_n \bmod \xi) \in X^+$.

Let $k' = \varprojlim_{n \geq n_0} (k_n, f)$; since $k_{n+1} = k_n^{1/p}$, the projections $pr_n\colon k' \to k_n$ for any $n \geq n_0$ are isomorphisms. (Note that the residue field k_∞ of K_∞ is then the perfect closure $(k')^{1/p^\infty}$ of k'.)

Theorem 1.3.2. *$X(K_\bullet, \xi, n_0)$ is a complete discrete valuation ring of characteristic p, with uniformiser Π, and residue field k'. Up to canonical isomorphism (described in the proof below) $X^+(K_\bullet, \xi, n_0)$ depends only on the equivalence class of the tower $K_\bullet$, and not on the choices of ξ and n_0 satisfying* (1.3.1).

Proof. Define a partial order on triples $(K_\bullet, \xi, n_0)$ satisfying (1.3.1) by setting $(K'_\bullet, \xi', n'_0) \geq (K_\bullet, \xi, n_0)$ if and only if $v_p(\xi') \leq v_p(\xi)$ and for some $r \geq 0$ one has $n'_0 + r \geq n_0$ and $K'_n = K_{n+r}$ for every $n \geq 0$. It is obvious that under this order any two triples have an upper bound if and only if the associated towers of extensions are equivalent.

If $(K'_\bullet, \xi', n'_0) \geq (K_\bullet, \xi, n_0)$ and r is as above then there is a canonical map

$$\begin{aligned} X^+(K_\bullet, \xi, n_0) &\to X^+(K'_\bullet, \xi', n'_0) \\ g\colon (x_n)_{n \geq n_0} &\mapsto (x_{n+r} \bmod \xi')_{n \geq n'_0}. \end{aligned}$$

If $\xi = \xi'$, g is obviously an isomorphism. In general we can define a map h in the other direction by

$$h\colon (y_n)_{n \geq n'_0} \mapsto (y_{n+s-r}^{p^s})_{n \geq n_0}$$

which is well-defined and independent of s for s sufficiently large. Then g and h are mutual inverses. For three triples $(K''_\bullet, \xi'', n''_0) \geq (K'_\bullet, \xi', n'_0) \geq (K_\bullet, \xi, n_0)$ the isomorphisms just described are obviously transitive, so we obtain the desired independence on choices.

Truncating $K_\bullet$ if necessary we may therefore assume that $n_0 = 0$ and $\xi = \varpi_0$. We then have by 1.2.1

$$X^+/(\Pi^{p^m}) = \varprojlim \mathfrak{o}_n/(\varpi_0, \varpi_n^{p^m}) \xrightarrow[pr_m]{\sim} \mathfrak{o}_m/(\varpi_0).$$

Therefore $\varprojlim X^+/(\Pi^{p^m}) = \varprojlim \mathfrak{o}_m/(\varpi_0) = X^+$, so X^+ is Π-adically complete and separated, and Π is not nilpotent. Since $X^+/(\Pi)$ is a field, X^+ is therefore a discrete valuation ring with uniformiser Π. □

To make the definition of X^+ truly functorial, we define for an equivalence class $\mathcal{K}$ of towers

$$X^+_{\mathcal{K}} := \varinjlim X^+(K_\bullet, \xi, n_0)$$

where the limit is taken over triples $(K_\bullet, \xi, n_0)$ with $K_\bullet \in \mathcal{K}$ and (ξ, n_0) satisfying (1.3.1), and the transition maps are the isomorphisms g in the preceding proof. We let $\Pi_{\mathcal{K}}$ denote any uniformiser of $X^+_{\mathcal{K}}$, and define $k_{\mathcal{K}} = X^+_{\mathcal{K}}/(\Pi_{\mathcal{K}})$ to be its residue field.

Definition. The field of fractions $X_{\mathcal{K}}$ of $X^+_{\mathcal{K}}$ is the *norm field* of $\mathcal{K}$.

Of course this is illogical terminology, because when $d > 0$ this has nothing to do with norms. But when $d = 0$ it is just the field of norms $X_K(K_\infty)$ for the extension K_∞/K in the sense of Fontaine and Wintenberger ([12], [13], and [23] — especially 2.2.3.3), and for $d > 0$ see also remark 1.3.9 below.

Let $K_\bullet$ be a tower of d-big local fields, $\mathcal{K}$ its equivalence class, and L_∞/K_∞ a finite extension. Then there exists a finite extension L_0/K_0 contained in L_∞ such that $L_\infty = K_\infty L_0$; write $L_n = K_n L_0$. The equivalence class $\mathcal{L}$ of $L_\bullet$ depends only on L_∞.

Theorem 1.3.3. *Let $\mathcal{K}$ and $\mathcal{L}$ be as above. Then if $\mathcal{K}$ is strictly deeply ramified so is $\mathcal{L}$.*

Proof. The condition on the extension degrees is clear. By Proposition 1.2.8 with $(K, K', L, L') = (K_n, K_{n+1}, L_n, L_{n+1})$ we have

$$\delta(L_{n+1}/K_{n+1}) \le \delta(L_n/K_n) - \frac{1}{d+2}\min(v_p(\xi), \delta(L_n/K_n))$$

and so $\delta(L_n/K_n) \to 0$ as $n \to \infty$. Using the exact sequences of differentials for the extensions $L_{n+1}/L_n/K_n$ and $L_{n+1}/K_{n+1}/K_n$, it follows that the annihilators of the kernel and cokernel of the canonical map

$$\mathfrak{o}_{L_{n+1}} \otimes_{\mathfrak{o}_{K_{n+1}}} \Omega(K_{n+1}/K_n) \to \Omega(L_{n+1}/L_n)$$

have p-adic valuation tending to zero as $n \to \infty$. Therefore $L_\bullet$ satisfies (1.3.1) for any ξ' with $0 < v_p(\xi') < v_p(\xi)$ (and suitable n_0). □

Theorem 1.3.4. *Let $K_\bullet$ be strictly deeply ramified, $\mathcal{K}$ its equivalence class and L_∞/K_∞ a finite extension.*

(i) $X_{\mathcal{L}}$ is a finite separable extension of $X_{\mathcal{K}}$. More generally, if L'_∞/K_∞ is another finite extension and $\tau\colon L_\infty \to L'_\infty$ is a K_∞-homomorphism, the maps $\tau\colon \mathfrak{o}_{L_n}/\xi \hookrightarrow \mathfrak{o}_{L'_n}/\xi$, for n sufficiently large and $v_p(\xi)$ sufficiently small, induce an injection $X_{\mathcal{K}}(\tau)\colon X^+_{\mathcal{L}} \hookrightarrow X^+_{\mathcal{L}'}$ which makes $X_{\mathcal{L}'}/X_{\mathcal{L}}$ a separable extension of degree $[L'_\infty : \tau L_\infty]$.

(ii) The sequences $(e(L_n/K_n))$, $(s(L_n/K_n))$ and $(f_0(L_n/K_n))$ are stationary for n sufficiently large. Their limits equal $e(X_{\mathcal{L}}/X_{\mathcal{K}})$, $s(X_{\mathcal{L}}/X_{\mathcal{K}})$ and $f_0(X_{\mathcal{L}}/X_{\mathcal{K}})$ respectively.

(iii) There exists a constant $c \geq 0$ such that $\delta(L_n/K_n) = cp^{-n}$ for n sufficiently large.

Proof. It suffices in (i) to consider the case of a single extension L_∞/K_∞. Let $m = [L_\infty : K_\infty]$. Changing ξ and n_0 if necessary, we can assume that (1.3.1) holds for both $K_\bullet$ and $L_\bullet$ with the same ξ and n_0, and that $[L_n : K_n] = [L_\infty : K_\infty] = m$ for $n \geq n_0$. Then for every $n \geq n_0$, $\mathfrak{o}_{L_n}/\xi$ is a finite flat $\mathfrak{o}_n/\xi$-algebra of rank m. Therefore by Nakayama's lemma $X^+_{\mathcal{L}}$ is a finite flat $X^+_{\mathcal{K}}$-algebra of rank m, so $X_{\mathcal{L}}/X_{\mathcal{K}}$ is a finite extension of degree m.
Consider the discriminant $\mathfrak{d} = \mathfrak{d}_{X_{\mathcal{L}}/X_{\mathcal{K}}} \subset X^+_{\mathcal{K}}$ of $X^+_{\mathcal{L}}/X^+_{\mathcal{K}}$. The projection of $\mathfrak{d}$ to $\mathfrak{o}_n/\xi$ equals the discriminant of $\mathfrak{o}_{L_n}/\xi$ over $\mathfrak{o}_n/\xi$. Since $\delta(L_n/K_n) \to 0$ the latter is nonzero for n sufficiently large. So $X_{\mathcal{L}}/X_{\mathcal{K}}$ is separable. Its residue field extension is isomorphic to k_{L_n}/k_n for n sufficiently large. So the sequences $(f_0(L_n/K_n))$ and $(s(L_n/K_n))$ are ultimately stationary, hence the same holds for $e(L_n/K_n) = [L_n : K_n]/f(L_n/K_n)$.
Let $v_{X_{\mathcal{K}}}(\mathfrak{d}) = r$; then for $n \geq n_0$, (ϖ_n^r) equals the discriminant of $\mathfrak{o}_{L_n}/\xi$ over $\mathfrak{o}_n/\xi$. So for n sufficiently large, $v_p(\varpi_n^r) = m\delta(L_n/K_n)$. Therefore $\delta(L_n/K_n) = p^{-n}c$ where c equals rp^n/me_{K_n}, which is constant for n sufficiently large. □

So if $\mathcal{K}$ is strictly deeply ramified, for any finite L_∞/K_∞ we may define

$$X^+_{\mathcal{K}}(L_\infty) := X^+_{\mathcal{L}}, \quad X_{\mathcal{K}}(L_\infty) := X_{\mathcal{L}}$$

which by the above is a functor from the category of finite extensions of K_∞ to that of $X_{\mathcal{K}}$.

Theorem 1.3.5. *The functor $X_{\mathcal{K}}(-)$ defines an equivalence between the category of finite extensions of K_∞ and the category of finite separable extensions of $X_{\mathcal{K}}$.*

Proof.
The functor is fully faithful. It is enough to show that if L_∞/K_∞ is a finite Galois extension then any non-trivial $\sigma \in \mathrm{Gal}(L_\infty/K_\infty)$ induces a non-trivial automorphism $X_{\mathcal{K}}(\sigma)$ of $X_{\mathcal{K}}(L_\infty) = X_{\mathcal{L}}$. In that case since $[X_{\mathcal{L}} : X_{\mathcal{K}}] = [L_\infty : K_\infty]$ it follows that $X_{\mathcal{L}}/X_{\mathcal{K}}$ is a Galois extension, and that $X_{\mathcal{K}}(-)\colon \mathrm{Gal}(L_\infty/K_\infty) \xrightarrow{\sim} \mathrm{Gal}(X_{\mathcal{L}}/X_{\mathcal{K}})$, from which the fully faithfulness is formal by Galois theory.
Assume that $X_{\mathcal{K}}(\sigma) = 1$. Then replacing σ by a suitable power, we may assume it has prime order. Replacing K_∞ by the fixed field of σ, and truncating the tower if necessary we may then assume that L_∞/K_∞ is cyclic of prime degree ℓ, with Galois group G say.
In this case for n sufficiently large, L_n/K_n is cyclic of degree ℓ and so $\mathfrak{o}_{L_n} = \mathfrak{o}_{K_n}[x_n]$ for some $x_n \in \mathfrak{o}_{L_n}$. If $g_n \in \mathfrak{o}_{K_n}[T]$ is the minimal polynomial of x_n

then

$$\mathfrak{D}_{L_n/K_n} = (g_n'(x_n)) = \prod_{1\neq\sigma\in G}(x_n - \sigma x_n).$$

So since $\delta(L_n/K_n) \to 0$, it follows that if $1 \neq \sigma \in G$ and n is sufficiently large, then $\sigma x_n \not\equiv x_n \pmod{\xi}$. So σ acts nontrivially on $\mathfrak{o}_{L_n}/\xi$ hence also on $X_{\mathcal{L}}$.
The functor is essentially surjective.
Using fully faithfulness, it is enough to show that if $Y/X_{\mathcal{K}}$ is a finite Galois extension then there exists L_∞/K_∞ and a $X_{\mathcal{K}}$-isomorphism $X_{\mathcal{K}}(L_\infty) \xrightarrow{\sim} Y$. Let $Y^+ \subset Y$ be the valuation ring of Y. Building the extension step-by-step we are reduced to the cases:
(a) $Y/X_{\mathcal{K}}$ is unramified. The categories of finite unramified extensions of $X_{\mathcal{K}}$ and K_∞ are equivalent to the categories of finite separable extensions of their respective residue fields $k_{\mathcal{K}}$ and k_∞. But as k_∞ is the perfect closure of $k_{\mathcal{K}}$ these categories are equivalent.
(b) $Y/X_{\mathcal{K}}$ is ramified and of prime degree ℓ. There are two subcases:
(b1) $e(Y/X_{\mathcal{K}}) = \ell$. Then $Y^+ = X^+_{\mathcal{K}}[\Pi_Y]$ where the uniformiser Π_Y satisfies an Eisenstein polynomial $G(T) \in X^+_{\mathcal{K}}[T]$.
Choose n_0 such that (1.3.1) holds and $v_p(\xi) > v_p(\varpi_{n_0})$. For every $n \geq n_0$, let $g_n \in \mathfrak{o}_n[T]$ be any monic polynomial such that $\bar{g}_n = pr_n(G) \in (\mathfrak{o}_n/\xi)[T]$. Then g_n is an Eisenstein polynomial, and $g_n(T^p) \equiv g_{n+1}(T)^p \pmod{\xi}$. Fix an algebraic closure $\overline{K}$ of K_∞ and let $\bar{\mathfrak{o}}$ be its valuation ring.

Claim: There exist $n_1 \geq n_0$, $\xi' \in \mathfrak{o}_{n_1}$ with $v_p(\xi') \leq v_p(\xi)$, and roots $x_n \in \bar{\mathfrak{o}}$ of g_n, such

(i) For every $n \geq n_1$, $x_{n+1}^p \equiv x_n \pmod{\xi'}$

(ii) If $L_n := K_n(x_n) \subset \overline{K}$ then $L_{n+1} = K_{n+1}L_n$ for all $n \geq n_1$.

(iii) If $n \geq n_1$ then $(\mathfrak{o}_{L_{n+1}}/\xi')^p = \mathfrak{o}_{L_n}/\xi'$, and there is an isomorphism of $X^+_{\mathcal{K}}$-algebras

$$Y^+ \xrightarrow{\sim} \varprojlim_{n\geq n_1}\left(\mathfrak{o}_{L_n}/\xi', f\right)$$

mapping Π_Y to $(x_n \bmod \xi')_n$.

Granted this claim, $L_\infty := \bigcup L_n$ is an extension with $X_{\mathcal{K}}(L_\infty) \simeq Y$.

Proof of claim. (i) Let $S_n = \{x_{n,i} \mid 1 \leq i \leq \ell\} \subset \bar{\mathfrak{o}}$ be the set of roots of g_n. Then for all $n \geq 0$ and all i we have

$$\prod_{j=1}^{\ell}(x_{n+1,i}^p - x_{n,j}) = g_n(x_{n+1,i}^p) \equiv g_{n+1}(x_{n+1,i})^p \equiv 0 \pmod{\xi}.$$

Choose $n_1 \geq n_0$ and $\xi' \subset \mathfrak{o}_{n_1}$ such that $0 < v_p(\xi') \leq \ell^{-1}v_p(\xi)$. Then for each i there exists j with $x_{n+1,i}^p \equiv x_{n,j} \pmod{\xi'}$. Choosing such a j for each i then determines a map $S_{n+1} \to S_n$, and by compactness $\varprojlim S_n$ is nonempty. Let (x_n) be any element of the inverse limit; then (i) is satisfied.

If $L_n = K_n(x_n)$, then $[L_n : K_n] = e(L_n/K_n) = \ell$. Since it satisfies an Eisenstein polynomial, x_n is a uniformiser of L_n, and $\mathfrak{o}_{L_n}/\xi' = (\mathfrak{o}_n/\xi')[x_n] = (\mathfrak{o}_n/\xi')[T]/\bar{g}_n(T)$. Therefore for each n there is a unique surjection

$$f \colon \mathfrak{o}_{L_{n+1}}/\xi' \twoheadrightarrow \mathfrak{o}_{L_n}/\xi' \tag{1.3.6}$$

which is Frobenius on $\mathfrak{o}_{n+1}/\xi$ and maps x_{n+1} to x_n (mod ξ').

Let $\mu_n \colon Y^+ \twoheadrightarrow \mathfrak{o}_{L_n}/\xi'$ be the map taking Π_Y to x_n, and whose restriction to $X_{\mathcal{K}}^+$ is pr_n. The different of $Y/X_{\mathcal{K}}$ is $(G'(\Pi_Y))$, and it is nonzero since $Y/X_{\mathcal{K}}$ is separable. Let $r = v_Y(G'(\Pi_Y))$. Then $\bar{g}_n'(x_n) = \mu_n(G'(\Pi_Y))$ equals x_n^r times a unit. Therefore if n is large enough so that $v_{L_n}(\xi) > r$, we have $v_{L_n}(g_n'(x_n)) = r$. Therefore $\delta(L_n/K_n) = v_p(g_n'(x_n)) \to 0$. Order the roots of g_n so that $x_n = x_{n,1}$. Since

$$\prod_{i \neq 1}(x_{n+1}^p - x_{n,i}) \equiv \prod_{i \neq 1}(x_n - x_{n,i}) \equiv g_n'(x_n) \pmod{\xi}'$$

it follows that for n sufficiently large, x_{n+1}^p is closer to x_n than to any of the other roots $\{x_{n,i} \mid i \neq 1\}$ of g_n. By Krasner's lemma, $x_n \in K_n(x_{n+1}^p)$, so $L_n \subset L_{n+1}$ and the map (1.3.6) is induced by the Frobenius endomorphism of $\mathfrak{o}_{L_{n+1}}/\xi'$ (by its uniqueness).

We have to check that $L_{n+1} = K_{n+1}L_n$ for n sufficiently large. Since $[L_{n+1} : K_{n+1}] = \ell = [L_n : K_n]$ it is enough to show that the extensions L_n/K_n and K_{n+1}/K_n are linearly disjoint. If not, since $[L_n : K_n]$ is prime, there exists a K_n-homomorphism $\tau \colon L_n \to K_{n+1}$, and so $\ell = p$. But as $\delta(L_n/K_n) \to 0$ and $\Omega(K_{n+1}/K_n)$ surjects onto $(\mathfrak{o}_{n+1}/\xi)^{d+1}$ this implies that for n sufficiently large, $\Omega(K_{n+1}/\tau L_n)$ surjects onto k_{n+1}^{d+1}, which is impossible as $[K_{n+1} : \tau L_n] = p^d$.

Finally, making n_1 sufficiently large, we have a commutative diagram

$$\begin{tikzcd}
X_{\mathcal{K}}^+ \arrow[r, hook] \arrow[d, two heads, "pr_{n+1}"] & Y^+ \arrow[d, two heads, "\mu_{n+1}"'] \arrow[ddr, two heads, "\mu_n"] & \\
\mathfrak{o}_{n+1}/\xi' \arrow[r, hook] \arrow[dr, two heads, "f"'] & \mathfrak{o}_{L_{n+1}}/\xi' \arrow[dr, two heads, "f"'] & \\
& \mathfrak{o}_n/\xi' \arrow[r, hook] & \mathfrak{o}_{L_n}/\xi'
\end{tikzcd} \tag{1.3.7}$$

where $L_{n+1} = K_{n+1}L_n$ for $n \geq n_1$, inducing a $X_{\mathcal{K}}^+$-homorphism

$$Y^+ \to X_{\mathcal{K}}^+(L_\infty) = \varprojlim_{n \geq n_1} (\mathfrak{o}_{L_n}/\xi', f).$$

Since Y^+ and $X_{\mathcal{K}}^+(L_\infty)$ are both valuation rings of extensions of $X_{\mathcal{K}}$ of the same degree, this is an isomorphism. □

(b2) $e=1$ and $s=1$. Then $Y^+=X^+_{\mathcal{K}}[U]$ for some $U\in(Y^+)^*$, whose reduction mod $\Pi_{\mathcal{K}}$ generates $k_Y/k_{\mathcal{K}}$. As in (b1), let G be the minimal polynomial of U, and get $\bar g_n\in(\mathfrak{o}_n/\xi)[T]$ be its image, and $g_n\in\mathfrak{o}_n[T]$ any monic lift. Then g_n is a fake Eisenstein polynomial (cf. §1.1) hence is irreducible; just as above we find roots $u_n\in\bar{\mathfrak{o}}$ of g_n such that $u^p_{n+1}\equiv u_n \pmod{\xi'}$ for n sufficiently large and suitable ξ'. The remainder of the argument proceeds exactly as for (b1). □

Remark 1.3.8. The condition 1.3.1 is closely related, in the case $d=0$, to that of strictly arithmetically profinite extension [23, §1.2.1]. It is possible to weaken the condition without affecting the results: one could instead just require that there exist surjections $\Omega(K_{n+1}/K_n)\twoheadrightarrow(\mathfrak{o}_{n+1}/\xi_{n+1})^{d+1}$ where $\xi_n\subset\mathfrak{o}_n$ is a sequence of ideals whose p-adic valuations do not tend too rapidly to zero.

Remark 1.3.9. Suppose that K (and therefore also $X_{\mathcal{K}}$) is a $(d+1)$-dimensional local field. Then, as Fesenko and Zerbes have remarked to the author, local class field theory for higher dimensional local fields [17] gives a reciprocity homomorphism $K^M_{d+1}(K)\to\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, where $K^M_*()$ is Milnor K-theory, which becomes an isomorphism after passing to a suitable completion $\widehat{K^M_{d+1}(K)}$. Therefore there is a commutative diagram

$$\begin{tikzcd}
\varprojlim_{\text{norms}} \widehat{K^M_{d+1}(K_n)} \arrow[rr, "\sim"] \arrow[d, equal] & & \widehat{K^M_{d+1}(X_{\mathcal{K}})} \arrow[d, equal] \\
\varprojlim \mathrm{Gal}(\overline{K}/K_n)^{\mathrm{ab}} = \mathrm{Gal}(\overline{K}/K_\infty)^{\mathrm{ab}} \arrow[rr, "\sim"] & & \mathrm{Gal}(\overline{X_{\mathcal{K}}}/X_{\mathcal{K}})^{\mathrm{ab}}
\end{tikzcd}$$

which may be viewed as the generalisation of the Fontaine-Wintenberger definition (for $d=0$) of $X_{\mathcal{K}}$ as the inverse limit of the K_n with respect to the norm maps.

2 (ϕ,Γ)-modules

2.1 Definitions

We review Fontaine's definition [11] of the (ϕ,Γ)-module associated to a p-adic representation, in an appropriately axiomatic setting. The key assumptions making the theory possible are (2.1.1) and (2.1.2) below.

We begin with a strictly deeply ramified tower $K_\bullet$ of d-big local fields (always of characteristic zero) such that K_n/K_0 is Galois for each n, and set $K=K_0$, $\Gamma_K=\mathrm{Gal}(K_\infty/K)$. Fixing an algebraic closure $\overline{K}$ of K containing K_∞, write $\mathcal{G}_K=\mathrm{Gal}(\overline{K}/K)\supset\mathcal{H}_K=\mathrm{Gal}(\overline{K}/K_\infty)$. All algebraic extensions of K will be tacitly assumed to be subfields of $\overline{K}$.

Let $\mathbf{E}_K=X_{\mathcal{K}}$ be the norm field of the tower $K_\bullet$, and $\mathbf{E}^+_K$ its valuation ring. To be consistent with the notation established in [8], we write $\bar\pi$, or when there is no confusion simply π, for a uniformiser of $\mathbf{E}_K$. Then $\mathbf{E}^+_K$ is (noncanonically) isomorphic to $k_{\mathcal{K}}[[\bar{\pi}]]$. For a finite extension L/K, one writes $\mathbf{E}_L$ for the norm field of the tower $LK_\bullet$, and $\mathbf{E}$ for $\varinjlim \mathbf{E}_L$ (the limit over all finite extensions L/K). The group $\mathcal{G}_K$ then acts continuously (for the valuation topology) on $\mathbf{E} = \mathbf{E}_K^{\mathrm{sep}}$, and this action identifies the subgroup $\mathcal{H}_K$ with $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K)$.

If E is any of these rings of characteristic p, write E^{rad} for the perfect closure $\sqrt[p^\infty]{E}$ of E, and $\widetilde{\mathbf{E}}$ for the completion of E^{rad}. In particular, $\widetilde{\mathbf{E}}^+$ is the valuation ring of the algebraic closure of $\mathbf{E}_K$, and can be alternatively described as $\varprojlim(\mathfrak{o}_{\overline{K}}/p, f)$, also known as $\mathcal{R}$. By continuity the action of $\mathcal{G}_K$ on $\mathbf{E}$ extends uniquely to a continuous action on $\mathbf{E}^{\mathrm{rad}}$ and $\widetilde{\mathbf{E}}$, and for any L on has $\widetilde{\mathbf{E}}_L = \widetilde{\mathbf{E}}^{\mathcal{H}_L}$.

In the theory of (ϕ, Γ)-modules there are two kinds of rings of characteristic zero which appear. The first are those with perfect residue ring, which are completely canonical. These are:

- $\widetilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+) \subset \widetilde{\mathbf{A}} = W(\widetilde{\mathbf{E}})$;
- $\widetilde{\mathbf{A}}_L = W(\widetilde{\mathbf{E}}_L)$, for any finite L/K;
- $\widetilde{\mathbf{A}}_L^+ = W(\widetilde{\mathbf{E}}_L^+) = \widetilde{\mathbf{A}}^+ \cap \widetilde{\mathbf{A}}_L$

They carry a unique lifting of Frobenius (namely the Witt vector endomorphism F), and the action of $\mathcal{G}_K$ on $\widetilde{\mathbf{E}}$ defines an action on $\widetilde{\mathbf{A}}$. The ring $\widetilde{\mathbf{A}}$ has a canonical topology (also called the weak topology) which is the weakest structure of topological ring for which $\widetilde{\mathbf{A}} \to \widetilde{\mathbf{E}}$ is continuous (for the valuation topology on $\widetilde{\mathbf{E}}$). Equivalently, in terms of the definition of $W(\widetilde{\mathbf{E}})$ as $\widetilde{\mathbf{E}}^{\mathbb{N}}$ with Witt vector multiplication and addition, it is the product of the valuation topologies on the factors. The $\mathcal{G}_K$-action is evidently continuous with respect to the canonical topology. The other natural topology to put on $\widetilde{\mathbf{A}}$ is the p-adic (or strong) topology.

The other rings of characteristic zero have imperfect residue rings, and depend on certain choices. Let $\mathbf{A}_K^+$ be a complete regular local ring of dimension 2, together with an isomorphism $\mathbf{A}_K^+/(p) \simeq \mathbf{E}_K^+$. Such a lift of $\mathbf{E}_K^+$ exists and is unique up to nonunique isomorphism. If C is a p-Cohen ring with residue field k, then any $\mathbf{A}_K^+$ is (non-canonically) isomorphic to $C[[\pi]]$. Define $\mathbf{A}_K$ to be the p-adic completion of $(\mathbf{A}_K^+)_{(p)}$; it is a p-Cohen ring with residue field $\mathbf{E}_K$.

Fix a principal ideal $I = (\pi)$ of $\mathbf{A}_K^+$ lifting $(\bar{\pi}) \subset \mathbf{E}_K^+$. Then $\mathbf{A}_K$ is the p-adic completion of $\mathbf{A}_K^+[1/\pi]$. The essential choice to be made is a lifting $\phi \colon \mathbf{A}_K^+ \to \mathbf{A}_K^+$ of the absolute Frobenius endomorphism of $\mathbf{E}_K^+$, which is required to satisfy two conditions. The first is simply

$$\phi(I) \subset I. \tag{2.1.1}$$

It is clear that ϕ extends to an endomorphism of $\mathbf{A}_K$, whose reduction mod p is the absolute Frobenius of $\mathbf{E}_K$.

For any finite extension L/K there exists a finite étale extension $\mathbf{A}_L/\mathbf{A}_K$, unique up to unique isomorphism, with residue field $\mathbf{E}_L$. Let $\mathbf{A}_{\overline{K}} = \varinjlim \mathbf{A}_L$, the direct limit taken over finite extensions L/K, and let $\mathbf{A}$ be the p-adic completion of $\mathbf{A}_{\overline{K}}$. Then $\mathbf{A}_{\overline{K}}$ is the maximal unramified extension of $\mathbf{A}_K$, and the isomorphism $\mathcal{H}_K \simeq \mathrm{Gal}(\mathbf{E}/\mathbf{E}_K)$ extends to an isomorphism with $\mathrm{Aut}(\mathbf{A}_{\overline{K}}/\mathbf{A}_K)$. This in turn extends to a unique action of $\mathcal{H}_K$ on $\mathbf{A}$, continuous for both the canonical and p-adic topologies, and for any finite L/K one has $\mathbf{A}^{\mathcal{H}_L} = \mathbf{A}_L$ by the Ax-Sen-Tate theorem [6].

Since $\mathbf{A}_L/\mathbf{A}_K$ is étale there is a unique extension of ϕ to an endomorphism of $\mathbf{A}_L$ whose reduction mod p is Frobenius; by passage to the limit and completion it extends to an endomorphism of $\mathbf{A}$. We use ϕ to denote any of these endomorphisms.

The lifting ϕ of Frobenius determines (see [7, Ch,IX, §1, ex.14] and [11, 1.3.2]) a unique embedding

$$\mu_K \colon \mathbf{A}_K \hookrightarrow W(\mathbf{E}_K)$$

such that $\mu\circ\phi = F\circ\mu$, which maps $\mathbf{A}_K^+$ into $W(\mathbf{E}_K^+)$. We identify $\mathbf{A}_K$ with its image under this map. An alternative description of μ_K is as follows: consider the direct limit

$$\phi^{-\infty}\mathbf{A}_K = \varinjlim(\mathbf{A}_K, \phi)$$

on which ϕ is an automorphism. Its p-adic completion is a complete unramified DVR of characteristic zero, with perfect residue field $\mathbf{E}_K^{\mathrm{rad}}$, hence is canonically isomorphic to $W(\mathbf{E}_k^{\mathrm{rad}})$. Likewise the action of ϕ on $\mathbf{A}$ determines an embedding $\mu\colon \mathbf{A} \hookrightarrow W(\mathbf{E})$, which is uniquely characterised by the same properties as μ_K. The embeddings $\mathbf{A}_K \hookrightarrow \mathbf{A} \hookrightarrow W(\widetilde{\mathbf{E}})$ induce topologies on $\mathbf{A}_K$ and $\mathbf{A}$. One writes $\mathbf{A}^+ = \mathbf{A} \cap \widetilde{\mathbf{A}}^+$. Then $\mathbf{A}^+/p\mathbf{A}^+ \simeq \mathbf{E}^+$ by [11, 1.8.3], and a basis of neighbourhoods of 0 for the canonical topology on $\mathbf{A}$ is the collection of $\mathbf{A}^+$-submodules

$$p^m\mathbf{A} + \pi^n\mathbf{A}^+, \quad m, n \geq 0.$$

The reduction map $\mathbf{A} \to \mathbf{E}$ is $\mathcal{H}_K$-equivariant by construction, and so μ is $\mathcal{H}_K$-equivariant. The second, and much more serious, condition to be satisfied by ϕ is:

$$\mathbf{A} \subset \widetilde{\mathbf{A}} \text{ is stable under the action of } \mathcal{G}_K. \tag{2.1.2}$$

In particular, $\mathbf{A}$ inherits an action of $\mathcal{G}_K$, and $\mathbf{A}_K$ and $\mathbf{A}_K^+$ inherit an action of Γ_K, continuous for the canonical topology.

A $\mathbb{Z}_p$-representation of $\mathcal{G}_K$ is by definition a $\mathbb{Z}_p$-module of finite type with a continuous action of $\mathcal{G}_K$. Assuming (2.1.1) and (2.1.2) above are satisfied, Fontaine's theory associates to a $\mathbb{Z}_p$-representation of $\mathcal{G}_K$ the $\mathbf{A}_K$-module of finite type

$$\mathbf{D}(V) = \mathbf{D}_K(V) := (\mathbf{A} \otimes_{\mathbb{Z}_p} V)^{\mathcal{H}_K}.$$

The functor $\mathbf{D}$ is faithful and exact. The $\mathbf{A}_K$-module $\mathbf{D}(V)$ has commuting semilinear actions of ϕ and Γ_K. Being a finitely-generated $\mathbf{A}_K$-module, $\mathbf{D}(V)$ has a natural topology (which is the quotient topology for any surjection $\mathbf{A}_K^d \to \mathbf{D}(V)$), for which the action of Γ_K is continuous. Therefore $\mathbf{D}(V)$ has the structure of an étale (ϕ, Γ_K)-module, and just as in [11] we have:

Theorem 2.1.3. *Assume conditions* (2.1.1) *and* (2.1.2) *are satisfied. The functor* $\mathbf{D}$ *is an equivalence of categories*

$$(\mathbb{Z}_p\textit{-representations of } \mathcal{G}_K) \longrightarrow (\textit{étale } (\phi, \Gamma_K)\textit{-modules over } \mathbf{A}_K)$$

and an essential inverse is given by $D \mapsto (\mathbf{A} \otimes_{\mathbf{A}_K} D)^{\phi=1}$.

Lemma 2.1.4. *(i) The sequences*

$$0 \to \mathbb{Z}_p \to \mathbf{A} \xrightarrow{\phi-1} \mathbf{A} \to 0 \tag{2.1.5}$$

$$0 \to \mathbb{Z}_p \to \mathbf{A}^+ \xrightarrow{\phi-1} \mathbf{A}^+ \to 0 \tag{2.1.6}$$

are exact, and for every $n > 0$, *the map*

$$\phi - 1 \colon \pi^n \mathbf{A}^+ \to \pi^n \mathbf{A}^+ \tag{2.1.7}$$

is an isomorphism.
(ii) For any $n > 0$ *and for any* L/K, *the map* $\phi - 1 \colon \mathbf{E}_L^+ \to \mathbf{E}_L^+$ *is an isomorphism.*

Proof. It suffices (by passage to the limit) to prove the corresponding statements mod p^m. By dévissage it is enough to check them mod p. Therefore (2.1.5), (2.1.6) follow from the Artin–Schreier sequences for $\mathbf{E}$ and $\mathbf{E}^+$, and (2.1.7) follows from (ii), since $\mathbf{A}^+/p\mathbf{A}^+ = \mathbf{E}^+$. Rewriting the map as $\pi^{n(p-1)}\phi - 1 \colon \mathbf{E}_L^+ \to \mathbf{E}_L^+$, by Hensel's lemma it is an isomorphism. □

2.2 Cohomology

We assume that we are in the situation of the previous subsection. In particular, we assume that conditions (2.1.1) and (2.1.2) are satisfied. If G is a profinite group and M a topological abelian group with a continuous G-action, by $H^*(G, M)$ we shall always mean continuous group cohomology. Write $\mathcal{C}^\bullet(G, M)$ for the continuous cochain complex of G with coefficients in M, so that $H^*(G, M) = H^*(\mathcal{C}^\bullet(G, M))$. If $\phi \in \mathrm{End}_G(M)$ write $\mathcal{C}^\bullet_\phi(G, M)$ for the simple complex associated to the double complex $[\mathcal{C}^\bullet(G, M) \xrightarrow{\phi-1} \mathcal{C}^\bullet(G, M)]$. Write $H^*_\phi(G, M)$ for the cohomology of $\mathcal{C}^\bullet_\phi(G, M)$, and $H^*_\phi(M)$ for the cohomology of the complex $M \xrightarrow{\phi-1} M$ (in degrees 0 and 1).
If $H \subset G$ is a closed normal subgroup and M is discrete then there are two Hochschild–Serre spectral sequences converging to $H^*_\phi(G, M)$, whose E_2-terms are respectively

$$H^a(G/H, H^b_\phi(H, M)) \quad \text{and} \quad H^a_\phi(G/H, H^b(H, M)),$$

and which reduce when $H = \{1\}$ and $H = G$ respectively to the long exact sequence

$$H^a(G, M^{\phi=1}) \to H^a_\phi(G, M) \to H^{a-1}(G, M/(\phi-1)) \to H^{a+1}(G, M^{\phi=1})$$

and the short exact sequences

$$0 \to H^{b-1}(G,M)/(\phi-1) \to H^b_\phi(G,M) \to H^b(G,M)^{\phi=1} \to 0.$$

Theorem 2.2.1. *Let V be a $\mathbb{Z}_p$-representation of $\mathcal{G}_K$, and set $D = \mathbf{D}_K(V)$. There are isomorphisms*

$$H^*(\mathcal{G}_K, V) \xrightarrow{\sim} H^*_\phi(\Gamma_K, D) \tag{2.2.2}$$

$$H^*(\mathcal{H}_K, V) \xrightarrow{\sim} H^*_\phi(D) \tag{2.2.3}$$

which are functorial in V, and compatible with restriction and corestriction.

Remarks. (i) In the case when K has perfect residue field, and K_∞ is the cyclotomic $\mathbb{Z}_p$-extension, we recover Théorème 2.1 of [15], since taking γ to be a topological generator of $\Gamma_K \simeq \mathbb{Z}_p$, the complex

$$D \xrightarrow{\binom{\phi-1}{\gamma-1}} D \oplus D \xrightarrow{(\gamma-1, 1-\phi)} D$$

computes $H^*_\phi(\Gamma_K, D)$.

(ii) An oversimplified version of the proof runs as follows: from the short exact sequence (2.1.5) we have, tensoring with V and applying the functor $R\Gamma(\mathcal{H}_K, -)$, an isomorphism (in an unspecified derived category)

$$R\Gamma(\mathcal{H}_K, V) \xrightarrow{\sim} R\Gamma(\mathcal{H}_K, \mathbf{A} \otimes V \xrightarrow{\phi-1} \mathbf{A} \otimes V). \tag{2.2.4}$$

But for $i > 0$, $H^i(\mathcal{H}_K, \mathbf{A} \otimes V) = 0$, and $H^0(\mathcal{H}_K, \mathbf{A} \otimes V) = D$, so the right-hand side of (2.2.4) is isomorphic to $[D \xrightarrow{\phi-1} D]$. Applying $R\Gamma(\Gamma_K, -)$ then would give

$$R\Gamma(\mathcal{G}_K, V) \xrightarrow{\sim} R\Gamma(\Gamma_K, D \xrightarrow{\phi-1} D).$$

Since the formalism of derived categories in continuous cohomology requires extra hypotheses (see for example [16] or [19, Ch.4]) which do not hold in the present situation, we fill in this skeleton by explicit reduction to discrete modules. (Note that in general these Galois cohomology groups will not be of finite type over $\mathbb{Z}_p$, hence need not commute with inverse limits.)

Proof. We construct a functorial isomorphism (2.2.2); once one knows that it is compatible with restriction, one may obtain (2.2.3) by passage to the limit over finite extensions L/K; alternatively it can be proved directly (and more simply) by the same method as (2.2.2). The compatibility of the constructed isomorphisms with restriction and corestriction is an elementary verification which we leave to the interested reader.

Write $V_m = V/p^m V$ and $D_m = D/p^m D$; we have $D_m = \mathbf{D}_K(V_m)$ since $\mathbf{D}_K$ is exact. A basis of neighbourhoods of 0 in D_m is given by the open subgroups

$$D_m \cap (\pi^n \mathbf{A}^+ \otimes V_m) = (\pi^n \mathbf{A}^+ \otimes V_m)^{\mathcal{H}_K}$$

which are stable under Γ_K and ϕ. Write also

$$D_{m,n}=D_m/(\pi^n\mathbf{A}^+\otimes V_m)^{\mathcal{H}_K}$$

which is a discrete Γ_K-module; we have topological isomorphisms

$$D_m=\varprojlim_n(D_{m,n}),\quad D=\varprojlim_m(D_m)$$

and $H^*_\phi(\Gamma_K,D)$ is the cohomology of $\varprojlim_{m,n}\mathcal{C}^\bullet_\phi(\Gamma_K,D_{m,n})$.

From 2.1.4 we obtain for every $m,n\geq 1$ a short exact sequence

$$0\to V_m\to(\mathbf{A}/\pi^n\mathbf{A}^+)\otimes V_m\xrightarrow{\phi-1}(\mathbf{A}/\pi^n\mathbf{A}^+)\otimes V_m\to 0$$

and so the canonical map

$$\mathcal{C}^\bullet(\mathcal{G}_K,V_m)\to\mathcal{C}^\bullet_\phi(\mathcal{G}_K,(\mathbf{A}/\pi^n\mathbf{A}^+)\otimes V_m)\tag{2.2.5}$$

is a quasi-isomorphism, for every $m,n\geq 1$.

The inclusion $D_{m,n}\hookrightarrow(\mathbf{A}/\pi^n\mathbf{A}^+)\otimes V_m$ induces a morphism of complexes

$$\alpha_{m,n}\colon\mathcal{C}^\bullet_\phi(\Gamma_K,D_{m,n})\to\mathcal{C}^\bullet_\phi(\mathcal{G}_K,(\mathbf{A}/\pi^n\mathbf{A}^+)\otimes V_m).$$

Passing to the inverse limit and taking cohomology, this together with (2.2.5) defines a functorial map

$$H^*_\phi(\Gamma_K,D)\to H^*(\mathcal{G}_K,V)\tag{2.2.6}$$

whose inverse will be (2.2.2). To prove it is an isomorphism, it is enough to show:

Proposition 2.2.7. *For every $m\geq 1$, $\varprojlim_n(\alpha_{m,n})$ is a quasi-isomorphism.*

Proof. First note that the exactness of $\mathbf{D}$ implies that there is a short exact sequence

$$0\to D_m\to D_{m+1}\to D_1\to 0$$

which clearly has a continuous set-theoretical splitting (it is enough to give a continuous section of the surjection $\mathbf{A}_K\to\mathbf{E}_K$ which is easy), so gives rise to a long exact sequence of continuous cohomology. Suppose the result is shown for $m=1$. Then (2.2.6) is an isomorphism for every V with $pV=0$, and so by the 5-lemma it is an isomorphism for every V of finite length, whence the result holds for all $m\geq 1$. So we may assume for the rest of the proof that $pV=0$ and $m=1$, and therefore replace $\mathbf{A}$ by $\mathbf{E}$.

Fix a finite Galois extension L/K such that $\mathcal{H}_L$ acts trivially on V. We then have a natural map

$$D_{1,n}=\frac{(\mathbf{E}\otimes V)^{\mathcal{H}_K}}{(\pi^n\mathbf{E}^+\otimes V)^{\mathcal{H}_K}}\to\frac{(\mathbf{E}\otimes V)^{\mathcal{H}_L}}{(\pi^n\mathbf{E}^+\otimes V)^{\mathcal{H}_L}}=\mathbf{E}_L/\pi^n\mathbf{E}^+_L\otimes V.$$

The map $\alpha_{1,n}$ therefore factors as the composite of two maps

$$\begin{aligned}\mathcal{C}^\bullet_\phi(\Gamma_K, D_{1,n}) &\xrightarrow{\beta_n} \mathcal{C}^\bullet_\phi(\mathrm{Gal}(L_\infty/K), \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V)\\ &\xrightarrow{\gamma_n} \mathcal{C}^\bullet_\phi(\mathcal{G}_K, \mathbf{E}/\pi^n\mathbf{E}^+ \otimes V)\end{aligned}$$

which we treat in turn:

(a) γ_n *is a quasi-isomorphism.* We may compute the induced map $H^*(\gamma_n)$ on cohomology using the morphism of associated spectral sequences, which on E_2-terms is the map

$$\begin{aligned}&H^a(\mathrm{Gal}(L_\infty/K), H^b_\phi(\mathbf{E}_L/\pi^n\mathbf{E}_L^+)\otimes V)\\ &\qquad\to H^a(\mathrm{Gal}(L_\infty/K), H^b_\phi(\mathcal{H}_L, \mathbf{E}_L/\pi^n\mathbf{E}_L^+)\otimes V) \qquad (2.2.8)\end{aligned}$$

We then have a commutative square (where $\mathbf{E}$ is regarded as a discrete $\mathcal{H}_L$-module)

$$\begin{tikzcd} H^b_\phi(\mathbf{E}_L) \arrow[r] \arrow[d] & H^b_\phi(\mathbf{E}_L/\pi^n\mathbf{E}_L^+) \arrow[d] \\ H^b_\phi(\mathcal{H}_L, \mathbf{E}) \arrow[r] & H^b_\phi(\mathcal{H}_L, \mathbf{E}/\pi^n\mathbf{E}^+) \end{tikzcd}$$

in which all the arrows are isomorphisms; in fact by 2.1.4(ii), the horizontal arrows are isomorphisms, and since $H^b(\mathcal{H}_L, \mathbf{E}) = 0$ for $b > 0$ the same is true of the left vertical arrow. Therefore the maps (2.2.8) are isomorphisms, and hence γ_n is a quasi-isomorphism, for every $n \geq 1$.

(b) $\varprojlim(\beta_n)$ *is a quasi-isomorphism.* We consider the cohomology of the finite group $\Delta = \mathrm{Gal}(L_\infty/K_\infty)$ acting on the short exact sequence

$$0 \to \pi^n\mathbf{E}_L^+ \otimes V \to \mathbf{E}_L \otimes V \to \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V \to 0. \qquad (2.2.9)$$

Lemma 2.2.10. *(i)* $H^j(\Delta, \mathbf{E}_L \otimes V) = 0$ *for* $j > 0$.
(ii) There exists $r \geq 0$ *such that for all* $j > 0$ *and* $n \in \mathbb{Z}$, *the group* $H^j(\Delta, \pi^n\mathbf{E}_L^+ \otimes V)$ *is killed by* π^r.

Proof. It is enough to prove (ii) for $n = 0$ (since π is fixed by Δ) and since $\mathbf{E}_L = \varinjlim \pi^{-n}\mathbf{E}_L^+$, (ii) implies (i). It is therefore enough to know that if M is any $\mathbf{E}_L^+$-module with a semilinear action of Δ, then there exists $r \geq 0$ such that $\pi^r H^j(\Delta, M) = 0$ for any $j > 0$, which is standard.[4] □

To complete the computation of β_n, we next recall [16, 1.9] that an inverse system (X_n) of abelian groups is *ML-zero* if for every n there exists $r = r(n) \geq 0$

[4] Let $M \to N^\bullet$ be the standard resolution. Choose $y \in \mathbf{E}_L^+$ such that $x = \mathrm{tr}_{\mathbf{E}_L/\mathbf{E}_K}(y) \neq 0$, and let $\lambda(m) = \sum_{g\in\Delta} g(ym)$. Then the composite $(N^\bullet)^\Delta \hookrightarrow N^\bullet \xrightarrow{\lambda} (N^\bullet)^\Delta$ is multiplication by x, hence by passing to cohomology, multiplication by x kills $H^j(\Delta, M)$ for $j > 0$.

such that $X_{n+r} \to X_n$ is the zero map. The class of ML-zero inverse systems is a Serre subcategory [16, 1.12]. A morphism $(X_n) \to (Y_n)$ is said to be an *ML-isomorphism* if its kernel and cokernel are ML-zero, and if this is so, the induced maps

$$\varprojlim X_n \to \varprojlim Y_n, \quad R^1 \varprojlim X_n \to R^1 \varprojlim Y_n \tag{2.2.11}$$

are isomorphisms. This implies that if $(f_n)\colon (X_n^\bullet) \to (Y_n^\bullet)$ is a morphism of inverse systems of complexes with surjective transition maps $X_{n+1}^i \to X_n^i$, $Y_{n+1}^i \to Y_n^i$, then if $(H^*(f_n))\colon (H^*(X_n^\bullet)) \to (H^*(Y_n^\bullet))$ is an ML-isomorphism, the map $\varprojlim(f_n)\colon \varprojlim X_n^\bullet \to \varprojlim Y_n^\bullet$ is a quasi-isomorphism. (Consider the induced map between the exact sequences [16, (2.1)] for $X_n^\bullet$ and $Y_n^\bullet$.)
From the exact sequence of cohomology of (2.2.9) and the lemma, we deduce that:

- for all $j > 0$, the inverse system $(H^j(\Delta, \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V))_n$ is ML-zero;
- the map of inverse systems

  $$(D_{1,n})_n \to (H^0(\Delta, \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V))_n$$

  is an ML-isomorphism.

We now have a spectral sequence of inverse systems of abelian groups $({}_nE_2^{ij})_n \Rightarrow ({}_nE_\infty^{i+j})_n$ with

$$\begin{aligned}{}_nE_2^{ij} &= H_\phi^i(\Gamma_K, H^j(\Delta, \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V))\\ {}_nE_\infty^k &= H_\phi^k(\mathrm{Gal}(L_\infty/K), \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V).\end{aligned}$$

such that, for all $i \geq 0$ and $j > 0$, the inverse system $({}_nE_2^{ij})_n$ are ML-zero. Therefore the edge homomorphism

$$({}_nE_2^{i0})_n \to ({}_nE_\infty^i)_n$$

is an ML-isomorphism. Moreover for all $i \geq 0$ the map of inverse systems

$$(H_\phi^i(\Gamma_K, D_{m,n}))_n \to ({}_nE_2^{i0})_n$$

is an ML-isomorphism, so composing with the edge homomorphism gives an ML-isomorphism

$$(H_\phi^i(\Gamma_K, D_{1,n}))_n \to (H_\phi^i(\mathrm{Gal}(L_\infty/K), \mathbf{E}_L/\pi^n\mathbf{E}_L^+ \otimes V))_n.$$

Hence $\varprojlim(\beta_n)_n$ is a quasi-isomorphism. □

2.3 Kummer towers

Let F be any local field of characteristic 0, with perfect residue field. Set $\varpi = \varpi_F$, $k = k_F$, $\mathfrak{o} = \mathfrak{o}_F$. (Later in this section we will require further that F is absolutely unramified.)

Let $K \supset F$ be any d-big local field such that $\mathfrak{o}_K/\mathfrak{o}_F$ is formally smooth (i.e., ϖ is a uniformiser of K). Let $\{t_\alpha \mid 1 \le \alpha \le d\} \subset \mathfrak{o}_K^*$ be a set of units whose reductions $\{\bar{t}_\alpha\} \subset k_K$ form a p-basis for k_K.

Fix an algebraic closure $\overline{K}$ of K. Let $(\varepsilon_n)_{n\ge 0}$ be a compatible system of primitive p^n-th roots of unity in $\overline{K}$, and for each α let $(t_{\alpha,n})_{n\ge 0}$ be a compatible system of p^n-th roots of t_α.

Set $F_n = F(\varepsilon_n)$, $\mathfrak{o}_n = \mathfrak{o}_{F_n}$, $k_n = k_{F_n}$, $K'_n = K(t_{1,n}, \dots, t_{d,n})$ and $K_n = K'_n(\varepsilon_n)$. The tower $\{F_n\}$ is strictly deeply ramified; choose $n_0 \ge 0$, $\xi \in K_{n_0}$ with $0 < v_p(\xi) \le 1$, and uniformisers $\varpi_n \in \mathfrak{o}_n$ such that $\varpi_{n+1}^p \equiv \varpi_n^p \pmod{\xi}$ for all $n \ge n_0$. Let $X_{\mathcal{F}}$ be the field of norms of $\{F_n\}$ and $k_{\mathcal{F}} = \varprojlim (k_n, f)$ its residue field. Put $\bar{\pi} = \Pi_{\mathcal{F}}$, so that $X_{\mathcal{F}} \simeq k_{\mathcal{F}}[[\bar{\pi}]]$, and the isomorphism is canonical once the uniformisers ϖ_n are fixed (since $k_{\mathcal{F}}$ is perfect). Write $^-$ for reduction mod ξ.

We have $\mathfrak{o}_{K'_n} = \mathfrak{o}_K[t_{1,n}, \dots, t_{d,n}]$ since this ring is a DVR, and so ϖ_n satisfies an Eisenstein polynomial over K'_n as well as over F. Hence $\mathfrak{o}_{K_n} = \mathfrak{o}_{K'_n}[\varpi_n] = \mathfrak{o}_n \otimes_{\mathfrak{o}} \mathfrak{o}_K[\{t_{\alpha,n}\}]$, and so

$$\mathfrak{o}_{K_n}/\xi = \mathfrak{o}_n/\xi \otimes_k k_K[\bar{t}_{1,n}, \dots, \bar{t}_{d,n}] = \mathfrak{o}_n/\xi \otimes_k k_K^{1/p^n}$$

and we have a commutative diagram

$$\begin{tikzcd}
\mathfrak{o}_{n+1}/\xi \otimes_k k_K^{1/p^{n+1}} \arrow[r, "1\otimes f^{n+1}", "\sim"'] \arrow[d, "f"'] & \mathfrak{o}_{n+1}/\xi \underset{f^{-n-1},\,k}{\otimes} k_K \arrow[d, "f\otimes 1"] \\
\mathfrak{o}_n/\xi \otimes_k k_K^{1/p^n} \arrow[r, "1\otimes f^n", "\sim"'] & \mathfrak{o}_n/\xi \underset{f^{-n},\,k}{\otimes} k_K \arrow[d, "\wr"'] \\
& k_n[\varpi_n]/(\varpi_n^{rp^n}) \underset{f^{-n},\,k}{\otimes} k_K
\end{tikzcd}$$

Therefore

$$\mathbf{E}_K^+ = X_{\mathcal{K}}^+ = \varprojlim_{n \ge n_0} k_n[\varpi_n]/(\varpi_n^{rp^n}) \underset{f^{-n},\,k}{\otimes} k_K = k_{\mathcal{F}}[[\bar{\pi}]] \underset{f^{-\infty},\,k}{\widehat{\otimes}} k_K$$

where $f^{-\infty}\colon k \hookrightarrow k_{\mathcal{F}}$ is the homomorphism making the diagram

$$\begin{tikzcd}
k_{\mathcal{F}} \arrow[r, "\sim"] & \dots \arrow[r, "\sim", "f"'] & k_{n+1} \arrow[r, "\sim", "f"'] & k_n & \\
 & & k \arrow[u, hook] \arrow[r, "\sim", "f"'] & k \arrow[u, hook] \arrow[r, "\sim", "f^n"'] & k \arrow[llllu, bend left, "f^{-\infty}"]
\end{tikzcd}$$

commute. In other words, if we view $k_{\mathcal{F}}$ as an extension of k via the map $f^{-\infty}$ just defined, we have $\mathbf{E}_K^+ = k_{\mathcal{F}}[[\bar{\pi}]]\widehat{\otimes}_k k_K$.

Set $K'_\infty = \bigcup K'_n \subset K_\infty$. Define the various Galois groups

$$\begin{aligned}
\Gamma_K &= \mathrm{Gal}(K_\infty/K) = \Gamma_F \ltimes \Delta_{K/F} \\
\Gamma_F &= \mathrm{Gal}(K_\infty/K'_\infty) = \mathrm{Gal}(F_\infty/F) \hookrightarrow \mathbb{Z}_p^* \\
\Delta_{K/F} &= \mathrm{Gal}(K_\infty/F_\infty) \simeq \mathbb{Z}_p^d
\end{aligned}$$

acting on K_∞ as follows: if $a \in \mathbb{Z}_p^*$ is the image of $\gamma_a \in \Gamma_F$ and $\underline{b} \in \mathbb{Z}_p^d$ the image of $\delta_{\underline{b}} \in \Delta_{K/F}$ then

$$\begin{aligned}
\gamma_a \colon \varepsilon_n &\mapsto \varepsilon_n^a & \qquad \delta_{\underline{b}} \colon \varepsilon_n &\mapsto \varepsilon_n \\
t_{\alpha,n} &\mapsto t_{\alpha,n} & t_{\alpha,n} &\mapsto \varepsilon_n^{b_\alpha} t_{\alpha,n}.
\end{aligned}$$

To be more precise we suppose from now on that $F/\mathbb{Q}_p$ is unramified, so that $\mathfrak{o}_n = \mathfrak{o}[\varepsilon_n]$, and we may choose $\varpi_n = \varepsilon_n - 1$. Then the projections $k_{\mathcal{F}} \to k$, $k_{\mathcal{K}} \to k_K$ are isomorphisms, and Γ_K acts on $\mathbf{E}_K^+ = k_K[[\bar{\pi}]]$ as follows: for $a \in \mathbb{Z}_p^*$,

$$\gamma_a \colon \Pi \mapsto (1+\Pi)^a - 1, \quad \gamma_a = \text{ identity on } k_c K$$

and for $\underline{b} \in \mathbb{Z}_p^d$, $\delta_{\underline{b}}$ is the unique automorphism of $\mathbf{E}_K^+$ whose reduction mod $(\bar{\pi})$ is the identity, and which satisfies

$$\delta_{\underline{b}} \colon \bar{\pi} \mapsto \bar{\pi}, \quad \bar{t}_\alpha \mapsto (1+\bar{\pi})^{b_\alpha} \bar{t}_\alpha.$$

Such a unique automorphism exists since k_K is formally étale over $\mathbb{F}_p(\bar{t}_1, \dots, \bar{t}_d)$.

To lift to characteristic 0, set $\mathbf{A}_K^+ = \mathfrak{o}_K[[\pi]]$, with the obvious surjection to $\mathbf{E}_K^+ = k_K[[\bar{\pi}]]$. The lifting ϕ of Frobenius is given as follows: on $\mathfrak{o}_K$ it is the unique lifting of Frobenius for which $\phi(t_i) = t_i^p$; and $\phi(\pi) = (1+\pi)^p - 1$. It is then immediate that the conditions (2.1.1), (2.1.2) hold, and the action of Γ_K on $\mathbf{A}_K^+$ satisfies

$$\begin{aligned}
\gamma_a \colon \pi &\mapsto (1+\pi)^a - 1 & \qquad \delta_{\underline{b}} \colon \pi &\mapsto \pi \\
\gamma_a &= \text{identity on } \mathfrak{o}_K & t_\alpha &\mapsto (1+\pi)^{b_\alpha} t_\alpha.
\end{aligned}$$

Remark 2.3.1. There is a natural generalisation of this construction for a Lubin-Tate formal group G over $\mathfrak{o}_F$ associated to a distinguished polynomial $g \in \mathfrak{o}_F[X]$. One takes F_∞/F to be the Lubin-Tate extension generated by the division points of G, and $K'_n = K(\{t_{\alpha,n}\})$ where $g(t_{\alpha,n+1}) = t_{\alpha,n}$. Then $\mathbf{A}^+_K$ is the affine algebra of G over $\mathfrak{o}_K$; the lifting of Frobenius is given by g. For some details when $d = 0$, and indications of what does and what does not extend, see Lionel Fourquaux's Ph.D. thesis [14, §1.4.1].

References

[1] A. Abbès, T. Saito: *Ramification of local fields with imperfect residue fields.* American J. of Math. 124 (2002), 879–920

[2] — , — : *Ramification of local fields with imperfect residue fields II.* In: Kazuya Kato's fiftieth birthday, Doc. Math. 2003, Extra Vol., 5–72

[3] V. Abrashkin: *An analogue of the field-of-norms functor and the Grothendieck conjecture.* `arXiv:math.NT/0503200`

[4] F. Andreatta: *Generalized ring of norms and generalised (ϕ, Γ)-modules.* To appear in Ann. Sci. Éc. Norm. Sup.

[5] F. Andreatta, A. Iovita: *Cohomology of generalised (ϕ, Γ)-modules.* Preprint.

[6] J. Ax: *Zeros of Polynomials over Local Fields—The Galois Action.* J. of Algebra 15 (1970), 417–428

[7] N. Bourbaki: *Algèbre Commutative, Chapitres 8 et 9.* Masson, Paris, 1983

[8] F. Cherbonnier, P. Colmez: *Représentations p-adiques surconvergentes.* Invent. math. 133 (1998), 581–611

[9] J. Coates, R. Greenberg: *Kummer theory for abelian varieties over local fields.* Invent. math. 124 (1996), 129–174

[10] G. Faltings: *p-adic Hodge theory.* J. Amer. Math. Soc. 1 (1988), 255–299

[11] J.-M. Fontaine: *Représentation p-adiques des corps locaux.* In: The Grothendieck Festschrift Vol.II, (P. Cartier *et al.*, ed.), 249–309. Birkhäuser, 1990

[12] J.-M. Fontaine, J. P. Wintenberger: *Le ≪corps des normes≫ de certaines extensions algébriques de corps locaux.* CRAS 288 série A (1979), 367–370

[13] — , — : *Extensions algébriques et corps des normes des extensions APF des corps locaux.* CRAS 288 série A (1979), 441–444

[14] L. Fourquaux: Ph.D. thesis, Université Paris 6, December 2005.

[15] L. Herr: *Sur la cohomologie galoisienne des corps p-adiques.* Bull. Soc. Math. France 126 (1998), 563–600

[16] U. Jannsen: *Continuous étale cohomology.* Math. Ann. 280 (1988), 207–245

[17] K. Kato: *A generalization of local class field theory by using K-groups II.* J. Fac. Sci. Univ. Tokyo 27 (1980), 603–683

[18] H. Matsumura: *Commutative Algebra.* 2nd edition, Benjamin/Cummings, 1980

[19] J. Nekovář: *Selmer complexes.* Preprint (March 2006), available at `http://www.math.jussieu.fr/~nekovar/pu/`

[20] A. J. Scholl: *An introduction to Kato's Euler systems.* Galois Representations in Arithmetic Algebraic Geometry (A. J. Scholl & R. L. Taylor, ed.), 379–460. Cambridge University Press, 1998

[21] J-P. Serre: *Corps locaux.* Hermann, 1968

[22] J. Tate: *p-divisible groups.* Proceedings of a conference on local fields, Driebergen (T. A. Springer, ed.), 158–183, Springer-Verlag (1967)

[23] J. P. Wintenberger: *Le corps des normes de certaines extensions infinies de corps locaux; applications.* Annales scientifiques de l'É.N.S 4^{e} série 16 n^{o}1 (1983), 59–89

[24] I. B. Zhukov: *On ramification theory in the case of an imperfect residue field.* Mat. Sb. 194 (2003), no. 12, 3–30; translation in Sb. Math. 194 (2003), no. 11-12, 1747–1774

Anthony J. Scholl
DPMMS, University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB, England
a.j.scholl@dpmms.cam.ac.uk

Divisibility Sequences and Powers of Algebraic Integers

Joseph H. Silverman

Received: November 15, 2005

Abstract. Let α be an algebraic integer and define a sequence of rational integers $d_n(\alpha)$ by the condition

$$d_n(\alpha) = \max\{d \in \mathbb{Z} : \alpha^n \equiv 1 \pmod{d}\}.$$

We show that $d_n(\alpha)$ is a strong divisibility sequence and that it satisfies $\log d_n(\alpha) = o(n)$ provided that no power of α is in $\mathbb{Z}$ and no power of α is a unit in a quadratic field. We completely analyze some of the exceptional cases by showing that $d_n(\alpha)$ splits into subsequences satisfying second order linear recurrences. Finally, we provide numerical evidence for the conjecture that aside from the exceptional cases, $d_n(\alpha) = d_1(\alpha)$ for infinitely many n, and we ask whether the set of such n has postive (lower) density.

2000 Mathematics Subject Classification: Primary: 11R04; Secondary: 11A05, 11D61
Keywords and Phrases: divisibility sequence, multiplicative group

Introduction

A sequence of positive integers $\{d_n\}$ is called a *divisibility sequence* if it has the property

$$m|n \Longrightarrow d_m|d_n. \tag{1}$$

Well-known examples of divisibility sequences include sequences of the form $d_n = a^n - 1$, the Fibonacci sequence F_n, and elliptic divisibility sequences D_n. The first two also satisfy a linear recurrence. A complete characterization of linear recurrence divisibility sequences is given in [2]. Elliptic divisibility sequences are associated to points of infinite order on elliptic curves. Thus if $P \in E(\mathbb{Q})$, then the sequence D_n is formed by writing $x(nP) = A_n/D_n^2$, see [9].

In this paper we investigate divisibility sequences $(d_n(\alpha))_{n\geq 1}$ associated to algebraic integers $\alpha \in \bar{\mathbb{Z}}$ by the rule

$$d_n(\alpha) = \max\{d \in \mathbb{Z} : \alpha^n \equiv 1 \pmod{d}\}. \tag{2}$$

(We assume throughout that $\alpha \neq 0$ and that α is not a root of unity.) It is not difficult to show that $d_n(\alpha)$ is a divisibility sequence, and indeed that it satisfies the stronger divisibility property

$$\gcd\bigl(d_m(\alpha), d_n(\alpha)\bigr) = d_{\gcd(m,n)}(\alpha),$$

see Proposition 2.

These sequences are interesting in their own right as generalizations of the classical divisibility sequences $a^n - 1$ with $a \in \mathbb{Z}$. They are also interesting as a special case of divisibility sequences attached to points of infinite order on algebraic groups (see [8, Section 6]) for which we can prove unconditional results.

We now briefly summarize the contents of this paper. We begin in Section 1 with the proof that $d_n(\alpha)$ is a strong divisibility sequence. Section 2 contains a variety of numerical examples illustrating varied behaviors of $d_n(\alpha)$ for different choices of α. In Section 3 we prove a useful result on linear dependence of Galois conjugates, and in Section 4 we combine this with a deep result of Corvaja and Zannier [5] to prove:

Theorem 1. *Let $\alpha \in \bar{\mathbb{Z}}$ and let $d_n(\alpha)$ be the associated divisibility sequence* (2). *Then*

$$\lim_{n\to\infty} \frac{\log d_n(\alpha)}{n} = 0$$

unless either some power of α is in $\mathbb{Z}$ or some power of α is a unit in a quadratic extension of $\mathbb{Q}$.

The theorem says that aside from a few specific cases, the sequences $d_n(\alpha)$ grow slower than exponentially. One of the exceptional cases is easy to analyze. If $\alpha^r \in \mathbb{Z}$ with $|\alpha^r| \geq 2$ and if no smaller power of α is in $\mathbb{Z}$, then one easily checks that

$$d_n(\alpha) = \begin{cases} |\alpha^n - 1| & \text{if } r|n, \\ 1 & \text{if } r \nmid n. \end{cases}$$

In particular, $d_n(\alpha)$ contains a subsequence that grows exponentially.

In Section 5 we analyze the other exceptional case and give a complete description of $d_n(\alpha)$ for real quadratic units $\alpha = u + v\sqrt{D}$. If the norm of α is 1, we prove that $d_n(\alpha)$ satisfies a fourth order linear recurrence. More precisely, we show that the subsequences $d_{2n}(\alpha)$ and $d_{2n+1}(\alpha)$ both satisfy the same second order linear recurrence, but with different starting values. If the norm of α is -1, then we prove that $d_n(\alpha) = 1$ for all of the odd values of n. The subsequence of even terms $d_{2n}(\alpha) = d_n(\alpha^2)$ satisfies a fourth order linear recurrence, since α^2 has norm 1. The proofs of these statements involve elementary, but rather intricate, calculations.

Finally, in Section 6 we observe that except in the two exceptional cases, the sequences $d_n(\alpha)$ appear to include many small values. Theorem 1 says that $\log d_n(\alpha) = o(n)$, and $d_n(\alpha)$ does contain arbitrarily large values, but experimentally one finds for example that $d_n(\alpha)$ is frequently equal to $d_1(\alpha)$. We present one such experiment in Section 6 and use it to conjecture that the set

$$\{n \geq 1 : d_n(\alpha) = d_1(\alpha)\}$$

is infinite (generalizing a conjecture of Ailon and Rudnick [1]) and to ask whether this set in fact has positive (lower) density.

Acknowledgements. The author thanks Mike Rosen for his assistance in simplifying the proof of Proposition 3.

1. Divisibility sequences associated to algebraic integers

We begin by reminding the reader of some classical definitions.

Definition 1. A *divisibility sequence* is a sequence of of positive integers $(d_n)_{n \geq 1}$ with the property that

$$m|n \Longrightarrow d_m|d_n. \tag{3}$$

The sequence is *normalized* if $d_1 = (1)$, which can always be arranged by replacing d_n by d_n/d_1. A *strong divisibility sequence* satisfies the more stringent requirement that

$$d_{\gcd(m,n)} = \gcd(d_n, d_m) \qquad \text{for all } m, n \in \mathbb{N}. \tag{4}$$

Examples of strong divisibility sequences include the Fibonacci sequence and elliptic divisibility sequences.

Our principal objects of study in this note are the sequences $(d_n(\alpha))$ defined by (2). Our first task is to show that they are strong divisibility sequences.

Proposition 2. *Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer. The associated sequence $(d_n(\alpha))_{n \geq 1}$ defined by* (2) *is a strong divisibility sequence.*

Proof. We begin by verifying that (d_n) is a divisibility sequence, i.e., it satisfies (3). Let $m, n \in \mathbb{N}$ satisfy $m|n$ and write

$$\alpha^m - 1 = d_m v \qquad \text{and} \qquad \alpha^n - 1 = d_n w.$$

By assumption, $m|n$, so we can use the identity

$$X^N - 1 = (X - 1)(X^{N-1} + X^{N-2} + \cdots + X + 1)$$

with $X = \alpha^m$ and $N = n/m$ to obtain

$$\alpha^n - 1 = (\alpha^m - 1)z \qquad \text{with } z \in \bar{\mathbb{Z}}.$$

Let $g = \gcd(d_m, d_n)$ and write

$$d_m x + d_n y = g \qquad \text{with } x, y \in \mathbb{Z}.$$

We multiply through by w and substitute to obtain

$$gw = d_m xw + d_n yw = d_m xw + d_m vzy = d_m(xw + vzy).$$

Subtituting this in above yields (note that $g|d_m$)

$$\alpha^n - 1 = d_n \cdot \frac{d_m}{g} \cdot (xw + vzy).$$

Thus $d_n d_m/g$ divides $\alpha^n - 1$. But d_n is, by definition, the largest natural number dividing $\alpha^n - 1$, so $d_m = g$. This shows that $d_m | d_n$, so (d_n) is a divisibility sequence.

We next show that (d_n) is a strong divisibility sequence, i.e., it satisfies (4). Let $m, n \in \mathbb{N}$ be arbitrary and let $k = \gcd(m,n)$. Then $k|m$ and $k|n$, so from above we know that $d_k | d_m$ and $d_k | d_n$. Therefore $d_k | \gcd(d_m, d_n)$.

To prove the opposite divisibility, we write $m = kM$ and $n = kN$. Then $\gcd(M,N) = 1$, so there are polynomials $A(X), B(X) \in \mathbb{Z}[X]$ satisfying

$$A(X) \cdot (X^M - 1) + B(X) \cdot (X^N - 1) = X - 1.$$

(To see this, it is enough to observe that the resultant of $\frac{X^M-1}{X-1}$ and $\frac{X^N-1}{X-1}$ is 1.) Substituting $X = \alpha^k$ yields

$$A(\alpha^k) \cdot (\alpha^m - 1) + B(\alpha^k) \cdot (\alpha^n - 1) = \alpha^k - 1.$$

As above, write $\alpha^m - 1 = a_m v$ and $\alpha^n - 1 = a_n w$ and let $g = \gcd(a_m, a_n)$. Then

$$g \cdot \left(A(\alpha^k) \cdot \frac{d_m}{g} \cdot v + B(\alpha^k) \cdot \frac{d_n}{g} \cdot w \right) = \alpha^k - 1,$$

where the quantity in parentheses is in $\bar{\mathbb{Z}}$. It follows that $g \le d_k$, since d_k is the largest natural number dividing $\alpha^k - 1$. We have now shown that $g \le d_k$ and $d_k | g$, which completes the proof that $d_k = g = \gcd(d_m, d_n)$. □

Remark 1. The fact that $d_n(\alpha)$ is a divisibility sequence follows from the [8, Proposition 8] applied to the torus obtained by restriction of scalars from $\mathbb{Z}[\alpha]$ to $\mathbb{Z}$ of the multiplicative group $\mathbb{G}_m$. Thus Proposition 2 strengthens [8] (for certain tori) by showing that the divisibility sequence is strong. To avoid introducing unnecessary machinery, we have been content to prove here the case that we need, but we note that it is not difficult to generalize Proposition 2 to the more general setting of commutative algebraic groups studied in [8].

2. Numerical examples

In this section we look at numerical examples that illustrate different sorts of behavior.

Example 1. The most elementary example is $\alpha \in \mathbb{Z}$ with $|\alpha| > 1$, which yields most classical examples $a_n = \alpha^n - 1$ of divisibility sequences. However, there are many deep open problems for even this simple case. For example, are there infinitely many values of n for which $a_n(2)$ is prime?

Example 2. Let $\alpha = 1 + i$. The associated sequence is

$$(a_n(1+i)) = 1,1,1,5,1,1,1,15,1,1,1,65,1,1,1,255,1,1,1,1025,\ldots$$

The pattern is clear and, using the fact that $\alpha^4 = -4$, it is easy to verify

$$a_n = |(-4)^{n/4} - 1| \quad \text{if } 4|n, \text{ and otherwise} \quad a_n = 1.$$

Although very elementary, we point out that for this example we have

$$\limsup_{n\to\infty} \frac{\log(a_n)}{n} = \frac{1}{4}\log(4) > 0. \tag{5}$$

Example 3. We again work in the Gaussian integers, but now we take $\alpha = 2+i$. The associated sequence is

$$(a_n(2+i)) = 1,2,1,8,1,2,1,48,1,2,1,104,1,2,1,1632,1,2,1,8,1,2,1,\dots$$

The pattern for $\alpha = 2+i$ is less regular than for $\alpha = 1+i$, but the data certainly suggest that all of the odd entries are equal to 1. Unfortunately, it turns out that this is not true, since $a_{27} = 109$. Indeed, 914 of the first 1000 a_n's with n odd are equal to 1, but some of them get quite large, for example $a_{1917} = 835921$. (Question: Are there infinitely many n satisfying $a_n(2+i) = 1$?)

The a_n with even n seem to fluctuate more than the odd n, and in particular, many large values appear, as is apparent from the following longer list of values:

$$\begin{aligned}(a_n(2+i)) = {}& 1,2,1,8,1,2,1,48,1,2,1,104,1,2,1,1632,1,2,1,8,1,2,1,1872,\\ & 1,2,109,232,1,1342,1,3264,1,2,1,3848,149,2,1,1968,1,2,\\ & 1,712,1,2,1,445536,1,2,1,424,1,218,1,1392,1,2,1,69784,\\ & 1,2,1,6528,1,2,1,8,1,2,1,15168816,1,298,1,8,1,2,1,\dots\end{aligned}$$

It is not hard to see that $\sup a_n = \infty$. More precisely, if p is a rational prime with $p \equiv 1 \pmod 4$, then $\alpha^{p-1} \equiv 1 \pmod p$, so $p|a_{p-1}$. Hence there are infinitely many n such that $\log(a_n) \ge \log(n)$. However, this is much slower growth than (5), so we might ask whether $\log(a_n)/n$ has a positive limsup. Table 1 lists the values of a_n for those $n < 3000$ satisfying $a_n > a_m$ for all $m < n$. The table suggests that

$$\limsup_{n\to\infty} \frac{\log(a_n(2+i))}{n} = 0.$$

In Section 4 we use [5] to prove that this is indeed the case, but we note that [5] itself relies on Schmidt's subspace theorem, so is far from elementary.

Example 4. Let $\alpha = 2+\sqrt{3}$. The associated sequence is

$$\begin{aligned}(a_n(2+\sqrt{3}\,)) = {}& 1,2,5,8,19,30,71,112,265,418,989,1560,3691,5822,\\ & 13775,21728,51409,81090,191861,302632,716035,1129438,\\ & 2672279,4215120,9973081,15731042,37220045,58709048,\dots\end{aligned}$$

The sequence clearly grows quite rapidly and regularly. We will show that it satisfies the linear recurrence

$$a_{n+4} = 4a_{n+2} - a_n.$$

In other words, if we define two subsequences using the odd and even terms, respectively,

$$b_n = a_{2n-1} \qquad \text{and} \qquad c_n = \frac{1}{2}a_{2n} \qquad \text{for } n = 1,2,3,\dots,$$

Then b_n and c_n satisfy the linear recurrence, $x_{n+2} = 4x_{n+1} - x_n$, with starting values 1 and 5 for b_n and 1 and 4 for c_n. This is typical for the division

n	a_n	$\log(a_n)/n$
1	1	0.0000
2	2	0.3466
4	8	0.5199
8	48	0.4839
12	104	0.3870
16	1632	0.4623
24	1872	0.3139
32	3264	0.2528
36	3848	0.2293
48	445536	0.2710
72	15168816	0.2296
96	2679453504	0.2261
144	4682401135776	0.2026
288	73018777396433948352	0.1588
576	16262888139288561844854144	0.1008
1152	28839207217834356759345681513216	0.0629
1440	118208444086469083866098414522688	0.0513
1728	194974704634639262404276022769124992	0.0470
2016	773127404949837686996635213979409984	0.0410
2160	54208082000209968285932117562946424303904	0.0434

Table 1. Growth of $a_n(2+i)$

sequences associated to *units* in real quadratic fields (see Section 5). As the next example shows, nonunits appear to behave quite differently.

Example 5. Let $\alpha = 2 + 3\sqrt{3}$. The associated sequence is

$$\begin{aligned}(a_n(2+3\sqrt{3}\,)) = {} & 1, 6, 13, 24, 1, 234, 1, 48, 13, 66, 1, 34632, 1, 6, 13, 96,\\ & 1, 702, 1, 264, 13, 6, 1, 346320, 1, 6, 13, 24, 59, 2574, \ldots\end{aligned}$$

Notice the striking difference between this sequence and the sequence for $2+\sqrt{3}$ examined in Example 4. We will show that

$$\log\bigl(a_n(2+3\sqrt{3}\,)\bigr) = o(n),$$

so this example resembles Example 3.

3. Linear dependence of Galois conjugates

In this section we prove an elementary result on the linear dependence of Galois conjugates. With an eye towards future applications and since the proof is no more difficult, we give a result that is more general than needed in this paper.

Proposition 3. *Let K be a field with separable closure K^s, let X/K be a commutative algebraic group, which we write additively, and let $x \in X(K^s)$. Suppose that for every $\sigma \in G_{K^s/K}$, the points x and x^σ are dependent in X. Then one of the following two conditions is true:*

(a) *There is an $n \geq 1$ such that $nx \in X(K)$.*

(b) *There is an* $n \geq 1$ *such that*

$$[K(nx) : K] = 2, \qquad \textit{and also} \qquad \mathrm{Trace}_{K(x)/K}(x) \in X(K)_{\mathrm{tors}}.$$

Conversely, if either (a) *or* (b) *is true, then* x *and* x^σ *are dependent for every* $\sigma \in G_{K^s/K}$.

Proof. Let $V = X(K^s) \otimes \mathbb{Q}$ and for any $y \in X(K^s)$, let V_y be the vector subspace (over $\mathbb{Q}$) of V generated by y and all of its Galois conjugates. Then $G_{K^s/K}$ acts continuously on V_y and we obtain a represenation $\rho_y : G_{K^s/K} \to \mathrm{GL}(V_y)$. The image is a finite subgroup of $\mathrm{GL}(V_y)$, which in general will yield information about y if $\dim(V_y)$ is smaller than $[K(y) : K]$. We have $y^\sigma = \rho_y(\sigma)y$ in V, so there are torsion points $t_\sigma \in X(K^s)_{\mathrm{tors}}$ so that $y^\sigma = \rho_y(\sigma)y + t_\sigma$ in $X(K^s)$. There are only finitley many distinct t_σ, so we can find an integer $n \geq 1$ such that

$$(ny)^\sigma = \rho_y(\sigma)(ny) \qquad \text{for all } \sigma \in G_{K^s/K}. \tag{6}$$

We start with the assumption that x and x^σ are dependent for all $\sigma \in G_{K^s/K}$, or equivalently, that V_x has dimension 1. Hence $\rho_x : G_{K^s/K} \to \mathrm{GL}(V_x) = \mathbb{Q}^*$, and since the image has finite order, it lies in $\{\pm 1\}$. We consider two cases depending on this image.

First, if $\mathrm{Image}(\rho_x) = \{1\}$, then (6) tells us that nx is fixed by $G_{K^s/K}$. Hence $x \in X(K)$, which verifies that x satisfies (a).

Second, suppose that $\mathrm{Image}(\rho_x) = \{\pm 1\}$, and let L be the fixed field of the kernel of ρ_x, so $[L : K] = 2$. Then (6) tells us that nx is fixed by $G_{K^s/L}$, so $nx \in X(L)$, and further it tells us that if $\sigma \notin G_{K^s/L}$, then $(nx)^\sigma = -nx$. Thus $nx \notin G(K)$, so $L = K(nx)$, which gives the first part of (b). For the second part, we use the fact that $nx \in X(L)$ to compute

$$\begin{aligned} n\,\mathrm{Trace}_{K(x)/K}(x) &= \mathrm{Trace}_{K(x)/K}(nx) \\ &= \frac{[K(x) : L]}{n}\,\mathrm{Trace}_{L/K}(nx) = nx + (-nx) = 0. \end{aligned}$$

This shows that $\mathrm{Trace}_{K(x)/K}(x)$ is in $X(K)_{\mathrm{tors}}$, which completes the proof that x satisfies (b)

We will not need the opposite implication, but for completeness, we sketch the proof. First, if $nx \in X(K)$, then for every $\sigma \in G_{K^s/K}$ we have $x^\sigma = x + t_\sigma$ for some n-torsion point $t_s \in X(K^s)_{\mathrm{tors}}$. Hence $nx^\sigma - nx = 0$, so x^σ and x are dependent.

Next suppose that $[K(nx) : K] = 2$ and $\mathrm{Trace}(x) \in X(K)_{\mathrm{tors}}$. Let $\sigma \in G_{K^s/K}$. If σ fixes $K(nx)$, then $(nx)^\sigma - nx = 0$, so $(nx)^\sigma$ and nx are dependent. If σ does not fix $K(nx)$, then

$$\begin{aligned} [K(x) : K(nx)]\big((nx)^\sigma + nx\big) &= [K(x) : K(nx)]\,\mathrm{Trace}_{K(nx)/K}(nx) \\ &= \mathrm{Trace}_{K(x)/K}(nx) \\ &= n\,\mathrm{Trace}_{K(x)/K}(x) \in X(K)_{\mathrm{tors}}. \end{aligned}$$

This proves that $(nx)^\sigma$ and nx are dependent, which completes the proof of the theorem. □

We state as a corollary the special case that is needed later.

Corollary 4. *Let $\alpha \in \bar{\mathbb{Q}}^*$ and suppose that for every $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$, the elements α and α^σ are multiplicatively dependent. Then there is an integer $n \geq 1$ so that one of the following is true.*

(a) $\alpha^n \in \mathbb{Q}$.
(b) $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] = 2$ *and* $\mathrm{N}(\alpha) = \pm 1$.

Proof. Apply Proposition 3 to the multiplicative group $\mathbb{G}_m/\mathbb{Q}$ and note that the torsion subgroup of $\mathbb{G}_m(\mathbb{Q})$ consists only of ± 1. □

4. The growth of divisibility sequences

In this section we apply Corvaja and Zannier's recent results [5] on generalized greatest common divisors (see also [3, 4]) to bound the growth rate of divisibility sequences $(d_n(\alpha))$. More precisely, Theorem 5 describes precise conditions that force a divisibility sequence $(d_n(\alpha))$ to grow slower than exponentially. We note that [5] is itself an application of Schmidt's subspace theorem, so although the proof of the theorem is not long, it describes a deep property of divisibility sequences associated to algebraic integers.

Theorem 5. *Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer and let $(d_n(\alpha))$ be the associated divisibility sequence,*

$$d_n(\alpha) = \max\{d \in \mathbb{Z} : \alpha^n \equiv 1 \pmod{d}\}.$$

Assume that one of the following two conditions is true:

(a) $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \geq 3$ *for all* $r \geq 1$.
(b) $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \geq 2$ *for all* $r \geq 1$ *and* $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \neq \pm 1$.

Then

$$\limsup_{n\to\infty} \frac{\log(d_n(\alpha))}{n} = 0.$$

In other words, $d_n(\alpha)$ grows slower than exponentially.

Proof. To ease notation, we write d_n for $d_n(\alpha)$. Let $K = \mathbb{Q}(\alpha)$, let $L/\mathbb{Q}$ be the Galois closure of K and let $\mathcal{O}_L$ be the ring of integers of L. By definition we have

$$\alpha^n - 1 \in d_n R,$$

so in particular $\alpha^n - 1 \in d_n\mathcal{O}_L$. Applying an automorphism $\sigma \in G_{L/\mathbb{Q}}$, we see that $(\alpha^\sigma)^n - 1 \in d_n\mathcal{O}_L$, since $d_n \in \mathbb{Z}$. Hence for every prime ideal $\mathfrak{p}$ of L we have

$$\min\bigl\{\mathrm{ord}_\mathfrak{p}(\alpha^n - 1), \mathrm{ord}_\mathfrak{p}(\alpha^{\sigma n} - 1)\bigr\} \geq \mathrm{ord}_\mathfrak{p}(d_n).$$

Multiplying by an appropriate multiple of $\log \mathrm{N}_{L/\mathbb{Q}}\,\mathfrak{p}$ and summing over primes yields

$$\log\gcd(\alpha^n - 1, \alpha^{\sigma n} - 1) \geq \log d_n, \tag{7}$$

where gcd is the generalized greatest common divisor used in [5, 8].

Suppose now that α and α^σ are multiplicatively independent in $\bar{\mathbb{Q}}^*$. Then [5, Proposition] tells us that for every $\epsilon > 0$ there is an $n_0 = n_0(\epsilon, \alpha, \alpha^\sigma)$ with the property that

$$\log \gcd(\alpha^n - 1, \alpha^{\sigma n} - 1) \le \epsilon n \qquad \text{for all } n \ge n_0. \tag{8}$$

Combining (7) and (8) yields the desired result.

So we are reduced to the case that for every $\sigma \in G_{L/\mathbb{Q}}$, the elements α and α^σ are multiplicatively dependent. Corollary 4 says that in this case, there is an integer r with the property $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \le 2$, which completes the proof of the theorem if α satisfies condition (a). If in addition $[\mathbb{Q}(\alpha^s) : \mathbb{Q}] \ne 1$ for all $s \ge 1$, then Corollary 4 says that α has norm ±1, which proves the theorem when α satisfies condition (b). □

The theorem says that except in special cases, the sequence $d_n(\alpha)$ cannot grow too rapidly. One might ask if $d_n(\alpha)$ is frequently very small. We consider this question later in Section 6.

5. Real quadratic divisibility sequences

Theorem 5 says that $d_n(\alpha)$ grows slowly except in a few specified instances. In this section we analyze the cases that $d_n(\alpha)$ may grow rapidly. We assume throughout that α is not a root of unity.

The first case allowed by Theorem 5 is when there is an $r \ge 1$ such that $\alpha^r \in \mathbb{Z}$. By assumption, $|\alpha^r| \ge 2$, so we find that

$$d_{rn}(\alpha) = |\alpha^{rn} - 1| \ge |\alpha^r|^n - 1 \ge 2^n - 1.$$

Thus this "Kummer case" yields

$$\limsup_{n\to\infty} \frac{\log(d_n(\alpha))}{n} \ge \frac{\log 2}{r} > 0.$$

Further, if α^r is the smallest power of α that is in $\mathbb{Z}$, then it is easy to see that $d_n(\alpha) = 1$ if $r \nmid n$.

The more interesting case arises when α^r lies in a real quadratic extension of $\mathbb{Q}$ and has norm ±1. The following elementary identities will be useful in analyzing this case.

Lemma 6. *For each $n \in \mathbb{N}$, let $A_n, B_n \in \mathbb{Q}[X, X^{-1}]$ be the Laurent polynomials*

$$A_n(X, X^{-1}) = \frac{X^n + X^{-n}}{2} \qquad \textit{and} \qquad B_n(X, X^{-1}) = \frac{X^n - X^{-n}}{2}.$$

Then the following identities hold in $\mathbb{Q}[X, X^{-1}]$.

(a) $A_{2n} - 1 = 2B_n^2$
(b) $B_{2n} = 2A_nB_n$
(c) $(A_1 + 1)(A_{2n-1} - 1) = (B_n + B_{n-1})^2$
(d) $B_1B_{2n-1} = B_n^2 - B_{n-1}^2$

Proof. Substitute the definition of A_n and B_n into each of the stated identities and use elementary algebra to simplify. We illustrate with (c). First we compute

$$\begin{aligned} 2(B_n + B_{n-1}) &= X^n - X^{-n} + X^{n-1} - X^{-n+1} \\ &= X^{n-1}(X+1) - X^{-n}(1+X) \\ &= (X+1)(X^{n-1} - X^{-n}). \end{aligned}$$

Replacing X by X^{-1} introduces a minus sign into B_n and B_{n-1}, so

$$2(B_n + B_{n-1}) = -(X^{-1}+1)(X^{-n+1} - X^n).$$

Now multiplying these two expressions yields

$$\begin{aligned} 4(B_n + B_{n-1})^2 &= -(X+1)(X^{-1}+1)(X^{n-1} - X^{-n})(X^{-n+1} - X^n) \\ &= (X + X^{-1} + 2)(X^{2n-1} + X^{-2n+1} - 2) \\ &= 4(A_1 + 1)(A_{2n-1} - 1). \end{aligned}$$

The other parts are similar. □

The next two propositions give a complete description of $d_n(\alpha)$ for $\alpha = u + v\sqrt{D}$ with $u, v \in \mathbb{Z}$. The other cases of real quadratic irrationalities are handled similarly. The details are left to the reader.

Theorem 7. *Let $D \geq 2$ be an integer that is not a perfect square, and let $\alpha = u + v\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ be the unit associated to a nontrivial positive solution (i.e., $u, v > 0$) of the Pell equation*

$$u^2 - v^2 D = 1.$$

Write

$$\alpha^n = \bigl(u + v\sqrt{D}\bigr)^n = u_n + v_n\sqrt{D},$$

so the divisibility sequence associated to α is given by

$$d_n(\alpha) = \gcd(u_n - 1, v_n).$$

Then

$$d_n(\alpha) = \begin{cases} 2v_{n/2} & \text{if } n \text{ is even,} \\ \gcd(u-1, v)\dfrac{v_{(n+1)/2} + v_{(n-1)/2}}{v} & \text{if } n \text{ is odd.} \end{cases}$$

The sequence $d_n(\alpha)$ satisfies the fourth order linear recursion

$$d_{n+4} = 2ud_{n+2} - d_n$$

whose characteristic polynomial is

$$T^4 - 2uT^2 + 1 = \bigl(T^2 - (u + v\sqrt{D})\bigr)\bigl(T^2 - (u - v\sqrt{D})\bigr).$$

The sequence grows exponentially,

$$\lim_{n\to\infty} \frac{\log d_n(\alpha)}{n} = \frac{1}{2}\log(\alpha) > 0. \tag{9}$$

Theorem 8. *Let $D, \alpha, u_n, v_n, d_n(\alpha)$ be as in the statement of Theorem 7 except now we assume that*

$$u^2 - v^2D = -1.$$

Then

$$d_n(\alpha) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{2}, \\ 2v_{n/2} & \text{if } n \equiv 0 \pmod{4}, \\ \dfrac{v_{n/2+1} + v_{n/2-1}}{u} & \text{if } n \equiv 2 \pmod{4}, \end{cases}$$

In particular, the even terms $d_{2n}(\alpha)$ satisfy a linear recurrence and grow exponentially, but the odd terms $d_{2n+1}(\alpha)$ form a constant sequence.

Proof of Theorem 7. Letting $\bar\alpha = u - v\sqrt{D}$, we have the usual formulas

(10) $$u_n = \frac{\alpha^n + \bar\alpha^n}{2} \quad\text{and}\quad v_n = \frac{\alpha^n - \bar\alpha^n}{2\sqrt{D}}.$$

The sequences (u_n) and (v_n) satisfy the recurrence

$$x_{n+2} = 2ux_{n+1} - x_n$$

with initial values

$$u_0 = 1, \quad u_1 = u, \quad v_0 = 0, \quad v_1 = v.$$

We observe that $v|v_n$ for every $n \geq 0$, so if we define a reduced sequence by $\tilde v_n = v_n/v$, then $\tilde v_n$ is the linear recursion sequence defined by

(11) $$\tilde v_0 = 0, \quad \tilde v_1 = 1, \quad \tilde v_{n+2} = 2u\tilde v_{n+1} - \tilde v_n.$$

By assumption, $\alpha\bar\alpha = 1$, so we have $\bar\alpha = \alpha^{-1}$ and the identities in Lemma 6(a,b) with $X = \alpha$ yield

(12) $$u_{2n} - 1 = d_{2n} - 1 = 2B_n^2 = 2v_n^2D,$$

(13) $$v_{2n} = \frac{B_{2n}}{\sqrt{D}} = \frac{2A_nB_n}{\sqrt{D}} = 2u_nv_n,$$

Using these, it is easy to compute the even terms of the divisibility sequence,

$$d_{2n}(\alpha) = \gcd(2v_n^2D, 2u_nv_n) = 2v_n \gcd(v_nD, u_n) = 2v_n.$$

For the last equality, we use the fact that $u_n^2 - Dv_n^2 = 1$ to conclude that u_n and v_nD are relatively prime.

Similarly, the identities in Lemma 6(c,d) with $X = \alpha$ give

(14) $$\begin{aligned}(u+1)(u_{2n-1} - 1) &= (A_1 + 1)(d_{2n-1} - 1) \\ &= (B_n + B_{n-1})^2 = (v_n + v_{n-1})^2D,\end{aligned}$$

(15) $$vv_{2n-1} = \frac{B_1B_{2n-1}}{D} = \frac{B_n^2 - B_{n-1}^2}{D} = v_n^2 - v_{2n-1}^2.$$

These give us a somewhat complicated formula for the odd terms in the divisibility sequence,

(16) $$d_{2n-1}(\alpha) = \gcd\left(\frac{(v_n + v_{n-1})^2D}{u+1}, \frac{v_n^2 - v_{n-1}^2}{v}\right).$$

Using the reduced sequence $\tilde{v}_n = v_n/v$, we observe that

$$(v_n + v_{n-1})^2 D = (\tilde{v}_n + \tilde{v}_{n-1})^2 v^2 D = (\tilde{v}_n + \tilde{v}_{n-1})^2 (u^2 - 1),$$

so we can rewrite (16) as

$$\begin{aligned} d_{2n-1}(\alpha) &= \gcd\left(\frac{(\tilde{v}_n + \tilde{v}_{n-1})^2(u^2-1)}{u+1}, \frac{(\tilde{v}_n^2 - \tilde{v}_{n-1}^2)v^2}{v} \right) \\ &= \gcd\bigl((\tilde{v}_n + \tilde{v}_{n-1})^2(u-1), (\tilde{v}_n^2 - \tilde{v}_{n-1}^2)v \bigr) \\ &= (\tilde{v}_n + \tilde{v}_{n-1}) \gcd\left((\tilde{v}_n + \tilde{v}_{n-1})(u-1), (\tilde{v}_n - \tilde{v}_{n-1})v \right). \end{aligned} \tag{17}$$

It remains to show the the gcd is equal to $\gcd(u-1,v)$.

A first observation is that adjacent terms of the sequence $(\tilde{v}_n)$ are relatively prime, i.e., $\gcd(\tilde{v}_n, \tilde{v}_{n-1}) = 1$, and further, they are alternately odd and even. This follows easily by induction from the initial values and recursive formula (11) satisfied by the sequence $(\tilde{v}_n)$. Hence

$$\gcd\left(\tilde{v}_n + \tilde{v}_{n-1}, \tilde{v}_n - \tilde{v}_{n-1} \right) = 1, \tag{18}$$

since the gcd certainly divides $\gcd(2\tilde{v}_n, 2\tilde{v}_{n-1}) = 2$, and it cannot equal 2 since $\tilde{v}_n + \tilde{v}_{n-1}$ is odd.

It is convenient to write out explicitly the closed sum for $\tilde{v}_n$:

$$\begin{aligned} \tilde{v}_n = \frac{v_n}{v} &= \frac{(u + v\sqrt{D})^n - (u - v\sqrt{D})^n}{2\sqrt{D}v} \\ &= \frac{1}{2\sqrt{D}v} \sum_{k=0}^{n} \binom{n}{k} u^{n-k} (v\sqrt{D})^k (1 - (-1)^k) \\ &= \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} u^{n-2k-1} v^{2k} D^k. \end{aligned}$$

In particular, there are rational integers $E_n \in \mathbb{Z}$ such that

$$\tilde{v}_n = nu^{n-1} + v^2 D E_n. \tag{19}$$

We first compute (using $v^2 D = u^2 - 1$)

$$\begin{aligned} \tilde{v}_n - \tilde{v}_{n-1} &= \bigl(nu^{n-1} + v^2 D E_n \bigr) - \bigl((n-1)u^{n-2} + v^2 D E_{n-1} \bigr) \\ &= nu^{n-2}(u-1) + u^{n-2} + (u^2-1)(E_n - E_{n-1}) \\ &\equiv 1 \pmod{u-1}. \end{aligned}$$

This proves that

$$\gcd(u-1, \tilde{v}_n - \tilde{v}_{n-1}) = 1. \tag{20}$$

If we could prove that $\gcd(\tilde{v}_n + \tilde{v}_{n-1}, v) = 1$, we would be done, but unfortunately it is easy to produce examples where this fails to be true. To obtain a weaker identity that suffices, we begin with the formula

$$\begin{aligned} \tilde{v}_n + \tilde{v}_{n-1} &= nu^{n-1} + (n-1)u^{n-2} + v^2 D (E_n + E_{n-1}) \\ &\equiv u^{n-2}\bigl(n(u+1) - 1 \bigr) \pmod{v}. \end{aligned} \tag{21}$$

Multiplying by $u-1$ yields

$$\begin{aligned}
&(\tilde v_n+\tilde v_{n-1})(u-1)\\
&\qquad\equiv u^{n-2}\big(n(u^2-1)-(u-1)\big) \pmod{v} &&\text{from (21),}\\
&\qquad\equiv u^{n-2}(nv^2D-(u-1)) \pmod{v} &&\text{since } u^2-1=v^2D,\\
&\qquad\equiv -u^{n-2}(u-1) \pmod{v}.
\end{aligned}$$

Hence

$$\begin{aligned}
\gcd\left((\tilde v_n+\tilde v_{n-1})(u-1),v\right)&=\gcd\left(-u^{n-2}(u-1),v\right)\\
&=\gcd(u-1,v),
\end{aligned}\tag{22}$$

since u and v are relatively prime.

Combining the above gcd computations, we find that

$$\begin{aligned}
&\gcd\big((\tilde v_n+\tilde v_{n-1})(u-1),(\tilde v_n-\tilde v_{n-1})v\big)\\
&\qquad=\gcd\left((\tilde v_n+\tilde v_{n-1})(u-1),v\right) &&\text{from (18) and (20),}\\
&\qquad=\gcd(u-1,v) &&\text{from (22).}
\end{aligned}$$

We are finally able to substitute this into (17) to obtain the formula

$$\begin{aligned}
d_{2n-1}(\alpha)&=(\tilde v_n+\tilde v_{n-1})\gcd\big((\tilde v_n+\tilde v_{n-1})(u-1),(\tilde v_n-\tilde v_{n-1})v\big)\\
&=(\tilde v_n+\tilde v_{n-1})\gcd(u-1,v)\\
&=\frac{(v_n+v_{n-1})\gcd(u-1,v)}{v},
\end{aligned}$$

which completes the proof of the stated formula for the odd terms in the divisibility sequence $d_n(\alpha)$.

In order to prove that $d_n(\alpha)$ satisfies a recurrence relation and to measure its exponential growth, we observe that we have proven that there are constants c_1 and c_2 (depending on u and v) so that

$$\begin{aligned}
d_{2n}(\alpha)&=c_1v_n,\\
d_{2n-1}(\alpha)&=c_2(v_n+v_{n-1}).
\end{aligned}\tag{23}$$

The sequence v_n satisfies $v_{n+2}=2uv_{n+1}-v_n$, so (23) implies the two recursions

$$\begin{aligned}
d_{2n+4}(\alpha)&=2ud_{2n+2}(\alpha)-d_n(\alpha)\\
d_{2n+3}(\alpha)&=2ud_{2n+1}(\alpha)-d_{2n-1}(\alpha).
\end{aligned}$$

Thus the sequence $d_n(\alpha)$ satisfies the recursive formula $x_{n+4}=2ux_{n+2}-x_n$ whose characteristic polynomial is

$$T^4-2uT^2+1=(T^2-\alpha)(T^2-\bar\alpha),$$

since $\alpha+\bar\alpha=2u$ and $\alpha\bar\alpha=1$. Finally, since we have chosen α to satisfy $|\alpha|>1$, the limit formula (9) follows from (23) and the fact that

$$\lim_{n\to\infty}\frac{\log v_n}{n}=\lim_{n\to\infty}\frac{\log\left(\dfrac{\alpha^n-\alpha^{-n}}{2\sqrt{D}}\right)}{n}=\log(\alpha).$$

This completes the proof of Theorem 7. □

Proof of Theorem 8. Clearly we have $d_{2n}(\alpha) = d_n(\alpha^2)$ directly from the definition. Let $\beta = \alpha^2$. Then $\beta\bar{\beta} = (\alpha\bar{\alpha})^2 = (-1)^2 = 1$, so the divisibility sequence $d_n(\beta)$ is of exactly the type described in Theorem 8. In order to obtain an explicit formula for $d_n(\beta) = d_{2n}(\alpha)$, we observe that

$$\begin{aligned}
v_{n/2}(\beta) &= v_n(\alpha) \quad \text{for even } n,\\
v_{(n\pm1)/2}(\beta) &= v_{n\pm1}(\alpha) \quad \text{for odd } n,\\
u(\beta) - 1 &= u_2(\alpha) - 1 = u^2 + v^2D - 1 = 2v^2D,\\
v(\beta) &= v_2(\alpha) = 2uv,\\
\gcd\bigl(u(\beta) - 1, v(\beta)\bigr) &= \gcd(2v^2D, 2uv) = 2v.
\end{aligned}$$

(Note that here u and v are given by $\alpha = u+v\sqrt{D}$.) We substitute these values into the formula for $a_n(\beta)$ provided by Theorem 8. Thus if n is even we find that

$$d_{2n}(\alpha) = d_n(\beta) = 2v_{n/2}(\beta) = 2v_n(\alpha),$$

and if n is odd we obtain

$$\begin{aligned}
d_{2n}(\alpha) = d_n(\beta) &= \frac{\gcd(u(\beta) - 1, v(\beta))(v_{(n+1)/2}(\beta) + v_{(n-1)/2}(\beta))}{v(\beta)}\\
&= \frac{2v(v_{n+1}(\alpha) + v_{n-1}(\alpha))}{2uv}\\
&= \frac{(v_{n+1}(\alpha) + v_{n-1}(\alpha))}{u}
\end{aligned}$$

This completes the proof of the formula for the even terms in the sequence $d_n(\alpha)$. It remains to show that $d_n(\alpha) = 1$ when n is odd.

We assume henceforth that n is odd. Then $u_n^2 - v_n^2D = -1$, which we rewrite as

$$(u_n + 1)(u_n - 1) - v_n^2D = -2. \tag{24}$$

This equation shows that $\gcd(u_n - 1, v_n)$ divides 2. However, it cannot equal 2, since otherwise the lefthand side of (24) would be divisible by 4. This completes the proof that $d_n(\alpha) = \gcd(u_n - 1, v_n) = 1$ when n is odd. □

6. Small entries in divisibility sequences

Theorem 5 tells us that except in a few specified cases, the sequence $d_n(\alpha)$ grows slower than exponentially, and although the values do occasionally get quite large, we find experimentally that $d_n(\alpha)$ is also often quite small. This leads us to make the following conjecture, which is the analog of a conjecture of Ailon and Rudnick [1] regarding $\gcd(a^n - 1, b^n - 1)$ for multiplicatively independent integers a and b.

$n \le$	$d_n = 1$	$d_n = 2$	$d_n = 3$	$d_n = 4$	$d_n = 5$	$d_n = 6$
1000	67.30 %	6.30 %	3.90 %	2.80 %	1.10 %	0.30 %
5000	66.32 %	6.10 %	3.72 %	2.50 %	0.78 %	0.32 %
10000	65.91 %	6.03 %	3.66 %	2.47 %	0.77 %	0.33 %
15000	65.82 %	5.99 %	3.60 %	2.42 %	0.78 %	0.33 %
20000	65.59 %	5.98 %	3.60 %	2.40 %	0.76 %	0.32 %

Table 2. Frequency of $\{n : d_n(\alpha) = k\}$ for $\alpha^3 - \alpha - 1 = 0$

Conjecture 9. *Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer and let $(d_n(\alpha))$ be the associated divisibility sequence* (2). *Assume that α satisfies one of the conditions* (a) *or* (b) *in Theorem 5. Then*

$$\{n \ge 1 : d_n(\alpha) = d_1(\alpha)\}$$

is infinite.

Example 6. It is worthwhile looking at a nontrivial example numerically. Let α be root of $T^3 - T - 1$. We find that the associated sequence starts

$$\begin{aligned}(d_n) = 1,1,1,1,1,1,2,1,1,1,1,1,3,4,1,1,1,1,1,1,2,1,1,5,1,3,1,8,\\ 1,1,1,1,1,1,2,1,1,1,9,1,1,4,1,1,1,1,1,35,2,1,1,3,1,\\ 1,1,16,1,59,1,1,1,1,2,1,3,1,1,1,1,4,1,5,1,1,1,1,2,9,1,\\ 1,1,1,1,8,1,1,1,1,1,1,6,1,1,1,1,35,1,4,1,101,\dots\end{aligned}$$

The data appears to support Conjecture 9 that $d_n = 1$ for infinitely many values of n. From this small amount of data it is less clear how often we should expect to have, say, $d_n = 2$ or $d_n = 3$. Table 2 gives the frequency of $d_n = k$ for each $k = 1, 2, \dots, 6$ and $n \le N$ for various values of N. The table suggests that the set $\{n \in \mathbb{N} : d_n = k\}$ is infinite, and indeed possibly that it has a positive density.

However, it is easily seen that there are some values of k for which the set is empty. For example, we claim that $d_n(\alpha) \ne 7$ for all n. The reason is that the smallest power of α satsifying $\alpha^n \equiv 1 \pmod{7}$ is α^{48} and

$$\alpha^{48} - 1 = 128800 + 226030\alpha + 170625\alpha^2 = 35(3680 + 6458\alpha + 4875\alpha^2).$$

Thus

$$7|d_n \Longrightarrow 48|n \Longrightarrow 35|d_n,$$

so d_n will never equal 7. It would be interesting to characterize the set $\{k \in \mathbb{N} : d_n(\alpha) \ne k \text{ for all } n\}$.

Based on this and various other examples, it is tempting to make a conjecture of the following sort, although given the scanty evidence, it seems safer to phrase it as a question.

Question 1. Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer and let $(d_n(\alpha))$ be the associated divisibility sequence (2) as usual. For each $k \in \mathbb{N}$, let

$$S_\alpha(k) = \{n \in \mathbb{N} : d_n(\alpha) = k\}.$$

Is it true that either $S_\alpha(k) = \emptyset$ or else $S_\alpha(k)$ has positive (lower) density in $\mathbb{N}$.

If Question 1 has an affirmative answer, it then becomes a very interesting question to describe the density of $S_\alpha(k)$ in terms of arithmetic properties of α, even for the initial nontrivial case $S_\alpha(d_1(\alpha))$.

Remark 2. The divisibility sequences $d_n(\alpha)$ studied in this paper can be defined in far more generality, for example using an element α in a ring of the form $R = \mathbb{Z}[T]/(F(T))$ for a monic polynomial $F(T) \in \mathbb{Z}[T]$. Thus $d_n(\alpha)$ is the largest rational integer d such that $\alpha^n - 1$ is divisible by d in the ring R.

As a particular example, consider the ring $R = \mathbb{Z}[T]/(T^2 - T)$ and element $\alpha = T + 2$. The natural isomorphism

$$R \cong \mathbb{Z}[T]/(T) \times \mathbb{Z}[T]/(T-1)$$

identifies $\alpha \leftrightarrow (2,3)$, so $d_n(\alpha) = \gcd(2^n - 1, 3^n - 1)$. Ailon and Rudnick [1] conjecture in this case that $d_n(\alpha) = 1$ for infinitely many n, and more generally they conjecture that if $a, b \in \mathbb{Z}$ are multiplicatively independent, then

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1) \quad \text{for infinitely many } n \geq 1. \tag{25}$$

Thus Conjecture 9 may be viewed as a generalization of Ailon and Rudnick's conjecture, and Question 1 suggests a strengthened statement. Ailon and Rudnick prove a strong version of (25) with $\mathbb{Z}$ replaced by the polynomial ring $\mathbb{C}[T]$. See also [6] and [7] for analogs over $\mathbb{F}_q[T]$ and for elliptic curves and [8, Section 7] for a more general conjecture on the infinitude, although not the density, of values of divisibility sequences associated to commutative group schemes.

References

[1] N. Ailon, Z. Rudnick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$, *Acta Arithmetica* 113 (2004), 31–38.

[2] J.P. Bézivin, A. Pethö, A.J. van der Poorten, A full characterisation of divisibility sequences, *Amer. J. of Math.* 112 (1990), 985–1001.

[3] Y. Bugeaud, P. Corvaja, U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Math. Zeit.* 243 (2003), no. 1, 79–84.

[4] P. Corvaja, U. Zannier, On the greatest prime factor of $(ab + 1)(ac + 1)$, *Proc. Amer. Math. Soc.* 131 (2002), 1705–1709.

[5] ——— A lower bound for the height of a rational function at S-unit points, *Monatshefte Math.*, 144 (2005), 203–224.

[6] J.H. Silverman, Common divisors of $a^n - 1$ and $b^n - 1$ over function fields, *New York Journal of Math.* (electronic) 10 (2004), 37–43.

[7] ——— Common divisors of elliptic divisibility sequences over function fields, *Manuscripta Math.*, 114 (2004), 432–446.

[8] ——— Generalized greatest common divisors, Divisibility sequences, and Vojta's conjecture for blowups *Monatsch. Math.*, 145 (2005), 333–350.

[9] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* 70 (1948), 31–74.

Joseph H. Silverman
Mathematics Department
Box 1917
Brown University
Providence
RI 02912 USA
jhs@math.brown.edu

On the Meromorphic Continuation of Degree Two L-Functions

To John Coates on the occasion of his 60^{th} birthday, with much gratitude.

Richard Taylor [1]

Received: January 9, 2005
Revised: June 28, 2006

Abstract. We prove that the L-function of any regular (distinct Hodge numbers), irreducible, rank two motive over the rational numbers has meromorphic continuation to the whole complex plane and satisfies the expected functional equation.

2000 Mathematics Subject Classification: 11R39, 11F80, 11G40.
Keywords and Phrases: Galois representation, modularity, L-function, meromorphic continuation.

Introduction

In this paper we extend the results of [Tay4] from the ordinary to the crystalline, low weight (i.e. in the Fontaine-Laffaille range) case. The underlying ideas are the same. However this extension allows us to prove the meromorphic continuation and functional equation for the L-function of any regular (i.e. distinct Hodge numbers) rank two "motive" over $\mathbb{Q}$. We avoid having to know what is meant by "motive" by working instead with systems of l-adic representations satisfying certain conditions which will be satisfied by the l-adic realisations of any "motive".
More precisely by a *rank* 2 *weakly compatible system of l-adic representations* $\mathcal{R}$ over $\mathbb{Q}$ we shall mean a 5-tuple $(M, S, \{Q_p(X)\}, \{\rho_\lambda\}, \{n_1, n_2\})$ where

[1] This material is based upon work partially supported by the National Science Foundation under Grant Nos. 9702885 and 0100090. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

- M is a number field;
- S is a finite set of rational primes;
- for each prime $p \notin S$ of $\mathbb{Q}$, $Q_p(X)$ is a monic degree 2 polynomial in $M[X]$;
- for each prime λ of M (with residue characteristic l say)
$$\rho_\lambda : G_{\mathbb{Q}} \longrightarrow GL_2(M_\lambda)$$
is a continuous representation such that, if $l \notin S$ then $\rho_\lambda|_{G_l}$ is crystalline, and if $p \notin S \cup \{l\}$ then ρ_λ is unramified at p and $\rho_\lambda(\mathrm{Frob}_p)$ has characteristic polynomial $Q_p(X)$; and
- n_1, n_2 are integers such that for all primes λ of M (lying above a rational prime l) the representation $\rho_\lambda|_{G_l}$ is Hodge-Tate with numbers n_1 and n_2, i.e. $\rho_\lambda \otimes_{\mathbb{Q}_l} \widehat{\mathbb{Q}_l^{ac}} \cong (M_\lambda \otimes_{\mathbb{Q}_l} \widehat{\mathbb{Q}_l^{ac}})(-n_1) \oplus (M_\lambda \otimes_{\mathbb{Q}_l} \widehat{\mathbb{Q}_l^{ac}})(-n_2)$ as $M_\lambda \otimes_{\mathbb{Q}_l} \widehat{\mathbb{Q}_l^{ac}}$-modules with M_λ-linear, $\widehat{\mathbb{Q}_l^{ac}}$-semilinear $G_{\mathbb{Q}_l}$-actions.

We call $\mathcal{R}$ *regular* if $n_1 \neq n_2$ and $\det \rho_\lambda(c) = -1$ for one (and hence all) primes λ of M. We remark that if $\mathcal{R}$ arises from a regular (distinct Hodge numbers) motive then one can use the Hodge realisation to check that $\det \rho_\lambda(c) = -1$ for all λ. Thus we consider this oddness condition part of regularity. It is not difficult to see that if one of the ρ_λ is absolutely reducible so are all the others. In this case we call $\mathcal{R}$ *reducible*, otherwise we call it *irreducible.* (If $\rho_{\lambda_0}^{\mathrm{ss}}$ is the sum of two characters these characters are Hodge-Tate and hence by results of [S1] themselves fit into compatible systems. The elements of these compatible systems provide the Jordan-Hölder factors of the other ρ_λ.)

We will call $\mathcal{R}$ *strongly compatible* if for each rational prime p there is a Weil-Deligne representation $\mathrm{WD}_p(\mathcal{R})$ of $W_{\mathbb{Q}_p}$ such that for primes λ of M not dividing p, $\mathrm{WD}_p(\mathcal{R})$ is equivalent to the Frobenius semi-simplification of the Weil-Deligne representation associated to $\rho_\lambda|_{G_p}$. ($\mathrm{WD}_p(\mathcal{R})$ is defined over $\overline{M}$, but it is equivalent to all its $\mathrm{Gal}\,(\overline{M}/M)$-conjugates.) If $\mathcal{R}$ is strongly compatible and if $i : M \hookrightarrow \mathbb{C}$ then we define an L-function $L(i\mathcal{R}, s)$ as the infinite product

$$L(i\mathcal{R}, s) = \prod_p L_p(i\mathrm{WD}_p(\mathcal{R})^\vee \otimes |\mathrm{Art}^{-1}|_p^{-s})^{-1}$$

which may or may not converge. Fix an additive character $\Psi = \prod \Psi_p$ of $\mathbb{A}/\mathbb{Q}$ with $\Psi_\infty(x) = e^{2\pi\sqrt{-1}x}$, and a Haar measure $dx = \prod dx_p$ on $\mathbb{A}$ with dx_∞ the usual measure on $\mathbb{R}$ and with $dx(\mathbb{A}/\mathbb{Q}) = 1$. If, say, $n_1 > n_2$ then we can also also define an ϵ-factor $\epsilon(i\mathcal{R}, s)$ by the formula

$$\epsilon(i\mathcal{R}, s) = \sqrt{-1}^{1+n_1-n_2} \prod_p \epsilon(i\mathrm{WD}_p(\mathrm{RS})^\vee \otimes |\mathrm{Art}^{-1}|_p^{-s}, \Psi_p, dx_p).$$

(See [Tat] for the relation between l-adic representations of $G_{\mathbb{Q}_p}$ and Weil-Deligne representations of $W_{\mathbb{Q}_p}$, and also for the definition of the local L and ϵ-factors.)

Theorem A *Suppose that $\mathcal{R} = (M, S, \{Q_x(X)\}, \{\rho_\lambda\}, \{n_1, n_2\})/\mathbb{Q}$ is a regular, irreducible, rank 2 weakly compatible system of l-adic representations with $n_1 > n_2$. Then the following assertions hold.*

1. *If $i : M \hookrightarrow \mathbb{C}$ then there is a totally real Galois extension $F/\mathbb{Q}$ and a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ such that $L(i\mathcal{R}|_{G_F}, s) = L(\pi, s)$.*
2. *For all rational primes $p \notin S$ and for all $i : M \hookrightarrow \mathbb{C}$ the roots of $i(Q_p(X))$ have absolute value $p^{-(n_1+n_2)/2}$.*
3. *$\mathcal{R}$ is strongly compatible.*
4. *For all $i : M \hookrightarrow \mathbb{C}$, the L-function $L(i\mathcal{R}, s)$ converges in $\operatorname{Re} s > 1 - (n_1 + n_2)/2$, has meromorphic continuation to the entire complex plane and satisfies a functional equation*

$$(2\pi)^{-(s+n_1)}\Gamma(s + n_1)L(i\mathcal{R}, s) = \epsilon(i\mathcal{R}, s)(2\pi)^{s+n_2-1}\Gamma(1 - n_2 - s)L(i\mathcal{R}^\vee, 1 - s).$$

More precisely we express $L(i\mathcal{R}, s)$ as a ratio of products of the L-functions associated to Hilbert modular forms over different subfields of F. (See section 6 for more details.)

For example suppose that $X/\mathbb{Q}$ is a rigid Calabi-Yau 3-fold, where by rigid we mean that $H^{2,1}(X(\mathbb{C}), \mathbb{C}) = (0)$. Then the zeta function $\zeta_X(s)$ of X has meromorphic continuation to the entire complex plane and satisfies a functional equation relating $\zeta_X(s)$ and $\zeta_X(4 - s)$. A more precise statement can be found in section six.

Along the way we prove the following result which may also be of interest. It partially confirms the Fontaine-Mazur conjecture, see [FM].

Theorem B *Let $l > 3$ be a prime and let $2 \leq k \leq (l + 1)/2$ be an integer. Let $\rho : G_\mathbb{Q} \to GL_2(\mathbb{Q}_l^{ac})$ be a continuous irreducible representation such that*

- *ρ ramifies at only finitely many primes,*
- $\det \rho(c) = -1$,
- *$\rho|_{G_l}$ is crystalline with Hodge-Tate numbers 0 and $1 - k$.*

Then the following assertions hold.

1. *There is a Galois totally real field F in which l is unramified, a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and an embedding λ of the field of rationality of π into $\mathbb{Q}_l^{ac}$ such that*
    - *$\rho_{\pi,\lambda} \sim \rho|_{G_F}$,*

- *π_x is unramified for all places x of E above l, and*
- *π_∞ has parallel weight k.*

2. *If ρ is unramified at a prime p and if α is an eigenvalue of $\rho(\mathrm{Frob}_p)$ then $\alpha \in \mathbb{Q}^{ac}$ and for any isomorphism $i : \mathbb{Q}_l^{ac} \xrightarrow{\sim} \mathbb{C}$ we have*

$$|i\alpha|^2 = p^{(k-1)/2}.$$

3. *Fix an isomorphism $i : \mathbb{Q}_l^{ac} \xrightarrow{\sim} \mathbb{C}$. There is a rational function $L_{l,i}(X) \in \mathbb{C}(X)$ such that the product*

$$L(i\rho, s) = L_{l,i}(l^{-s})^{-1} \prod_{p \neq l} i \det(1 - \rho_{I_p}(\mathrm{Frob}_p) p^{-s})^{-1}$$

converges in $\mathrm{Re}\, s > (k+1)/2$ and extends to a meromorphic function on the entire complex plane which satisfies a functional equation

$$(2\pi)^{-s}\Gamma(s)L(i\rho, s) = WN(\rho)^{k/2-s}(2\pi)^{s-k}\Gamma(k-s)L(i(\rho^\vee \otimes \epsilon^{k-1}), k-s),$$

where ϵ denotes the cyclotomic character, where $N(\rho)$ denotes the conductor of ρ (which is prime to l), and where W is a complex number. (W is given in terms of local ϵ-factors in the natural way. See section 6 for details.)

4. *If $k = 2$ further assume that for some prime $p \neq l$ we have*

$$\rho|_{G_p} \sim \begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}.$$

Then ρ occurs in the l-adic cohomology (with coefficients in some Tate twist of the constant sheaf) of some variety over $\mathbb{Q}$.

Again we actually show that $L(i\rho, s)$ is a ratio of products of the L-functions associated to Hilbert modular forms over different subfields of F. (See section 6 for more details.)

For further discussion of the background to these results and for a sketch of the arguments we use we refer the reader to the introduction of [Tay4].

The first three sections of this paper are taken up generalising results of Wiles [W2] and of Wiles and the author [TW] to totally real fields. Previous work along these lines has been undertaken by Fujiwara [Fu] (unpublished) and Skinner and Wiles [SW2]. However the generalisation we need is not available in the literature, so we give the necessary arguments here. We claim no great originality, this is mostly a technical exercise. We hope, however, that other authors may find theorems 2.6, 3.2 and 3.3 of some use.

In the fourth and fifth sections we generalise some of our results from [Tay4] about a potential version of Serre's conjecture. This is the most original part of this paper. The main result is theorem 5.7. Finally in section six we combine theorems 3.3 and 5.7 to deduce the main results of this paper which we have summarised above.

We would like to apologise for the long delay in submitting this paper (initially made available on the web in 2001) for publication. We would also like to thank the referee for reading the paper very carefully and making several useful suggestions.

Notation

Throughout this paper l will denote a rational prime, usually assumed to be odd and often assumed to be > 3.

If K is a perfect field we will let K^{ac} denote its algebraic closure and G_K denote its absolute Galois group $\mathrm{Gal}\,(K^{ac}/K)$. If moreover p is a prime number different from the characteristic of K then we will let $\epsilon_p : G_K \to \mathbb{Z}_p^\times$ denote the p-adic cyclotomic character and ω_p the Teichmüller lift of $\epsilon_p \bmod p$. In the case $p = l$ we will drop the subscripts and write simply $\epsilon = \epsilon_l$ and $\omega = \omega_l$. We will let c denote complex conjugation on $\mathbb{C}$.

If K is an l-adic field we will let $|\ |_K$ denote the absolute value on K normalised to take uniformisers to the inverse of the cardinality of the residue field of K. We will let I_K denote the inertia subgroup of G_K, W_K denote the Weil group of K and $\mathrm{Frob}_K \in W_K/I_K$ denote an arithmetic Frobenius element. We will also let $\mathrm{Art} : K^\times \xrightarrow{\sim} W_K^{\mathrm{ab}}$ denote the Artin map normalised to take uniformisers to arithmetic Frobenius elements. Please note these unfotunate conventions. We apologise for making them. (They are inherited from [CDT].) By an n-dimensional Weil-Deligne representation of W_K over a field M we shall mean a pair (r, N) where $r : W_K \to GL_n(M)$ is a homomorphism with open kernel and where $N \in M_n(M)$ satisfies

$$r(\sigma)Nr(\sigma)^{-1} = |\mathrm{Art}^{-1}\sigma|_K^{-1}N$$

for all $\sigma \in W_K$. We call (r, N) Frobenius semi-simple if r is semi-simple. For $n \in \mathbb{Z}_{>0}$ we define a character $\omega_{K,n} : I_K \to (K^{ac})^\times$ by

$$\omega_{K,n}(\sigma) = \sigma(\sqrt[l^n-1]{l})/\sqrt[l^n-1]{l}.$$

We will often write ω_n for $\omega_{\mathbb{Q}_l,n}$. Note that $\omega_{K,1} = \omega$.

Now suppose that $K/\mathbb{Q}_l$ is a finite unramified extension, that $\mathcal{O}$ is the ring of integers of a finite extension of K with maximal ideal λ and that $2 \le k \le l-1$. Let $\mathcal{MF}_{K,\mathcal{O},k}$ denote the abelian category whose objects are finite length $\mathcal{O}_K \otimes_{\mathbb{Z}_l} \mathcal{O}$-modules D together with a distinguished submodule D^0 and $\mathrm{Frob}_K \otimes 1$-semilinear maps $\varphi_{1-k} : D \to D$ and $\varphi_0 : D^0 \to D$ such that

- $\varphi_{1-k}|_{D^0} = l^{k-1}\varphi_0$, and
- $\mathrm{Im}\,\varphi_{1-k} + \mathrm{Im}\,\varphi_0 = D$.

Also let $\mathcal{MF}_{K,\mathcal{O}/\lambda^n,k}$ denote the full subcategory of objects D with $\lambda^n D = (0)$. If D is an object of $\mathcal{MF}_{K,\mathcal{O},k}$ we define $D^*[1-k]$ by

- $D^*[1-k] = \mathrm{Hom}\,(D, \mathbb{Q}_l/\mathbb{Z}_l)$;
- $D^*[1-k]^0 = \mathrm{Hom}\,(D/D^0, \mathbb{Q}_l/\mathbb{Z}_l)$;
- $\varphi_{1-k}(f)(z) = f(l^{k-1}x + y)$, where $z = \varphi_{1-k}(x) + \varphi_0(y)$;
- $\varphi_0(f)(z) = f(x \bmod D^0)$, where $z \equiv \varphi_{1-k}(x) \bmod (\varphi_0 D^0)$.

There is a fully faithful, $\mathcal{O}$-length preserving, exact, $\mathcal{O}$-additive, covariant functor $\mathbb{M}$ from $\mathcal{MF}_{K,\mathcal{O},k}$ to the category of continuous $\mathcal{O}[G_K]$-modules with essential image closed under the formation of sub-objects. (See [FL], especially section 9. In the notation of that paper $\mathbb{M}(D) = \underline{U}_S(D^*)$, where D^* is $D^*[1-k]$ with its filtration shifted by $k-1$. The reader could also consult section 2.5 of [DDT], where the case $k=2$ and $K = \mathbb{Q}_l$ is discussed.)
If K is a number field and x is a finite place of K we will write K_x for the completion of K at x, $k(x)$ for the residue field of x, ϖ_x for a uniformiser in K_x, G_x for a decomposition group above x, I_x for the inertia subgroup of G_x, and Frob_x for an arithmetic Frobenius element in G_x/I_x. We will also let $\mathcal{O}_K$ denote the integers of K and $\mathfrak{d}_K$ the different of K. If S is a finite set of places of K we will write $K_S^\times$ for the subgroup of $K^\times$ consisting of elements which are units outside S. We will write $\mathbb{A}_K$ for the adeles of K and $||\ ||$ for $\prod_x |\ |_{F_x} : \mathbb{A}_K^\times \to \mathbb{R}^\times$. We also use Art to denote the global Artin map, normalised compatibly with our local normalisations.
We will write μ_N for the group scheme of N^{th} roots of unity. We will write $W(k)$ for the Witt vectors of k. If G is a group, H a normal subgroup of G and ρ a representation of G, then we will let ρ^H (resp. ρ_H) denote the representation of G/H on the H-invariants (resp. H-coinvariants) of ρ. We will also let ρ^{ss} denote the semisimplification of ρ, $\mathrm{ad}\,\rho$ denote the adjoint representation and $\mathrm{ad}^0\rho$ denote the kernel of the trace map from $\mathrm{ad}\,\rho$ to the trivial representation.
Suppose that A/K is an abelian variety over a perfect field K with an action of $\mathcal{O}_M$ defined over K, for some number field M. Suppose also that X is a finite torsion free $\mathcal{O}_M$-submodule. The functor on K-schemes $S \mapsto A(S) \otimes_{\mathcal{O}_M} X$ is represented by an abelian variety $A \otimes_{\mathcal{O}_M} X$. (If X is free with basis $e_1, ..., e_r$ then we can take $A \otimes_{\mathcal{O}_M} X = A^r$. Note that for any ideal $\mathfrak{a}$ of $\mathcal{O}_M$ we then have a canonical isomorphism

$$(A \otimes_{\mathcal{O}_M} X)[\mathfrak{a}] \cong A[\mathfrak{a}] \otimes_{\mathcal{O}_M} X.$$

In general if $Y \supset X \supset \mathfrak{a}Y$ with Y free and $\mathfrak{a}$ a non-zero principal ideal of $\mathcal{O}_M$ prime to the characteristic of K then we can take

$$(A \otimes_{\mathcal{O}_M} X) = (A \otimes_{\mathcal{O}_M} \mathfrak{a}Y)/(A[\mathfrak{a}] \otimes_{\mathcal{O}_M} X/\mathfrak{a}Y).)$$

Again we get an identification

$$(A \otimes_{\mathcal{O}_M} X)[\mathfrak{a}] \cong A[\mathfrak{a}] \otimes_{\mathcal{O}_M} X.$$

If X has an action of some $\mathcal{O}_M$ algebra then $A \otimes_{\mathcal{O}_M} X$ canonically inherits such an action. We also get a canonical identification $(A \otimes_{\mathcal{O}_M} X)^\vee \cong A^\vee \otimes_{\mathcal{O}_M}$

$\mathrm{Hom}\,(X, \mathcal{O}_M)$. Suppose that $\mu : A \to A^\vee$ is a polarisation which induces an involution c on M. Note that c equals complex conjugation for every embedding $M \hookrightarrow \mathbb{C}$. Suppose also that $f : X \to \mathrm{Hom}_{\mathcal{O}_M}(X, \mathcal{O}_M)$ is c-semilinear. If for all $x \in X - \{0\}$, the totally real number $f(x)(x)$ is totally strictly positive then $\mu \otimes f : A \otimes_{\mathcal{O}_M} X \to (A \otimes_{\mathcal{O}_M} X)^\vee$ is again a polarisation which induces c on M.

If λ is an ideal of $\mathcal{O}_M$ prime to the characteristic of K we will write $\overline{\rho}_{A,\lambda}$ for the representation of G_K on $A[\lambda](K^{ac})$. If λ is prime we will write $T_\lambda A$ for the λ-adic Tate module of A, $V_\lambda A$ for $T_\lambda A \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\rho_{A,\lambda}$ for the representation of G_K on $V_\lambda A$. We have a canonical isomorphism $T_\lambda(A \otimes_{\mathcal{O}_M} X) \xrightarrow{\sim} (T_\lambda A) \otimes_{\mathcal{O}_M} X$.

Suppose that M is a totally real field. By an ordered invertible $\mathcal{O}_M$-module we shall mean an invertible $\mathcal{O}_M$-module X together with a choice of connected component X_x^+ of $(X \otimes M_x) - \{0\}$ for each infinite place x of M. If $\mathfrak{a}$ is a fractional ideal in M then we will denote by $\mathfrak{a}^+$ the invertible ordered $\mathcal{O}_M$-module $(\mathfrak{a}, \{(M_x^\times)^0\})$, where $(M_x^\times)^0$ denotes the connected component of 1 in $M_x^\times$. By an M-HBAV ('Hilbert-Blumenthal abelian variety') over a field K we shall mean a triple (A, i, j) where

- A/K is an abelian variety of dimension $[M : \mathbb{Q}]$,
- $i : \mathcal{O}_M \hookrightarrow \mathrm{End}\,(A/K)$
- and $j : (\mathfrak{d}_M^{-1})^+ \xrightarrow{\sim} \mathcal{P}(A, i)$ is an isomorphism of ordered invertible $\mathcal{O}_M$-modules.

Here $\mathcal{P}(A, i)$ is the invertible $\mathcal{O}_M$ module of symmetric (i.e. $f^\vee = f$) homomorphisms $f : (A, i) \to (A^\vee, i^\vee)$ which is ordered by taking the unique connected component of $(\mathcal{P}(A, i) \otimes M_x)$ which contains the class of a polarisation. (See section 1 of [Rap].)

If λ is a prime of M and if $x \in \mathfrak{d}_M^{-1}$ then $j(x) : A \to A^\vee$ gives rise to an alternating pairing

$$e_{j,x,0} : T_\lambda A \times T_\lambda A \longrightarrow \mathbb{Z}_l(1).$$

This corresponds to a unique $\mathcal{O}_{M,\lambda}$-bilinear alternating pairing

$$e_{j,x} : T_\lambda A \times T_\lambda A \longrightarrow \mathfrak{d}_{M,\lambda}^{-1}(1),$$

which are related by $e_{j,x,0} = \mathrm{tr} \circ e_{j,x}$. The pairing $x^{-1} e_{j,x}$ is independent of x and gives a perfect $\mathcal{O}_{M,\lambda}$-bilinear alternating pairing

$$e_j : T_\lambda A \times T_\lambda A \longrightarrow \mathcal{O}_{M,\lambda}(1),$$

which we will call the j-Weil pairing. (See section 1 of [Rap].) Again using the trace, we can think of e_j as an $\mathcal{O}_{M,\lambda}$-linear isomorphism

$$\widetilde{e}_j : T_\lambda A \otimes \mathfrak{d}_M^{-1} \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_\lambda A, \mathbb{Z}_l(1)).$$

More precisely

$$\widetilde{e}_j(a \otimes y)(b) = \mathrm{tr}\,(y e_j(a, b)) = e_{j,x,0}(x^{-1} y a, b).$$

The same formula (for $x \in \mathfrak{d}_M^{-1} - \mathfrak{a}\mathfrak{d}_M^{-1}$) gives rise to an $\mathcal{O}_{M,\lambda}$-linear isomorphism

$$\widetilde{e}_j : A[\mathfrak{a}] \otimes_{\mathcal{O}_M} \mathfrak{d}_M^{-1} \longrightarrow A[\mathfrak{a}]^\vee,$$

which is independent of x and which we will refer to as the j-Weil pairing on $A[\mathfrak{a}]$.

Suppose that F is a totally real number field and that π is an algebraic (see for instance [Cl]) cuspidal automorphic representation of $GL_2(\mathbb{A}_F)$ with field of definition (or coefficients) $M \subset \mathbb{C}$. (That is M is the fixed field of the group of automorphisms σ of $\mathbb{C}$ with $\sigma\pi^\infty = \pi^\infty$. By the strong multiplicity one theorem this is the same as the fixed field of the group of automorphisms σ of $\mathbb{C}$ with $\sigma\pi_x \cong \pi_x$ for all but finitely many places x of F.) We will say that π_∞ has weight $(\vec{k}, \vec{w}) \in \mathbb{Z}_{>0}^{\mathrm{Hom}\,(F,\mathbb{R})} \times \mathbb{Z}^{\mathrm{Hom}\,(F,\mathbb{R})}$ if for each infinite place $\tau : F \hookrightarrow \mathbb{R}$ the representation π_τ is the $(k_\tau - 1)^{st}$ lowest discrete series representation of $GL_2(F_x) \cong GL_2(\mathbb{R})$ (or in the case $k_\tau = 1$ the limit of discrete series representation) with central character $a \mapsto a^{2-k_\tau-2w_\tau}$. Note that $w = k_\tau + 2w_\tau$ must be independent of τ. If π_∞ has weight $((k,...,k),(0,...,0))$ we will simply say that it has weight k. In some cases, including the cases that π_∞ is regular (i.e. $k_\tau > 1$ for all τ) and the case π_∞ has weight 1, it is known that M is a CM number field and that for each rational prime l and each embedding $\lambda : M \hookrightarrow \mathbb{Q}_l^{ac}$ there is a continuous irreducible representation

$$\rho_{\pi,\lambda} : G_F \to GL_2(M_\lambda)$$

canonically associated to π. For any prime x of F not dividing l the restriction $\rho_{\pi,\lambda}|_{G_x}$ depends up to Frobenius semi-simplification only on π_x (and λ). (See [Tay1] for details. To see that M is a CM field one uses the Peterssen inner product

$$(f_1, f_2) = \int_{GL_2(F)(\mathbb{R}_{>0}^\times)^{\mathrm{Hom}\,(F,\mathbb{R})}} f_1(g)^c(f_2(g))|| \det g||^{w-2} dg.$$

For all $\sigma \in \mathrm{Aut}\,(\mathbb{C})$ the representation ${}^\sigma\pi^\infty$ extends to an algebraic automorphic representation $\pi(\sigma)$ of $GL_2(\mathbb{A}_F)$ with the same value for w. The pairing $(\ ,\ )$ gives an isomorphism ${}^c\pi(\sigma) \cong \pi(\sigma)^\vee || \det ||^{2-w}$. Thus ${}^{\sigma^{-1}c\sigma}\pi^\infty$ is independent of σ and M is a CM field.) We will write $\rho_{\pi,\lambda}|_{W_{F_x}}^{ss} = \mathrm{WD}_\lambda(\pi_x)$, where $\mathrm{WD}_\lambda(\pi_x)$ is a semi-simple two-dimensional representation of W_{F_x}. If π_x is unramified then $\mathrm{WD}_\lambda(\pi_x)$ is also unramified and $\mathrm{WD}_\lambda(\pi_x)(\mathrm{Frob}_x)$ has characteristic polynomial

$$X^2 - t_x X + (\mathrm{N}x)s_x$$

where t_x (resp. s_x) is the eigenvalue of

$$\left[GL_2(\mathcal{O}_{F_x}) \begin{pmatrix} \varpi_x & 0 \\ 0 & 1 \end{pmatrix} GL_2(\mathcal{O}_{F_x}) \right]$$

(resp. of

$$\left[GL_2(\mathcal{O}_{F_x})\begin{pmatrix} \varpi_x & 0 \\ 0 & \varpi_x \end{pmatrix} GL_2(\mathcal{O}_{F_x})\right])$$

on $\pi_x^{GL_2(\mathcal{O}_{F_x})}$. An explicit description of some other instances of $\mathrm{WD}_\lambda(\pi_x)$ may be found in section 4 of [CDT].

We may always conjugate $\rho_{\pi,\lambda}$ so that it is valued in $GL_2(\mathcal{O}_{M,\lambda})$ and then reduce it to get a continuous representation $G_F \to GL_2(\mathbb{F}_l^{ac})$. If for one such choice of conjugate the resulting representation is irreducible then it is independent of the choice of conjugate and we will denote it $\overline{\rho}_{\pi,\lambda}$.

1 l-adic modular forms on definite quaternion algebras

In this section we will establish some notation and recall some facts about l-adic modular forms on some definite quaternion algebras.

To this end, fix a prime $l > 3$ and a totally real field F of even degree in which l is unramified. Let D denote the division algebra with centre F which ramifies exactly at the set of infinite places of F. Fix a maximal order $\mathcal{O}_D$ in D and isomorphisms $\mathcal{O}_{D,x} \cong M_2(\mathcal{O}_{F,x})$ for all finite places x of F. These choices allow us to identify $GL_2(\mathbb{A}_F^\infty)$ with $(D \otimes_{\mathbb{Q}} \mathbb{A}^\infty)^\times$. For each finite place x of F also fix a uniformiser ϖ_x of $\mathcal{O}_{F,x}$. Also let A be a topological $\mathbb{Z}_l$-algebra which is either an algebraic extension of $\mathbb{Q}_l$, the ring of integers in such an extension or a quotient of such a ring of integers.

Let $U = \prod_x U_x$ be an open compact subgroup of $GL_2(\mathbb{A}_F^\infty)$ and let $\psi : (\mathbb{A}_F^\infty)^\times/F^\times \to A^\times$ be a continuous character. Also let $\tau : U_l \to \mathrm{Aut}\,(W_\tau)$ be a continuous representation of U_l on a finite A-module W_τ such that

$$\tau|_{U_l \cap \mathcal{O}_{F,l}^\times} = \psi|_{U_l \cap \mathcal{O}_{F,l}^\times}^{-1}.$$

We will write $W_{\tau,\psi}$ for W_τ when we want to think of it as a $U(\mathbb{A}_F^\infty)^\times$-module with U acting via τ and $(\mathbb{A}_F^\infty)^\times$ by ψ^{-1}.

We define $S_{\tau,\psi}(U)$ to be the space of continuous functions

$$f : D^\times \backslash GL_2(\mathbb{A}_F^\infty) \longrightarrow W_\tau$$

such that

- $f(gu) = \tau(u_l)^{-1} f(g)$ for all $g \in GL_2(\mathbb{A}_F^\infty)$ and all $u \in U$, and
- $f(gz) = \psi(z) f(g)$ for all $g \in GL_2(\mathbb{A}_F^\infty)$ and all $z \in (\mathbb{A}_F^\infty)^\times$.

If

$$GL_2(\mathbb{A}_F^\infty) = \coprod_i D^\times t_i U(\mathbb{A}_F^\infty)^\times$$

then

$$\begin{array}{ccc} S_{\tau,\psi}(U) & \xrightarrow{\sim} & \bigoplus_i W_{\tau,\psi}^{(U(\mathbb{A}_F^\infty)^\times \cap t_i^{-1} D^\times t_i)/F^\times} \\ f & \longmapsto & (f(t_i))_i. \end{array}$$

The index set over which i runs is finite.

Lemma 1.1 *Each group $(U(\mathbb{A}_F^\infty)^\times \cap t_i^{-1}D^\times t_i)/F^\times$ is finite and, as we are assuming $l > 3$ and l is unramified in F, the order of $(U(\mathbb{A}_F^\infty)^\times \cap t_i^{-1}D^\times t_i)/F^\times$ is not divisible by l.*

Proof: Set $V = \prod_{x \not| \infty} \mathcal{O}_{F,x}^\times$. Then we have exact sequences

$$(0) \longrightarrow (UV \cap t_i^{-1}D^{\det=1}t_i)/\{\pm 1\} \longrightarrow (U(\mathbb{A}_F^\infty)^\times \cap t_i^{-1}D^\times t_i)/F^\times \longrightarrow \\ (((\mathbb{A}_F^\infty)^\times)^2 V \cap F^\times)/(F^\times)^2$$

and

$$(0) \longrightarrow \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^2 \longrightarrow (((\mathbb{A}_F^\infty)^\times)^2 V \cap F^\times)/(F^\times)^2 \longrightarrow H[2] \longrightarrow (0),$$

where H denotes the class group of $\mathcal{O}_F$. We see that $(((\mathbb{A}_F^\infty)^\times)^2 V \cap F^\times)/(F^\times)^2$ is finite of 2-power order. Moreover $UV \cap t_i^{-1}D^{\det=1}t_i$ is finite. For $l > 3$ and l unramified in F, $D^\times$ and hence $UV \cap t_i^{-1}D^{\det=1}t_i$ contain no elements of order exactly l. The lemma follows. □

Corollary 1.2 *If B is an A-algebra then*

$$S_{\tau,\psi}(U) \otimes_A B \xrightarrow{\sim} S_{\tau \otimes_A B,\psi}(U).$$

If $x \not| l$, or if $x|l$ but $\tau|_{U_x} = 1$, then the Hecke algebra $A[U_x \backslash GL_2(F_x)/U_x]$ acts on $S_{\tau,\psi}(U)$. Explicitly, if

$$U_x h U_x = \coprod_i h_i U_x$$

then

$$([U_x h U_x]f)(g) = \sum_i f(gh_i).$$

Let U_0 denote $\prod_x GL_2(\mathcal{O}_{F,x})$. Now suppose that $\mathfrak{n}$ is an ideal of $\mathcal{O}_F$ and that, for each finite place x of F diving $\mathfrak{n}$, H_x is a quotient of $(\mathcal{O}_{F,x}/\mathfrak{n}_x)^\times$. Then we will write H for $\prod_{x|\mathfrak{n}} H_x$ and we will let $U_H(\mathfrak{n}) = \prod_x U_H(\mathfrak{n})_x$ denote the open subgroup of $GL_2(\mathbb{A}_F^\infty)$ defined by setting $U_H(\mathfrak{n})_x$ to be the subgroup of $GL_2(\mathcal{O}_{F,x})$ consisting of elements

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $c \in \mathfrak{n}_x$ and, in the case $x|\mathfrak{n}$, with ad^{-1} mapping to 1 in H_x.
If $x \not| l\mathfrak{n}$ then we will let T_x denote the Hecke operator

$$\left[U_H(\mathfrak{n}) \begin{pmatrix} \varpi_x & 0 \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n}) \right]$$

and S_x the Hecke operator

$$\left[U_H(\mathfrak{n}) \begin{pmatrix} \varpi_x & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n}) \right].$$

If $x|\mathfrak{n}$ and, either $x\not| l$ or $x|l$ but $\tau|_{U_H(\mathfrak{n})} = 1$, then we will set

$$\langle h \rangle = \left[U_H(\mathfrak{n}) \begin{pmatrix} \widetilde{h} & 0 \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n}) \right]$$

for $h \in H_x$ and $\widetilde{h}$ a lift of h to $\mathcal{O}_{F,x}^\times$; and

$$\mathbf{U}_{\varpi_x} = \left[U_H(\mathfrak{n}) \begin{pmatrix} \varpi_x & 0 \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n}) \right];$$

and

$$\mathbf{V}_{\varpi_x} = \left[U_H(\mathfrak{n}) \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n}) \right];$$

and

$$S_{\varpi_x} = \left[U_H(\mathfrak{n}) \begin{pmatrix} \varpi_x & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n}) \right].$$

For $x|\mathfrak{n}$ we note the decompositions

$$U_H(\mathfrak{n})_x \begin{pmatrix} \varpi_x & 0 \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n})_x = \coprod_{a \in k(x)} \begin{pmatrix} \varpi_x & \widetilde{a} \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n})_x,$$

and

$$U_H(\mathfrak{n})_x \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n})_x = \coprod_{a \in k(x)} \begin{pmatrix} \varpi_x & 0 \\ \varpi_x \widetilde{a} & 1 \end{pmatrix} U_H(\mathfrak{n})_x$$

and

$$U_H(\mathfrak{n})_x \begin{pmatrix} \varpi_x & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n})_x = \begin{pmatrix} \varpi_x & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n})_x,$$

where $\widetilde{a}$ is some lift of a to $\mathcal{O}_{F,x}$.

We will let $h_{\tau,A,\psi}(U_H(\mathfrak{n}))$ denote the A-subalgebra of $\mathrm{End}\,_A(S_{\tau,\psi}(U_H(\mathfrak{n})))$ generated by T_x for $x\not|l\mathfrak{n}$ and by $\mathbf{U}_{\varpi_x}$ for $x|\mathfrak{n}$ but $x\not| l$. It is commutative. We will call a maximal ideal $\mathfrak{m}$ of $h_{\tau,A,\psi}(U_H(\mathfrak{n}))$ *Eisenstein* if it contains $T_x - 2$ and $S_x - 1$ for all but finitely many primes x of F which split completely in some finite abelian extension of F. (The following remark may help explain the form of this definition. If $\overline{\rho} : G_F \to GL_2(\overline{\mathbb{F}}_l)$ is a continuous reducible representation, then there is a finite abelian extension L/F such that $\mathrm{tr}\,\overline{\rho}(G_L) = \{2\}$ and $(\epsilon_l^{-1} \det \overline{\rho})(G_L) = \{1\}$.)

For $k \in \mathbb{Z}_{\geq 2}$ and we will let $\mathrm{Symm}\,^{k-2}(A^2)$ denote the space of homogeneous polynomials of degree $k-2$ in two variables X and Y over A with a $GL_2(A)$-action via

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} f \right)(X,Y) = f\left((X,Y) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = f(aX + cY, bX + dY).$$

Let A be an $\mathcal{O}_L$ algebra for some extension $L/\mathbb{Q}_l$ containing the images of all embeddings $F \hookrightarrow \mathbb{Q}_l^{ac}$. Suppose that $(\vec{k}, \vec{w}) \in \mathbb{Z}_{>1}^{\mathrm{Hom}\,(F,\mathbb{Q}_l^{ac})} \times \mathbb{Z}^{\mathrm{Hom}\,(F,\mathbb{Q}_l^{ac})}$ is such that $k_\sigma + 2w_\sigma$ is independent of σ. We will write $\tau_{(\vec{k},\vec{w}),A}$ for the representation of $GL_2(\mathcal{O}_{F,l})$ on $W_{(\vec{k},\vec{w}),A} = \bigotimes_{\sigma: F\rightarrow \mathbb{Q}_l^{ac}} \mathrm{Symm}^{k_\sigma - 2}(A^2)$ via

$$g \longmapsto \otimes_{\sigma:F\rightarrow\mathbb{Q}_l^{ac}} (\mathrm{Symm}^{k_\sigma-2}(\sigma g) \otimes \det{}^{w_\sigma}(\sigma g)).$$

We will also write $S_{(\vec{k},\vec{w}),A,\psi}(U)$ for $S_{\tau_{(\vec{k},\vec{w}),A},\psi}(U)$. Let $S^{\mathrm{triv}}_{(\vec{k},\vec{w}),A,\psi}(U)$ denote (0) unless $(\vec{k},\vec{w}) = ((2,...,2),(w,...,w))$, in which case let it denote the subspace of $S_{(\vec{k},\vec{w}),A,\psi}(U)$ consisting of functions f which factor through the reduced norm. Set

$$S_{(\vec{k},\vec{w}),A,\psi}(U_l) = \lim_{\rightarrow U^l} S_{(\vec{k},\vec{w}),A,\psi}(U^l \times U_l).$$

It has a smooth action of $GL_2(\mathbb{A}_F^{\infty,l})$ (by right translation). If $(\vec{k},\vec{w}) = ((k,...,k),(0,...,0))$ then we will often write k in place of $(\vec{k},\vec{w})$. Set

$$S_{2,A,\psi} = \lim_{\rightarrow U} S_{2,A,\psi}(U)$$

and

$$S^{\mathrm{triv}}_{2,A,\psi} = \lim_{\rightarrow U} S^{\mathrm{triv}}_{2,A,\psi}(U).$$

They have smooth actions of $GL_2(\mathbb{A}_F^\infty)$.

Lemma 1.3 *Suppose that $(\vec{k},\vec{w}) \in \mathbb{Z}_{>1}^{\mathrm{Hom}\,(F,\mathbb{Q}_l^{ac})} \times \mathbb{Z}^{\mathrm{Hom}\,(F,\mathbb{Q}_l^{ac})}$ and $w = k_\sigma - 1 + 2w_\sigma$ is independent of σ. Also suppose that $\psi : \mathbb{A}_F^\times/F^\times \rightarrow (\mathbb{Q}_l^{ac})^\times$ is a continuous character satisfying $\psi(a) = (\mathrm{N}a)^{1-w}$ for all a in a non-empty open subgroup of $F_l^\times$. Choose an isomorphism $i : \mathbb{Q}_l^{ac} \xrightarrow{\sim} \mathbb{C}$. Define $i(\vec{k},\vec{w}) = (i\vec{k}, i\vec{w}) \in \mathbb{Z}_{>1}^{\mathrm{Hom}\,(F,\mathbb{C})} \times \mathbb{Z}^{\mathrm{Hom}\,(F,\mathbb{C})}$ by $(i\vec{k})_\tau = \vec{k}_{i^{-1}\tau}$ and $(i\vec{w})_\tau = \vec{w}_{i^{-1}\tau}$. Also define $\psi_i : \mathbb{A}_F^\times/F^\times \rightarrow \mathbb{C}^\times$ by $\psi_i(z) = i((\mathrm{N}z_l)^{w-1}\psi(z^\infty))(\mathrm{N}z_\infty)^{1-w}$. Then we have the following assertions.*

1. *$S_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac},\psi}(U_l)$ is a semi-simple admissible representation of $GL_2(\mathbb{A}_F^{\infty,l})$ and $S_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac},\psi}(U_l)^{U^l} = S_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac},\psi}(U_l \times U^l)$.*

2. *There is an isomorphism*

$$(S_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac},\psi}(U_l)/S^{\mathrm{triv}}_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac},\psi}(U_l)) \otimes_{\mathbb{Q}_l^{ac},i} \mathbb{C} \cong \bigoplus_\pi \pi^{\infty,l} \otimes \pi_l^{U_l}$$

   where π runs over regular algebraic cuspidal automorphic representations of $GL_2(\mathbb{A}_F)$ such that π_∞ has weight $(\vec{k},\vec{w})$ and such that π has central character ψ_i.

3. *$S_{2,\mathbb{Q}_l^{ac},\psi}$ is a semi-simple admissible representation of $GL_2(\mathbb{A}_F^\infty)$ and*

$$S^U_{2,\mathbb{Q}_l^{ac},\psi} = S_{2,\mathbb{Q}_l^{ac},\psi}(U).$$

4. There is an isomorphism

$$S_{2,\mathbb{Q}_l^{ac},\psi}\otimes_{\mathbb{Q}_l^{ac},i}\mathbb{C}\cong\bigoplus_{\chi}\mathbb{Q}_l^{ac}(\chi)\oplus\bigoplus_{\pi}\pi^{\infty}$$

where π runs over regular algebraic cuspidal automorphic representations of $GL_2(\mathbb{A}_F)$ such that π_∞ has weight 2 and such that π has central character ψ_i, and where χ runs over characters $(\mathbb{A}_F^\infty)^\times/F^\times_{>>0}\to(\mathbb{Q}_l^{ac})^\times$ with $\chi^2=\psi$.

Proof: We will explain the first two parts. The other two are similar. Let $C^\infty(D^\times\backslash(D\otimes_{\mathbb{Q}}\mathbb{A})^\times/U_l,\psi_\infty)$ denote the space of smooth functions

$$D^\times\backslash(D\otimes_{\mathbb{Q}}\mathbb{A})^\times/U_l\longrightarrow\mathbb{C}$$

which transform under $\mathbb{A}_F^\times$ by ψ_∞. Let τ_∞ denote the representation of $D_\infty^\times$ on $W_{\tau_\infty}=W_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac}}\otimes_i\mathbb{C}$ via

$$g\longmapsto\otimes_{\sigma:F\to\mathbb{Q}_l^{ac}}(\mathrm{Symm}^{k_\sigma-2}(i\sigma g)\otimes\det{}^{w_\sigma}(i\sigma g)).$$

Then there is an isomorphism

$$S_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac},\psi}(U_l)\xrightarrow{\sim}\mathrm{Hom}_{D_\infty^\times}(W_{\tau_\infty}^\vee,C^\infty(D^\times\backslash(D\otimes_{\mathbb{Q}}\mathbb{A})^\times/U_l,\psi_\infty))$$

which sends f to the map

$$y\longmapsto(g\longmapsto y(\tau_\infty(g_\infty)^{-1}\tau_{(\vec{k},\vec{w}),\mathbb{Q}_l^{ac}}(g_l)f(g^\infty))).$$

Everything now follows from the Jacquet-Langlands theorem. □

There is a pairing

$$\mathrm{Symm}^{k-2}(A^2)\times\mathrm{Symm}^{k-2}(A^2)\longrightarrow A$$

defined by

$$\langle f_1,f_2\rangle=(f_1(\partial/\partial Y,-\partial/\partial X)f_2(X,Y))|_{X=Y=0}.$$

By looking at the pairing of monomials we see that

$$\langle f_1,f_2\rangle=(-1)^k\langle f_2,f_1\rangle$$

and that if $2\leq k\leq l+1$ then this pairing is perfect. Moreover if

$$u=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in GL_2(A)$$

then

$$\begin{array}{rl}&\langle uf_1,uf_2\rangle\\=&(f_1(a\partial/\partial Y-c\partial/\partial X,b\partial/\partial Y-d\partial/\partial X)f_2(aX+cY,bX+dY))|_{X=Y=0}\\=&(f_1((\det u)\partial/\partial W,-(\det u)\partial/\partial Z)f_2(Z,W))|_{Z=W=0}\\=&(\det u)^{k-2}\langle f_1,f_2\rangle,\end{array}$$

where $Z = aX + cY$ and $W = bX + dY$. This extends to a perfect pairing $W_{(\vec{k},\vec{w}),A} \times W_{(\vec{k},\vec{w}),A} \to A$ such that

$$\langle ux, uy \rangle = (\mathrm{N} \det u)^{w-1} \langle x, y \rangle$$

for all $x, y \in W_{(\vec{k},\vec{w}),A}$ and all $u \in GL_2(\mathcal{O}_{F,l})$. Here $w = k_\sigma + 2w_\sigma - 1$, which is independent of σ.
We can define a perfect pairing $S_{k,A,\psi}(U_H(\mathfrak{n})) \times S_{k,A,\psi}(U_H(\mathfrak{n})) \to A$ by setting (f_1, f_2) equal to

$$\sum_{[x]} \langle f_1(x), f_2(x) \rangle \psi(\det x)^{-1} (\#(U_H(\mathfrak{n})(\mathbb{A}_F^\infty)^\times \cap x^{-1} D^\times x)/F^\times)^{-1},$$

where $[x]$ ranges over $D^\times \backslash (D \otimes_{\mathbb{Q}} \mathbb{A}^\infty)^\times / U_H(\mathfrak{n})(\mathbb{A}_F^\infty)^\times$. (We are using the fact that $\#(U_H(\mathfrak{n})(\mathbb{A}_F^\infty)^\times \cap x^{-1} D^\times x)/F^\times$ is prime to l.) The usual calculation shows that

$$([U_{H'}(\mathfrak{n}') g U_H(\mathfrak{n})] f_1, f_2)_{U_{H'}(\mathfrak{n}')} = \psi(\det g)(f_1, [U_H(\mathfrak{n}) g^{-1} U_{H'}(\mathfrak{n}')] f_2)_{U_H(\mathfrak{n})}.$$

Now specialise to the case that $A = \mathcal{O}$ is the ring on integers of a finite extension of $\mathbb{Q}_l$. We will write simply $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))$ for $h_{(\vec{k},\vec{w}),\mathcal{O},\psi}(U_H(\mathfrak{n}))$. It follows from lemma 1.3 and the main theorem in [Tay1] that there is a continuous representation

$$\rho : G_F \longrightarrow GL_2(h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n})) \otimes_{\mathcal{O}} \mathbb{Q}_l^{ac})$$

such that

- if $x \not| \mathfrak{n} l$ then ρ is unramified at x and $\operatorname{tr} \rho(\mathrm{Frob}_x) = T_x$; and
- $\det \rho = \epsilon(\psi \circ \mathrm{Art}^{-1})$.

From the theory of pseudo-representations (or otherwise, see [Ca2]) we deduce that if $\mathfrak{m}$ is a non-Eisenstein maximal ideal of $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))$ then ρ gives rise to a continuous representation

$$\rho_{\mathfrak{m}} : G_F \longrightarrow GL_2(h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}})$$

such that

- if $x \not| \mathfrak{n} l$ then $\rho_{\mathfrak{m}}$ is unramified at x and $\operatorname{tr} \rho_{\mathfrak{m}}(\mathrm{Frob}_x) = T_x$; and
- $\det \rho_{\mathfrak{m}} = \epsilon(\psi \circ \mathrm{Art}^{-1})$.

From the Cebotarev density theorem we see that $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ is generated by $\mathbf{U}_{\varpi_x}$ for $x | \mathfrak{n}$ but $x \not| l$ and by T_x for all but finitely many $x \not| l\mathfrak{n}$. (For let h denote the $\mathcal{O}$-subalgebra of $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ generated by $\mathbf{U}_{\varpi_x}$ for $x | \mathfrak{n}$ but

$x \not| l$ and by T_x for all but finitely many $x \not| l\mathfrak{n}$. The Cebotarev densitry theorem implies that $\operatorname{tr} \rho_{\mathfrak{m}}$ is valued in h and hence

$$T_x = \operatorname{tr} \rho_{\mathfrak{m}}(\mathrm{Frob}_x) \in h$$

for all $x \not| \mathfrak{n}l$. Thus $h = h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$.)
We will write $\overline{\rho}_{\mathfrak{m}}$ for ($\rho_{\mathfrak{m}} \bmod \mathfrak{m}$). If $\phi : h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}} \to R$ is a map of local $\mathcal{O}$-algebras then we will write ρ_ϕ for $\phi\rho_{\mathfrak{m}}$. If R is a field of characteristic l we will sometimes write $\overline{\rho}_\phi$ instead of ρ_ϕ.

Lemma 1.4 *Let $(\vec{k},\vec{w})$ be as above. Suppose that $x \not| \mathfrak{n}$ is a split place of F above l such that $2 \le k_x \le l-1$. If $\mathfrak{m}$ is a non-Eisenstein maximal ideal of $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))$ and if I is an open ideal of $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ (for the l-adic topology) then $((\rho_{\mathfrak{m}} \otimes \epsilon^{-w_x}) \bmod I)|_{G_x}$ is of the form $\mathbb{M}(D)$ for some object D of $\mathcal{MF}_{F_x,\mathcal{O},k_x}$ with $D \neq D^0 \neq (0)$.*

Proof: Combining the construction of $\rho_{\mathfrak{m}}$ with the basic properties of $\mathbb{M}$ listed in the section of notation, we see that it suffices to prove the following.
Suppose that π is a cuspidal automorphic representation of $GL_2(\mathbb{A}_F)$ such that π_∞ is regular algebraic of weight $(\vec{k},\vec{w})$. Let M denote the field of definition of π. Suppose that x is a split place of F above l with π_x unramified. Let M^{ac} denote the algebraic closure of M in $\mathbb{C}$ and fix an embedding $\lambda : M^{ac} \hookrightarrow \mathbb{Q}_l^{ac}$. Let $\tau : F \hookrightarrow M^{ac}$ be the embedding so that $\lambda \circ \tau$ gives rise to x. Suppose that $2 \le k_\tau \le l-1$. If I is a power of the prime of $\mathcal{O}_M$ induced by λ, then $(\rho_{\pi,\lambda} \otimes \epsilon^{-w_\tau})|_{G_x} \bmod I$ is of the form $\mathbb{M}(D)$ for some object D of $\mathcal{MF}_{F_x,\mathcal{O}_{M,\lambda},k_\tau}$ with $D \neq D^0 \neq (0)$.
By the construction of $\rho_{\pi,\lambda}$ in [Tay1], our assumption that ($\rho_{\pi,\lambda} \bmod \lambda$) is irreducible, and the basic properties of $\mathbb{M}$, we see that it suffices to treat the case that π_y is discrete series for some finite place y (cf [Tay2]). Because $2 \le k_\tau \le l-1$, it follows from [FL] that we need only show that $\rho_{\pi,\lambda}$ is crystalline with Hodge-Tate numbers $-w_\tau$ and $1-k_\tau-w_\tau$. In the case π_y is discrete series for some finite place y this presumably follows from Carayol's construction of $\rho_{\pi,\lambda}$ [Ca1] and Faltings theory [Fa], but for a definite reference we refer the reader to theorem VII.1.9 of [HT] (but note the different, more sensible, conventions in force in that paper). □

Corollary 1.5 *Suppose that $x \not| \mathfrak{n}$ is a split place of F. Suppose that $(\vec{k},\vec{w})$ is as above and that $2 \le k_x \le l-1$. If $\mathfrak{m}$ is a non-Eisenstein maximal ideal of $h_{(\vec{k},\vec{w}),\psi}(U_H(\mathfrak{n}))$ then $\overline{\rho}_{\mathfrak{m}}|_{I_x} \sim \omega_2^{k_x-1+(l+1)w_x} \oplus \omega_2^{l(k_x-1)+(l+1)w_x}$ or*

$$\begin{pmatrix} \omega^{k_x+w_x-1} & * \\ 0 & \omega^{w_x} \end{pmatrix}.$$

Proof: This follows easilly from the above lemma together with theorem 5.3, proposition 7.8 and theorem 8.4 of [FL]. □

The following lemma is well known.

Lemma 1.6 *Suppose that x is a finite place of F and that π is an irreducible admissible representation of $GL_2(F)$. If χ_1 and χ_2 are two characters of $F^\times$, let $\pi(\chi_1, \chi_2)$ denote the induced representation consisting of locally constant functions $GL_2(F) \to \mathbb{C}$ such that*

$$f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g\right) = \chi_1(a)\chi_2(b)|a/b|_x^{1/2} f(g)$$

(with $GL_2(F)$-action by right translation). Let U_1 (resp. U_2) denote the subgroup of elements in $GL_2(\mathcal{O}_{F,x})$ which are congruent to a matrix of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod (\varpi_x)$$

(resp.

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod (\varpi_x^2)).$$

1. *If $\pi^{U_1} \neq (0)$ then π is a subquotient of some $\pi(\chi_1, \chi_2)$ where the conductors of χ_1 and χ_2 are ≤ 1.*

2. *If the conductors of χ_1 and χ_2 are ≤ 1 then*

$$\pi(\chi_1, \chi_2)^{U_1}$$

is two dimensional with a basis e_1, e_2 such that

$$\mathbf{U}_{\varpi_x} e_i = (\mathrm{N}x)^{1/2} \chi_i(\varpi_x) e_i$$

and

$$\langle h \rangle e_i = \chi_i(h) e_i$$

for $h \in (\mathcal{O}_{F,x}/x)^\times$.

3. *If $\pi^{U_2} \neq (0)$ then π is either cuspidal or a subquotient of some $\pi(\chi_1, \chi_2)$ where the conductors of χ_1 and χ_2 are equal and ≤ 1.*

4. *If π is cuspidal then $\dim \pi^{U_2} \leq 1$ and $\mathbf{U}_{\varpi_x}$ acts as zero on π^{U_2}.*

5. *If χ_1 and χ_2 have conductor 1 then $\pi(\chi_1, \chi_2)^{U_2}$ is one dimensional and $\mathbf{U}_{\varpi_x}$ acts on it as 0.*

6. *If χ_1 and χ_2 have conductor 0 then $\pi(\chi_1, \chi_2)^{U_2}$ is three dimensional and $\mathbf{U}_{\varpi_x}$ acts on it with characteristic polynomial*

$$X(X - (\mathrm{N}x)^{1/2} \chi_1(\varpi_x))(X - (\mathrm{N}x)^{1/2} \chi_2(\varpi_x)).$$

As a consequence we have the following lemma.

Lemma 1.7 *Suppose that $\xi : h_{k,\psi}(U_H(\mathfrak{n}))_\mathfrak{m} \to \mathbb{Q}_l^{ac}$ and that $x \not| l$.*

1. *If $x(\mathfrak{n}) = 1$ and if ξ' is any extension of ξ to the subalgebra of* $\mathrm{End}\,(S_{k,\mathcal{O},\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}})$ *generated by $h_{k,\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ and $\langle h \rangle$ for $h \in H$, then*
$$\xi(\rho_{\mathfrak{m}})|_{G_x} \sim \begin{pmatrix} * & * \\ 0 & \chi_x \end{pmatrix}$$
where $\chi_x(\mathrm{Art}\,\varpi_x) = \xi(\mathbf{U}_{\varpi_x})$ and, for $u \in \mathcal{O}_{F,x}^{\times}$, we have $\chi_x(\mathrm{Art}\,u) = \xi'(\langle u \rangle)$.

2. *If $x(\mathfrak{n}) = 2$ and $H_x = \{1\}$ then either $\xi(\mathbf{U}_{\varpi_x}) = 0$ or $\xi(\mathbf{U}_{\varpi_x})$ is an eigenvalue of $\xi(\rho_{\mathfrak{m}})|_{G_x}(\sigma)$ for any $\sigma \in G_x$ lifting* Frob_x.

We also get the following corollary.

Corollary 1.8 1. *If $x \not| l$, $x(\mathfrak{n}) = 1$ and $\mathbf{U}_{\varpi_x}^2 - (\mathrm{N}x)\psi(\varpi_x) \notin \mathfrak{m}$ then*
$$\rho_{\mathfrak{m}}|_{G_x} \sim \begin{pmatrix} * & * \\ 0 & \chi_x \end{pmatrix}$$
where $\chi_x(\mathrm{Art}\,\varpi_x) = \mathbf{U}_{\varpi_x}$ and $\chi_x(\mathrm{Art}\,u) = \langle u \rangle$ for $u \in \mathcal{O}_{F,x}^{\times}$. In particular $\langle h \rangle \in h_{k,\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ for all $h \in H_x$.

2. *If $x \not| l$, $x(\mathfrak{n}) = 2$, $H_x = \{1\}$ and $\mathbf{U}_{\varpi_x} \in \mathfrak{m}$ then $\mathbf{U}_{\varpi_x} = 0$ in $h_{k,\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$.*

3. *If l is coprime to $\mathfrak{n}$ and for all $x|\mathfrak{n}$ we have $x(\mathfrak{n}) = 2$, $H_x = \{1\}$ and $\mathbf{U}_{\varpi_x} \in \mathfrak{m}$, then the algebra $h_{k,\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ is reduced.*

Proof: The first part follows from the previous lemma via a Hensel's lemma argument. For the second part one observes that by the last lemma $\xi(\mathbf{U}_{\varpi_x}) = 0$ for all $\xi : h_{k,\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}} \to \mathbb{Q}_l^{ac}$. Hence by lemma 1.6 we have that $\mathbf{U}_{\varpi_x} = 0$ on $S_{k,\mathbb{Q}_l^{ac},\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$. The third part follows from the second (because the algebra $h_{k,\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}}$ is generated by commuting semi-simple elements). □

2 Deformation rings and Hecke algebras I

In this section we extend the method of [TW] to totally real fields. This relies crucially on the improvement to the argument of [TW] found independently by Diamond [Dia] and Fujiwara (see [Fu], unpublished). Following this advance it has been clear to experts that some extension to totally real fields would be possible, the only question was the exact extent of the generalisation. Fujiwara has circulated some unpublished notes [Fu]. Then Skinner and Wiles made a rather complete analysis of the ordinary case (see [SW2]). We will treat the low weight, crystalline case. As will be clear to the reader, we have not tried to work in maximal generality, rather we treat the case of importance for this paper. We apologise for this. It would be very helpful to have these results documented in the greatest possible generality.

In this section and the next let F denote a totally real field of even degree in which a prime $l > 3$ splits completely. (As the reader will be able to check without undue difficulty it would suffice to assume that l is unramified in F.) Let D denote the quaternion algebra with centre F which is ramified at exactly the infinite places, let $\mathcal{O}_D$ denote a maximal order in D and fix isomorphisms $\mathcal{O}_{D,x} \cong M_2(\mathcal{O}_{F,x})$ for all finite places x of F. Let $2 \leq k \leq l-1$. Let $\psi : \mathbb{A}_F^\times/F^\times \to (\mathbb{Q}_l^{ac})^\times$ be a continuous character such that

- if $x \not| l$ is a prime of F then $\psi|_{\mathcal{O}_{F,x}^\times} = 1$,
- $\psi|_{\mathcal{O}_{F,l}^\times}(u) = (\mathrm{N}u)^{2-k}$.

For each finite place x of F choose a uniformiser ϖ_x of $\mathcal{O}_{F,x}$. Suppose that $\phi : h_{k,\mathbb{F}_l^{ac},\psi}(U_0) \to \mathbb{F}_l^{ac}$ is a homomorphism with non-Eisenstein kernel, which we will denote $\mathfrak{m}$. Let $\mathcal{O}$ denote the ring of integers of a finite extension $K/\mathbb{Q}_l$ with maximal ideal λ such that

- K contains the image of every embedding $F \hookrightarrow \mathbb{Q}_l^{ac}$,
- ψ is valued in $\mathcal{O}^\times$,
- there is a homomorphism $\widetilde{\phi} : h_{k,\mathcal{O},\psi}(U_0)_\mathfrak{m} \to \mathcal{O}$ lifting ϕ, and
- all the eigenvalues of all elements of the image of $\overline{\rho}_\phi$ are rational over $\mathcal{O}/\lambda$.

For any finite set Σ of finite places of F not dividing l we will consider the functor $\mathcal{D}_\Sigma$ from complete noetherian local $\mathcal{O}$-algebras with residue firld $\mathcal{O}/\lambda$ to sets which sends R to the set of $1_2 + M_2(\mathfrak{m}_R)$-conjugacy classes of liftings $\rho : G_F \to GL_2(R)$ of $\overline{\rho}_\phi$ such that

- ρ is unramified outside l and Σ,
- $\det \rho = \epsilon(\psi \circ \mathrm{Art}^{-1})$, and
- for each place x of F above l and for each finite length (as an $\mathcal{O}$-module) quotient R/I of R the $\mathcal{O}[G_x]$-module $(R/I)^2$ is isomorphic to $\mathbb{M}(D)$ for some object D of $\mathcal{MF}_{F_x,\mathcal{O},k}$.

This functor is represented by a universal deformation

$$\rho_\Sigma : G_F \longrightarrow GL_2(R_\Sigma).$$

(This is now very standard, see for instance appendix A of [CDT].)
Now let Σ be a finite set of finite places of F not dividing l such that if $x \in \Sigma$ then

- $\mathrm{N}x \equiv 1 \bmod l$,
- $\overline{\rho}_\phi$ is unramified at x and $\overline{\rho}_\phi(\mathrm{Frob}_x)$ has distinct eigenvalues $\alpha_x \neq \beta_x$.

By Hensel's lemma the polynomial $X^2 - T_x X + (\mathrm{N}x)\psi(\varpi_x)$ splits as $(X - A_x)(X - B_x)$ in $h_{k,\mathcal{O},\psi}(U_0)_\mathfrak{m}$, where $A_x \bmod \mathfrak{m} = \alpha_x$ and $B_x \bmod \mathfrak{m} = \beta_x$. For $x \in \Sigma$ we will let Δ_x denote the maximal l-power quotient of $(\mathcal{O}_F/x)^\times$. We will let $\mathfrak{n}_\Sigma = \prod_{x\in\Sigma} x$; $\Delta_\Sigma = \prod_{x\in\Sigma}\Delta_x$; $U_{0,\Sigma} = U_{\{1\}}(\mathfrak{n}_\Sigma)$; and $U_{1,\Sigma} = U_{\Delta_\Sigma}(\mathfrak{n}_\Sigma)$. We will let $\mathfrak{m}_\Sigma$ denote the ideal of either $h_{k,\psi}(U_{0,\Sigma})$ or $h_{k,\psi}(U_{1,\Sigma})$ generated by

- l;
- $T_x - \operatorname{tr}\overline{\rho}_\phi(\mathrm{Frob}_x)$ for $x \nmid l\mathfrak{n}_\Sigma$; and
- $\mathbf{U}_{\varpi_x} - \alpha_x$ for $x \in \Sigma$.

Lemma 2.1 *Let Σ satisfy the assumptions of the last paragraph.*

1. *If $x \in \Sigma$ then $\rho_\Sigma|_{G_x} \sim \chi_{\alpha,x} \oplus \chi_{\beta,x}$ where $\chi_{\alpha,x} \bmod \mathfrak{m}_{R_\Sigma}$ is unramified and takes Frob_x to α_x.*
2. *$\chi_{\alpha,x} \circ \mathrm{Art}\,|_{\mathcal{O}_{F,x}^\times}$ factors through Δ_x, and these maps make R_Σ into a $\mathcal{O}[\Delta_\Sigma]$-module.*
3. *The universal property of R_Σ gives rise to a surjection of $\mathcal{O}[\Delta_\Sigma]$-algebras*
$$R_\Sigma \twoheadrightarrow h_{k,\psi}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma}$$
under which ρ_Σ pushes forward to $\rho_{\mathfrak{m}_\Sigma}$.

Proof: The first part is proved in exactly the same manner as lemma 2.44 of [DDT]. The second part is then clear. The third part is clear because for $x \nmid \mathfrak{n}_\Sigma l$ we have $\operatorname{tr}\rho_\Sigma(\mathrm{Frob}_x) \mapsto T_x$ while for $x \in \Sigma$ we have $\chi_{\alpha,x}(\varpi_x) \mapsto \mathbf{U}_{\varpi_x}$. $\square$

Lemma 2.2 *The map*

$$\begin{array}{rcl} \eta : S_{k,\mathcal{O},\psi}(U_{0,\Sigma-\{x\}})_{\mathfrak{m}_{\Sigma-\{x\}}} & \longrightarrow & S_{k,\mathcal{O},\psi}(U_{0,\Sigma})_{\mathfrak{m}_\Sigma} \\ f & \longmapsto & A_x f - \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f \end{array}$$

is an isomorphism which induces an isomorphism

$$\eta^* : h_{k,\psi}(U_{0,\Sigma})_{\mathfrak{m}_\Sigma} \xrightarrow{\sim} h_{k,\psi}(U_{0,\Sigma-\{x\}})_{\mathfrak{m}_{\Sigma-\{x\}}}.$$

Proof: The map η is well defined because $\mathbf{U}_{\varpi_x} \circ \eta = \eta \circ A_x$. It is injective with torsion free cokernel because the composition of η with the adjoint of the natural inclusion $S_{k,\mathcal{O},\psi}(U_{0,\Sigma-\{x\}}) \hookrightarrow S_{k,\mathcal{O},\psi}(U_{0,\Sigma})$ is $(\mathrm{N}x)A_x - B_x \notin \mathfrak{m}_\Sigma$. As $\alpha_x/\beta_x \neq (\mathrm{N}x)^{\pm 1}$, no lift of $\overline{\rho}_\phi$ with determinant $\epsilon(\psi \circ \mathrm{Art}^{-1})$ has conductor at x exactly x. Thus

$$S_{k,\mathcal{O},\psi}(U_{0,\Sigma})_{\mathfrak{m}_\Sigma} = (S_{k,\mathcal{O},\psi}(U_{0,\Sigma-\{x\}}) + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} S_{k,\mathcal{O},\psi}(U_{0,\Sigma-\{x\}}))_{\mathfrak{m}_\Sigma}.$$

As

$$\mathbf{U}_{\varpi_x}(f_1 + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f_2) = (T_x f_1 + (\mathrm{N}x)\psi(\varpi_x) f_2) - \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f_1$$

and the matrix

$$\begin{pmatrix} T_x & (\mathrm{N}x)\psi(\varpi_x) \\ -1 & 0 \end{pmatrix}$$

has eigenvalues A_x and B_x which are distinct mod $\mathfrak{m}$, the lemma follows. □

We remark that $S_{k,\mathcal{O},\psi}(U_{1,\Sigma})$ is a Δ_Σ-module via $h \mapsto \langle h \rangle$.

Lemma 2.3 *1.* $\sum_{h\in\Delta_\Sigma} \langle h \rangle : S_{k,\mathcal{O},\psi}(U_{1,\Sigma})_{\Delta_\Sigma} \xrightarrow{\sim} S_{k,\mathcal{O},\psi}(U_{0,\Sigma})$.

2. $S_{k,\mathcal{O},\psi}(U_{1,\Sigma})$ *is a free* $\mathcal{O}[\Delta_\Sigma]$*-module.*

Proof: The second assertion follows from the first as we can compute that

$$\dim S_{k,\mathcal{O},\psi}(U_{1,\Sigma}) \otimes_{\mathcal{O}} K = [U_{0,\Sigma} : U_{1,\Sigma}] \dim S_{k,\mathcal{O},\psi}(U_{0,\Sigma}) \otimes_{\mathcal{O}} K.$$

(We use the fact that $[U_{0,\Sigma} : U_{1,\Sigma}]$ is coprime to $\#(U_{0,\Sigma}(\mathbb{A}_F^\infty)^\times \cap x^{-1}D^\times x)/F^\times$ for all $x \in (D \otimes_{\mathbb{Q}} \mathbb{A}^\infty)^\times$.)

Using the duality introduced above it suffices to check that the natural map

$$S_{k,\mathcal{O},\psi}(U_{0,\Sigma}) \otimes_{\mathcal{O}} K/\mathcal{O} \longrightarrow (S_{k,\mathcal{O},\psi}(U_{1,\Sigma}) \otimes_{\mathcal{O}} K/\mathcal{O})^{\Delta_\Sigma}$$

is an isomorphism. This is immediate from the definitions and the fact that $l \not| \#(U_{0,\Sigma}(\mathbb{A}_F^\infty)^\times \cap x^{-1}D^\times x)/F^\times$ for all $x \in (D \otimes_{\mathbb{Q}} \mathbb{A}^\infty)^\times$. □

As $S_{k,\mathcal{O},\psi}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma}$ is a direct summand of $S_{k,\mathcal{O},\psi}(U_{1,\Sigma})$, we deduce the following corollary.

Corollary 2.4 *1.* $S_{k,\mathcal{O},\psi}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma,\Delta_\Sigma} \xrightarrow{\sim} S_{k,\mathcal{O},\psi}(U_0)_{\mathfrak{m}}$ *compatibly with a map* $h_{k,\psi}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma} \to h_{k,\psi}(U_0)_{\mathfrak{m}}$ *sending* T_x *to* T_x *for* $x \not| l\mathfrak{n}_\Sigma$, $\langle h \rangle$ *to* 1 *for* $h \in \Delta_\Sigma$ *and* $\mathbf{U}_{\varpi_x}$ *to* A_x *for* $x \in \Sigma$.

2. $S_{k,\mathcal{O},\psi}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma}$ *is a free* $\mathcal{O}[\Delta_\Sigma]$*-module.*

Suppose that $\rho : G_F \to GL_2(\mathcal{O}/\lambda^n)$ is a lifting of $\overline{\rho}_\phi$ corresponding to some map $R_\emptyset \to \mathcal{O}/\lambda^n$. If x is a place of F above l and if $(\mathcal{O}/\lambda^n)^2 \cong \mathbb{M}(D)$ as a G_x-module, then we set

$$H^1_f(G_x, \mathrm{ad}^0\rho) = H^1(G_x, \mathrm{ad}^0\rho) \cap \mathrm{Im}\,(\mathrm{Ext}^1_{\mathcal{MF}_{F_x,\mathcal{O}/\lambda^n,k}}(D,D) \longrightarrow H^1(G_x, \mathrm{ad}\,\rho)).$$

Exactly as in section 2.5 of [DDT] we see that

$$\mathrm{Im}\,(\mathrm{Ext}^1_{\mathcal{MF}_{F_x,\mathcal{O}/\lambda^n,k}}(D,D) \longrightarrow H^1(G_x, \mathrm{ad}\,\rho)) \cong (\mathcal{O}/\lambda^n)^2 \oplus H^0(G_x, \mathrm{ad}^0\rho).$$

If two continuous $\mathcal{O}[G_x]$-modules have the same restriction to I_x, then one is in the image of $\mathbb{M}$ if and only if the other is. We conclude that the image of the composite

$$\mathrm{Ext}^1_{\mathcal{MF}_{\mathcal{O}/\lambda^n,k}}(D,D) \longrightarrow H^1(G_x, \mathrm{ad}\,\rho) \xrightarrow{\mathrm{tr}} H^1(G_x, \mathcal{O}/\lambda^n)$$

is at least one dimensional (coming from unramified twists) and hence that

$$\# H^1_f(G_x, \operatorname{ad}^0 \overline{\rho}_\phi) | \#(\mathcal{O}/\lambda^n) \# H^0(G_x, \operatorname{ad}^0 \overline{\rho}_\phi).$$

We will let $H^1_\Sigma(G_F, \operatorname{ad}^0 \rho)$ denote the kernel of the map

$$H^1(G_F, \operatorname{ad}^0 \rho) \longrightarrow \bigoplus_{x \not| \mathfrak{n}_\Sigma l} H^1(I_x, \operatorname{ad}^0 \rho) \oplus \bigoplus_{x|l} H^1(G_x, \operatorname{ad}^0 \rho)/H^1_f(G_x, \operatorname{ad}^0 \rho).$$

The trace pairing $(a, b) \mapsto \operatorname{tr} ab$ gives a perfect duality on $\operatorname{ad}^0 \overline{\rho}_\phi$. For $x|l$ we will let $H^1_f(G_x, \operatorname{ad}^0 \overline{\rho}_\phi(1))$ denote the annihilator in $H^1(G_x, \operatorname{ad}^0 \overline{\rho}_\phi(1))$ of $H^1_f(G_x, \operatorname{ad}^0 \overline{\rho}_\phi)$ under Tate local duality. We will also let $H^1_\Sigma(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1))$ denote the kernel of the restriction map from $H^1(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1))$ to

$$\begin{aligned} &\textstyle\bigoplus_{x \not| \mathfrak{n}_\Sigma l} H^1(I_x, \operatorname{ad}^0 \overline{\rho}_\phi(1)) \oplus \bigoplus_{x \in \Sigma} H^1(G_x, \operatorname{ad}^0 \overline{\rho}_\phi(1)) \oplus \\ &\qquad \textstyle\bigoplus_{x|l} H^1(G_x, \operatorname{ad}^0 \overline{\rho}_\phi)/H^1_f(G_x, \operatorname{ad}^0 \overline{\rho}_\phi(1))) \end{aligned}$$

so that

$$H^1_\Sigma(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1)) = \ker(H^1_\emptyset(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1)) \longrightarrow \bigoplus_{x \in \Sigma} H^1(G_x/I_x, \operatorname{ad}^0 \overline{\rho}_\phi(1))).$$

A standard calculation (see for instance section 2.7 of [DDT]) shows that

$$H^1_\Sigma(G_F, \operatorname{ad}^0 \overline{\rho}_\phi) \cong \operatorname{Hom}_{\mathcal{O}}(\mathfrak{m}_{R_\Sigma}/\mathfrak{m}^2_{R_\Sigma}, \mathcal{O}/\lambda),$$

so that R_Σ can be topologically generated by $\dim H^1_\Sigma(G_F, \operatorname{ad}^0 \overline{\rho}_\phi)$ elements as an $\mathcal{O}$-algebra. A formula of Wiles (see theorem 2.19 of [DDT]) then tells us that R_Σ can be topologically generated as an $\mathcal{O}$-algebra by

$$\#\Sigma + \dim H^1_\Sigma(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1))$$

elements.

Lemma 2.5 *Suppose that the restriction of $\overline{\rho}_\phi$ to $F(\sqrt{(-1)^{(l-1)/2} l})$ is irreducible. Then for any $m \in \mathbb{Z}_{>0}$ we can find a set Σ_m of primes such that*

1. $\#\Sigma_m = \dim H^1_\emptyset(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1))$,

2. R_{Σ_m} *can be topologically generated by* $\dim H^1_\emptyset(G_F, \operatorname{ad}^0 \overline{\rho}_\phi(1))$ *elements as an $\mathcal{O}$-algebra,*

3. *if $x \in \Sigma_m$ then $\mathrm{N}x \equiv 1 \bmod l^m$ and $\overline{\rho}_\phi(\mathrm{Frob}_x)$ has distinct eigenvalues α_x and β_x.*

Proof: By the above calculation we may replace the second requirement by the requirement that $H^1_{\Sigma_m}(G_F, \mathrm{ad}^0\overline{\rho}_\phi(1)) = (0)$ (for then R_{Σ_m} is generated by $\#\Sigma_m = \dim H^1_\emptyset(G_F, \mathrm{ad}^0\overline{\rho}_\phi(1))$ elements). Then we may suppress the first requirement, because any set satisfying the modified second requirement and the third requirement can be shrunk to one which also satisfies the first requirement. (Note that for x satisfying the third requirement $H^1(G_x/I_x, \mathrm{ad}^0\overline{\rho}_\phi(1))$ is one dimensional.) Next, by the Cebotarev density theorem, it suffices to show that for $[\gamma] \in H^1_\emptyset(G_F, \mathrm{ad}^0\overline{\rho}_\phi(1))$ we can find $\sigma \in G_F$ such that

- $\sigma|_{F(\zeta_{l^m})} = 1$,
- $\overline{\rho}_\phi(\sigma)$ has distinct eigenvalues, and
- $\gamma(\sigma) \notin (\sigma - 1)\mathrm{ad}^0\overline{\rho}_\phi$.

Let F_m denote the extension of $F(\zeta_{l^m})$ cut out by $\mathrm{ad}^0\overline{\rho}$. Finally it will suffice to show that

1. $H^1(\mathrm{Gal}\,(F_m/F), \mathrm{ad}^0\overline{\rho}(1)) = (0)$; and
2. for any non-trivial irreducible $\mathrm{Gal}\,(F_m/F)$-submodule V of $\mathrm{ad}^0\overline{\rho}_\phi$ we can find $\sigma \in \mathrm{Gal}\,(F_m/F(\zeta_{l^m}))$ such that $\mathrm{ad}^0\overline{\rho}_\phi(\sigma)$ has an eigenvalue other than 1 but σ does have an eigenvalue 1 on V.

(Given $[\gamma] \in H^1_\emptyset(G_F, \mathrm{ad}^0\overline{\rho}_\phi(1))$ the first assertion tells us that the $\mathcal{O}/\lambda$-span of γG_{F_m} contains some non-trivial irreducible $\mathrm{Gal}\,(F_m/F)$-submodule V of $\mathrm{ad}^0\overline{\rho}_\phi$. Let σ be as in the second assertion for this V. Then for some $\sigma' \in G_{F_m}$ we will have

$$\gamma(\sigma'\sigma) = \gamma(\sigma') + \gamma(\sigma) \notin (\sigma - 1)\mathrm{ad}^0\overline{\rho}_\phi.)$$

Because $l > 3$ is unramified in F, we see that $[F(\zeta_l) : F] > 2$ and so, by the argument of the penultimate paragraph of the proof of theorem 2.49 of [DDT], $H^1(\mathrm{Gal}\,(F_m/F), \mathrm{ad}^0\overline{\rho}(1)) = (0)$.

Suppose that V is an irreducible $\mathrm{Gal}\,(F_m/F)$-submodule of $\mathrm{ad}^0\overline{\rho}_\phi$ and write $\mathrm{ad}^0\overline{\rho}_\phi = V \oplus W$. If $W = (0)$ any $\sigma \in \mathrm{Gal}\,(F_m/F(\zeta_{l^m}))$ with an eigenvalue other than 1 on $\mathrm{ad}^0\overline{\rho}_\phi$ will suffice to prove the second assertion. Thus suppose that $W \neq (0)$. If $\dim W = 1$ then $\overline{\rho}_\phi$ is induced from a character of some quadratic extension E/F and any $\sigma \notin G_E$ will suffice to prove the second assertion (as E is not a subfield of $F(\zeta_{l^m})$). If $\dim W = 2$ then G_F acts on V via a quadratic character corresponding to some quadratic extension E/F and $\overline{\rho}_\phi$ is induced from some character χ of G_E. Let χ' denote the $\mathrm{Gal}\,(E/F)$-conjugate of χ. Then any $\sigma \in G_{E(\zeta_{l^m})}$ with $\chi/\chi'(\sigma) \neq 1$ will suffice to prove the second assertion. (Such a σ will exist unless the restriction of $\mathrm{ad}^0\overline{\rho}_\phi$ to $E(\sqrt{(-1)^{(l-1)/2}l})$ is trivial in which case $\overline{\rho}_\phi$ becomes reducible over $F(\sqrt{(-1)^{(l-1)/2}l})$, which we are assuming is not the case.) □

Combining lemma 2.5, corollary 2.4 and theorem 2.1 of [Dia] we obtain the following theorem.

Theorem 2.6 *Keep the notation and assumptions of the second and fourth paragraphs of this section and suppose that the restriction of $\overline{\rho}_\phi$ to the absolute Galois group of $F(\sqrt{(-1)^{(l-1)/2}l})$ is irreducible. Then the natural map*

$$R_\emptyset \longrightarrow h_{k,\psi}(U_0)_\mathfrak{m}$$

is an isomorphism of complete intersections and $S_{k,\mathcal{O},\psi}(U_0)_\mathfrak{m}$ is finite free as a $h_{k,\psi}(U_0)_\mathfrak{m}$-module.

3 Deformation rings and Hecke algebras II

In this section we use analogues of Wiles' arguments from [W2] to extend the isomorphism of theorem 2.6 from $\emptyset$ to any Σ.
We will keep the notation and assumptions of the last section. (Σ will again be *any* finite set of finite places of F not dividing l.) Let $\rho_{\widetilde{\phi}} : G_F \to GL_2(\mathcal{O})$ denote the Galois representation corresponding to $\widetilde{\phi}$ (a chosen lift of ϕ). The universal property of R_Σ gives maps

$$R_\Sigma \twoheadrightarrow R_\emptyset \xrightarrow{\widetilde{\phi}} \mathcal{O}.$$

We will denote the kernel by $\wp_\Sigma$. A standard calculation (see section 2.7 of [DDT]) shows that

$$\mathrm{Hom}_{\mathcal{O}}(\wp_\Sigma/\wp_\Sigma^2, K/\mathcal{O}) \cong H^1_\Sigma(G_F, (\mathrm{ad}^0\rho)\otimes K/\mathcal{O}),$$

where

$$H^1_\Sigma(G_F, (\mathrm{ad}^0\rho)\otimes K/\mathcal{O}) = \varinjlim_n H^1_\Sigma(G_F, (\mathrm{ad}^0\rho)\otimes \lambda^{-n}/\mathcal{O}).$$

In particular we see that

$$\#\ker(\wp_\Sigma/\wp_\Sigma^2 \twoheadrightarrow \wp_\emptyset/\wp_\emptyset^2) = \#(H^1_\Sigma(G_F,(\mathrm{ad}^0\rho)\otimes K/\mathcal{O})/H^1_\emptyset(G_F,(\mathrm{ad}^0\rho)\otimes K/\mathcal{O}))$$

divides

$$\begin{array}{rl} & \prod_{x\in\Sigma} \#H^1(I_x, (\mathrm{ad}^0\rho)\otimes K/\mathcal{O})^{G_x} \\ = & \prod_{x\in\Sigma} \#H^0(G_x, (\mathrm{ad}^0\rho)\otimes K/\mathcal{O}(-1)) \\ = & \prod_{x\in\Sigma} \#\mathcal{O}/(1-\mathrm{N}x)((1+\mathrm{N}x)^2\det\rho(\mathrm{Frob}_x) - (\mathrm{N}x)(\mathrm{tr}\,\rho\mathrm{Frob}_x))\mathcal{O}. \end{array}$$

Let $\mathfrak{n}'_\Sigma$ denote the product of the squares of the primes in Σ and set $U_\Sigma = U_{\{1\}}(\mathfrak{n}'_\Sigma)$. Let $h_\Sigma = h_{k,\psi}(U_\Sigma)_{\mathfrak{m}'_\Sigma}$ and $S_\Sigma = S_{k,\mathcal{O},\psi}(U_\Sigma)_{\mathfrak{m}'_\Sigma}$, where $\mathfrak{m}'_\Sigma$ is the maximal ideal of $h_{k,\psi}(U_\Sigma)$ generated by

- λ,
- $T_x - \mathrm{tr}\,\overline{\rho}_\phi(\mathrm{Frob}_x)$ for $x \not| l\mathfrak{n}'_\Sigma$, and

- $\mathbf{U}_{\varpi_x}$ for $x \in \Sigma$.

The Galois representation $\rho_{\mathfrak{m}'_\Sigma}$ induces a homomorphism $R_\Sigma \to h_\Sigma$ which takes $\operatorname{tr} \rho_\Sigma(\mathrm{Frob}_x)$ to T_x for all $x \not| \mathfrak{n}'_\Sigma l$. Corollary 1.8 tells us that for $x \in \Sigma$ we have $\mathbf{U}_{\varpi_x} = 0$ in h_Σ and that h_Σ is reduced. In particular the map $R_\Sigma \to h_\Sigma$ is surjective.
From lemma 1.3, lemma 1.6 and the strong multiplicity one theorem for $GL_2(\mathbb{A}_F)$ we see that $\dim(S_\Sigma \otimes_{\mathcal{O}} K)[\wp_\Sigma] = 1$.
We can write

$$S_\Sigma \otimes_{\mathcal{O}} K = (S_\Sigma \otimes_{\mathcal{O}} K)[\wp_\Sigma] \oplus (S_\Sigma \otimes_{\mathcal{O}} K)[\mathrm{Ann}_{\,h_\Sigma}(\wp_\Sigma h_\Sigma)].$$

We set

$$\Omega_\Sigma = S_\Sigma/(S_\Sigma[\wp_\Sigma] \oplus S_\Sigma[\mathrm{Ann}_{\,h_\Sigma}(\wp_\Sigma h_\Sigma)]).$$

By theorem 2.4 of [Dia] and theorem 2.6 above, we see that

$$\#\Omega_\emptyset = \#\wp_\emptyset/\wp_\emptyset^2.$$

Let $w_\Sigma \in GL_2(\mathbb{A}_F^\infty)$ be defined by $w_{\sigma,x} = 1_2$ if $x \notin \Sigma$ and

$$w_{\Sigma,x} = \begin{pmatrix} 0 & 1 \\ \varpi_x^2 & 0 \end{pmatrix}$$

if $x \in \Sigma$. Then w_Σ normalises U_Σ. We define a new pairing on $S_{k,\mathcal{O},\psi}(U_\Sigma)$ by

$$(f_1, f_2)' = (\prod_{x \in \Sigma} \psi(\varpi_x))^{-1}(f_1, w_\Sigma f_2).$$

Because $(\ ,\ )$ is a perfect pairing so is $(\ ,\ )'$. Moreover the action of any element of $h_{k,\psi}(U_\Sigma)$ is self adjoint with respect to $(\ ,\ )'$, so that $(\ ,\ )'$ restricts to a perfect pairing on S_Σ. Choose a perfect $\mathcal{O}$-bilinear pairing on $S_\Sigma[\wp_\Sigma]$, let j_Σ denote the natural inclusion

$$j_\Sigma : S_\Sigma[\wp_\Sigma] \hookrightarrow S_\Sigma,$$

and let $j_\Sigma^\dagger$ denote the adjoint of j_Σ with respect to $(\ ,\ )'$ on S_Σ and the chosen pairing on $S_\Sigma[\wp_\Sigma]$. Then one sees that

$$j_\Sigma^\dagger : \Omega_\Sigma \xrightarrow{\sim} S_\Sigma[\wp_\Sigma]/j_\Sigma^\dagger S_\Sigma[\wp_\Sigma].$$

If $x \not| l\mathfrak{n}'_\Sigma$ then define

$$i_x : S_{k,\mathcal{O},\psi}(U_\Sigma) \longrightarrow S_{k,\mathcal{O},\psi}(U_{\Sigma \cup \{x\}})$$

by

$$i_x(f) = (\mathrm{N}x)\psi(\varpi_x)f - \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} T_x f + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x^2 \end{pmatrix} f.$$

It is easy to check that i_x commutes with T_y for $y \not| l\mathfrak{n}'_{\Sigma\cup\{x\}}$ and with $\mathbf{U}_{\varpi_y}$ for $y \in \Sigma$. Moreover $\mathbf{U}_{\varpi_x} i_x = 0$ and so

$$i_x : S_\Sigma \longrightarrow S_{\Sigma\cup\{x\}}.$$

Moreover $i_x S_\Sigma[\wp_\Sigma] \subset S_{\Sigma\cup\{x\}}[\wp_{\Sigma\cup\{x\}}]$. We will let $i_x^\dagger$ denote the adjoint of i_x with respect to the pairings $(\ ,\ )'$ on S_Σ and $S_{\Sigma\cup\{x\}}$. (We warn the reader that the former is not simply the restriction of the latter.) An easy calculation shows that $i_x^\dagger$ equals

$$\psi(\varpi_x)(\mathrm{N}x)[U_\Sigma U_{\Sigma\cup\{x\}}] - T_x[U_\Sigma \begin{pmatrix} \varpi_x & 0 \\ 0 & 1 \end{pmatrix} U_{\Sigma\cup\{x\}}] + [U_\Sigma \begin{pmatrix} \varpi_x^2 & 0 \\ 0 & 1 \end{pmatrix} U_{\Sigma\cup\{x\}}]$$

and hence that

$$i_x^\dagger \circ i_x = \psi(\varpi_x)(\mathrm{N}x)(1-\mathrm{N}x)(T_x^2 - (1+\mathrm{N}x)^2\psi(\varpi_x)).$$

The following key lemma is often referred to as Ihara's lemma.

Lemma 3.1 *$S_{\Sigma\cup\{x\}}/i_x S_\Sigma$ is l-torsion free.*

Proof: It suffices to check that

$$i_x : S_{k,\mathcal{O}/\lambda,\psi}(U_\Sigma)_{\mathfrak{m}'_\Sigma} \longrightarrow S_{k,\mathcal{O}/\lambda,\psi}(U_{\Sigma\cup\{x\}})_{\mathfrak{m}'_{\Sigma\cup\{x\}}}$$

is injective, or even that the localisation at $\mathfrak{m}'_\Sigma$ of the kernel of

$$\begin{array}{rcl} S_{k,\mathcal{O}/\lambda,\psi}(U_\Sigma)^3 & \longrightarrow & S_{k,\mathcal{O}/\lambda,\psi}(U_{\Sigma\cup\{x\}}) \\ (f_1,f_2,f_3) & \longmapsto & f_1 + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f_2 + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x^2 \end{pmatrix} f_3 \end{array}$$

vanishes.
Let V denote the subgroup of elements $u \in U_\Sigma$ with

$$u_x \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod \varpi_x.$$

We see that

$$V \cap \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} V \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix}^{-1} = U_{\Sigma\cup\{x\}}$$

and that U_Σ is the subgroup of $GL_2(\mathbb{A}_F^\infty)$ generated by V and

$$\begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix}^{-1} V \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix}.$$

Thus the sequence

$$\begin{array}{ccccccc} (0) & \rightarrow & S_{k,\mathcal{O}/\lambda,\psi}(U_\Sigma) & \rightarrow & S_{k,\mathcal{O}/\lambda,\psi}(V) \oplus S_{k,\mathcal{O}/\lambda,\psi}(V) & \rightarrow & S_{k,\mathcal{O}/\lambda,\psi}(U_{\Sigma\cup\{x\}}) \\ & & f & \mapsto & (\begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f, -f) & & \\ & & & & (f_1,f_2) & \mapsto & f_1 + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f_2 \end{array}$$

is exact.

Hence it suffices to show that the localisation at $\mathfrak{m}'_\Sigma$ of the kernel of

$$\begin{array}{rcl} S_{k,\mathcal{O}/\lambda,\psi}(U_\Sigma)^2 & \longrightarrow & S_{k,\mathcal{O}/\lambda,\psi}(V) \\ (f_1,f_2) & \longmapsto & f_1 + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} f_2 \end{array}$$

vanishes. However if (f_1, f_2) is in the kernel then f_1 is invariant by the subgroup of $GL_2(\mathbb{A}_F^\infty)$ generated by U_Σ and

$$\begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} U_\Sigma \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix}^{-1},$$

i.e. by $U_\Sigma SL_2(F_x)$.

First suppose that $k = 2$. Then, by the strong approximation theorem, we see that f_1 is invariant by right translation by any element of $SL_2(\mathbb{A}_F^\infty)$, so that $f_1 \in S^{\rm triv}_{k,\mathcal{O}/\lambda,\psi}(U_\sigma)$. Any maximal ideal of $h_{2,\psi}(U_\Sigma)$ in the support of $S^{\rm triv}_{k,\mathcal{O}/\lambda,\psi}(U_\sigma)$ is Eisenstein.

Now suppose that $3 \leq k \leq l-1$. By the strong approximation theorem, given any $g \in GL_2(\mathbb{A}_F^\infty)$ and any $u \in GL_2(\mathcal{O}_{F,l})$, we can find a $\delta \in D^\times \cap gU_\Sigma SL_2(F_x)g^{-1}$ such that

$$g_l^{-1}\delta g_l \equiv u \bmod l.$$

Then

$$f_1(g) = f_1(\delta g) = f_1(g(g^{-1}\delta g)) = f_1(gu) = u^{-1}f_1(g),$$

so that

$$f_1(g) \in (\bigotimes_{\mathcal{O}_{F,l}\to\mathcal{O}/\lambda} \mathrm{Symm}^{k-2}((\mathcal{O}/\lambda)^2))^{GL_2(\mathcal{O}_{F,l})} = (0).$$

Thus $f_1 = 0$. □

In particular we see that $i_x S_\Sigma[\wp_\Sigma] = S_{\Sigma\cup\{x\}}[\wp_{\Sigma\cup\{x\}}]$. Thus

$$\begin{array}{rcl} \Omega_{\Sigma\cup\{x\}} & \cong & S_\Sigma[\wp_\Sigma]/j_\Sigma^\dagger i_x^\dagger S_\Sigma[\wp_\Sigma] \\ & \cong & S_\Sigma[\wp_\Sigma]/j_\Sigma^\dagger(1-\mathrm{N}x)(\mathrm{N}x)(T_x^2-(1+\mathrm{N}x)^2\psi(\varpi_x))S_\Sigma[\wp_\Sigma], \end{array}$$

and so

$$\#\Omega_{\Sigma\cup\{x\}} = \#\Omega_\Sigma \# \left(\mathcal{O}/(1-\mathrm{N}x)((\mathrm{N}x)\mathrm{tr}\,\rho(\mathrm{Frob}_x)^2 - (1+\mathrm{N}x)^2 \det\rho(\mathrm{Frob}_x))\right).$$

We conclude that

$$\#(\wp_\Sigma/\wp_\Sigma^2) | \#\Omega_\Sigma$$

for all Σ (which contains no prime above l). Combining this with theorem 2.4 of [Dia] we see obtain the following theorem.

Theorem 3.2 *Keep the notation and assumptions of the second and fourth paragraphs of section 2 and suppose that the restriction of $\overline{\rho}_\phi$ to the absolute Galois group of $F(\sqrt{(-1)^{(l-1)/2}l})$ is irreducible. If Σ is a finite set of finite places of F not dividing l then the natural map*

$$R_\Sigma \longrightarrow h_\Sigma$$

is an isomorphism of complete intersections and S_Σ is a free h_Σ-module.

As an immediate consequence we have the following theorem.

Theorem 3.3 *Let $l > 3$ be a prime and let $2 \leq k \leq l-1$ be an integer. Let F be a totally real field of even degree in which l splits completely. Let $\rho : G_F \to GL_2(\mathcal{O}_{\mathbb{Q}_l^{ac}})$ be a continuous irreducible representation unramified outside finitely many primes and such that for each place x of F above l the restriction $\rho|_{G_x}$ is crystalline with Hodge-Tate numbers 0 and $1-k$. Let $\overline{\rho}$ denote the reduction of ρ modulo the maximal ideal of $\mathcal{O}_{\mathbb{Q}_l^{ac}}$. Assume that the restriction of $\overline{\rho}$ to $F(\sqrt{(-1)^{(l-1)/2}l})$ is irreducible and that there is a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and an embedding $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ such that*

- *$\overline{\rho}_{\pi,\lambda} \sim \overline{\rho}$,*
- *π_x is unramified for every finite place x of F, and*
- *π_∞ has weight k.*

Then there is a regular algebraic cuspidal automorphic representation π' of $GL_2(\mathbb{A}_F)$ and an embedding $\lambda' : M_{\pi'} \to \mathbb{Q}_l^{ac}$ such that $\rho \sim \rho_{\pi',\lambda'}$ and π'_∞ has weight k.

Proof: We need only remark that $\det \rho / \det \rho_{\pi,\lambda}$ has finite l-power order and so by twisting π we may suppose that $\det \rho = \det \rho_{\pi,\lambda}$ (as $l > 2$). □

4 A potential version of Serre's conjecture

In this section we will prove the following result, which we will improve somewhat in section 5.

Proposition 4.1 *Let $l > 2$ be a prime. Suppose that $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l^{ac})$ is a continuous odd representation with $\overline{\rho}|_{I_l} \sim \omega_2^{k-1} \oplus \omega_2^{l(k-1)}$ for some integer $2 \leq k \leq l$. (In particular $\overline{\rho}|_{G_l}$ is absolutely irreducible.) Then there is a Galois totally real field F of even degree in which l splits completely, a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and an embedding $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ such that*

1. *$\overline{\rho}|_{G_F} \sim \overline{\rho}_{\pi,\lambda}$;*

2. *π_∞ has weight 2; and*

3. *for each place x of F above l, $\mathrm{WD}_\lambda(\pi_x)$ is tamely ramified and*

$$\mathrm{WD}_\lambda(\pi_x)|_{I_x} = \omega_2^{k-(l+1)} \oplus \omega_2^{lk-(l+1)}.$$

We remark that the key improvement of this over results in [Tay4] is the condition that l split completely in F. This may seem minor but it will be crucial for the arguments in section 5 and the proof of theorem 5.7. We now turn to the proof of the proposition.

Suppose that $\overline{\rho}$ is valued in $GL_2(k')$ for some finite field $k' \subset \mathbb{F}_l^{ac}$ and let k denote the unique quadratic extension of k' in $\mathbb{F}_l^{ac}$. We must have that $\overline{\rho}|_{G_l} = \mathrm{Ind}_{\mathbb{Q}_{l^2}}^{\mathbb{Q}_l} \theta$, where $\theta|_{I_l} = \omega_2^{k-1}$ with $2 \leq k \leq l$ and so θ is not equal to its $\mathrm{Gal}\,(\mathbb{Q}_{l^2}/\mathbb{Q}_l)$-conjugate. Set $\overline{\mu} = \epsilon^{-1} \det \overline{\rho}$, let N denote the minimum splitting field for $\overline{\mu}$ and $\mathfrak{f}_\mu$ its conductor. Thus N is a cyclic totally real extension of $\mathbb{Q}$. Choose an imaginary quadratic field M in which l remains prime and which contains only two roots of unity. Let δ_M denote the unique non-trivial character of $\mathbb{A}^\times/\mathbb{Q}^\times \mathrm{N}\mathbb{A}_M^\times$ and let $\mathfrak{f}_M$ denote the conductor of δ_M. Choose a Galois totally real field E'' such that $E''M$ contains a primitive root of unity ζ of order $2\#k^\times$. Note that the degree over $\mathbb{F}_l$ of every residue field of a prime of E'' above l is even.

Choose a continuous character $\chi_0 : M^\times(M_\infty^\times \times \prod_q \mathcal{O}_{M,q}^\times) \to M^\times$ which extends the canonical inclusion on $M^\times$ (use the fact that M has a prime $x \nmid 2$ with $-1 \notin (k(x)^\times)^2$) and let $\mathfrak{f}_0$ denote the conductor of χ_0. Also choose two distinct odd primes p_1 and p_2 such that for both $i = 1, 2$

- χ_0 is unramified above p_i;
- $p_i \neq l$;
- $\overline{\rho}$ is unramified at p_i;
- $\overline{\rho}(\mathrm{Frob}_{p_i})$ has distinct eigenvalues; and
- p_i splits in the Hilbert class field of M.

(We explain why this is possible. Let M' denote the extension of M cut out by $\overline{M}^{\ker \overline{\rho}}$ and by the Hilbert class field H of M. By the Cebotarev density theorem it suffices to find $\sigma \in \mathrm{Gal}\,(M'/H)$ so that $\overline{\rho}(\sigma)$ has distinct eigenvalues. A fortiori it suffices to find $\sigma \in I_l$ so that $\overline{\rho}(\sigma)$ has distinct eigenvalues. This is possible because $(l+1) \nmid k-1$.) Set $w = 2w_{E''M}\#(\mathcal{O}_M/l\mathfrak{f}_M\mathfrak{f}_\mu\mathfrak{f}_0\mathfrak{f}_0^c\mathcal{O}_M)^\times$, where $w_{E''M}$ denotes the number of roots of unity in $E''M$. Let S_1 denote set of rational primes dividing $\mathfrak{f}_M\mathfrak{f}_\mu\mathfrak{f}_0\mathfrak{f}_0^c$, let S_2 be a finite set of rational primes disjoint from S_1 which split in M and such that the primes of M above S_2 generate the class group of M, and set $S_0 = S_1 \cup S_2 \cup \{l, p_1, p_2\}$. As in the proof of lemma 1.1 of [Tay4] we can find an open subgroup W_0 of $\prod_{q \notin S_0} \mathcal{O}_{M,q}^\times/\mathbb{Z}_q^\times$ such that $W_0 \cap M_{S_0}^\times/\mathbb{Q}_{S_0}^\times \subset (M_{S_0}^\times/\mathbb{Q}_{S_0}^\times)^w$. Let w' denote the index of W_0 in

$\prod_{q\notin S_0}\mathcal{O}_{M,q}^{\times}/\mathbb{Z}_q^{\times}$. Then we can choose a Galois (over $\mathbb{Q}$) totally real field E' such that

- $E' \supset E''$;
- E' contains a primitive root of 1 of order ww'; and
- χ_0 extends to a continuous character $\chi_0 : \mathbb{A}_M^{\times} \to (E'M)^{\times}$.

(If $\widetilde{\chi}_0 : \mathbb{A}_M^{\times} \to \mathbb{C}^{\times}$ is any extension of χ_0 then $\widetilde{\chi}_0 c(\widetilde{\chi}_0)\prod_{x\not|\infty}|\ |_x$ has finite order and is valued in $\mathbb{R}_{>0}^{\times}$ and so is identically 1. Hence $c(\widetilde{\chi}_0)=\widetilde{\chi}_0^{-1}\prod_{x\not|\infty}|\ |_x$ and $\widetilde{\chi}_0$ is valued in a CM field.)
Let E denote the maximal totally real extension of E' which is unramified outside lp_1p_2 and tamely ramified at these primes. Choose primes $\wp_1$ and $\wp_2$ of EM above p_1 and p_2 respectively. Also choose a prime λ of EM above l and an embedding $k \hookrightarrow \mathcal{O}_{EM}/\lambda$ such that the composite of the Artin map $I_l \to \mathcal{O}_{M,l}^{\times}$ with the natural map $\mathcal{O}_{M,l}^{\times} \to (\mathcal{O}_{EM}/\lambda)^{\times}$ coincides with $\omega_2^{-1} : I_l \to k^{\times} \subset (\mathcal{O}_{EM}/\lambda)^{\times}$. Let $\mu : \mathrm{Gal}\,(N/\mathbb{Q}) \to (EM)^{\times}$ be the unique character reducing modulo λ to $\overline{\mu}$. For $i=1,2$ we can find $\alpha_i \in (\wp_i \cap M)\mathcal{O}_{E''M}$ which reduces modulo λ to an eigenvalue of $\overline{\rho}(\mathrm{Frob}_{p_i})$ and which satisfies $\alpha_i\alpha_i^c = p_i$. (First choose $\alpha_i' \in M \cap \wp_i$ satisfying $\alpha_i'(\alpha_i')^c = p_i$ and then multiply α_i' by a suitable root of unity in $E''M$.)

Lemma 4.2 *Let $\mathfrak{a}'$ denote the product of all primes of E above lp_1p_2 and factor $\mathfrak{a}'\mathcal{O}_{ME} = \mathfrak{a}\mathfrak{a}^c$, where $\wp_1\wp_2\lambda|\mathfrak{a}$ (which is possible as p_1 and p_2 split in M and as the degree over $\mathbb{F}_l$ of the residue field of every prime of E above l is even). There is a unit $\eta \in \mathcal{O}_E^{\times}$ with $\eta \equiv \zeta \bmod \mathfrak{a}$.*

Proof: Let $\overline{\zeta}$ denote the image of ζ in $\mathcal{O}_{E'}/(\mathfrak{a}' \cap \mathcal{O}_{E'}) = \mathcal{O}_{E'M}/(\mathfrak{a} \cap \mathcal{O}_{E'M})$. Let H denote the maximal totally real abelian extension of E which is unramified outside lp_1p_2 and which is tamely ramified above each of these three primes. Thus H/E' is Galois and $\mathrm{Gal}\,(H/E)$ is the commutator subgroup of $\mathrm{Gal}\,(H/E')$. In particular the transfer map $\mathrm{Gal}\,(E/E') \to \mathrm{Gal}\,(H/E)$ vanishes. By class field theory we can identify $(\mathcal{O}_{E'}/\mathfrak{a}')^{\times}/\mathcal{O}_{E'}^{\times}$ as a subgroup of $\mathrm{Gal}\,(E/E')$ and $(\mathcal{O}_E/\mathfrak{a})^{\times}/\mathcal{O}_E^{\times}$ as a subgroup of $\mathrm{Gal}\,(H/E)$ in such a way that the natural map

$$(\mathcal{O}_{E'}/\mathfrak{a}')^{\times}/\mathcal{O}_{E'}^{\times} \longrightarrow (\mathcal{O}_E/\mathfrak{a})^{\times}/\mathcal{O}_E^{\times}$$

corresponds to the transfer map on Galois groups and so is trivial. The lemma follows. □

Lemma 4.3 *There is a continuous character $\chi : \mathbb{A}_M^{\times} \to (EM)^{\times}$ such that*

- *$\chi|_{M^{\times}}$ is the canonical inclusion;*

- *$\chi|_{\mathcal{O}_{M,l}^\times}$ is the unique character of order prime to l with*
$$\chi|_{\mathcal{O}_{M,l}^\times}(x) \equiv x^{l+1-k} \bmod \lambda$$
for all $x \in \mathcal{O}_{M,l}^\times$ and all primes λ of EM above l (and where $\mathcal{O}_M \hookrightarrow \mathcal{O}_{EM}$ via the natural map);
- *for $i = 1, 2$, χ is non-ramified above p_i and $\chi|_{M_{\wp_i}}(p_i) = \alpha_i$; and*
- *$\chi|_{\mathbb{A}^\times} = \mu\delta_{M/\mathbb{Q}}||\ ||^{-1}i_\infty$ where $\delta_{M/\mathbb{Q}}$ is the unique non-trivial character of $\mathbb{A}^\times/\mathbb{Q}^\times \mathrm{N}\mathbb{A}_M^\times$, $||\ ||$ is the product of the usual absolute values and i_∞ is the projection onto $\mathbb{R}^\times$.*

Proof: Note that $\chi_0|_{\mathbb{A}^\times} = \nu\delta_{M/\mathbb{Q}}||\ ||^{-1}i_\infty$, where ν is a finite order character of $\mathbb{A}^\times/\mathbb{Q}^\times\mathbb{R}^\times$ with conductor dividing $\mathfrak{f}_0\mathfrak{f}_0^c\mathfrak{f}_M$. We look for $\chi = \chi_0\chi_1$. Thus we are required to find a finite order continuous character $\chi_1 : \mathbb{A}_M^\times/M^\times \longrightarrow (EM)^\times$ such that

- $\chi_1|_{\mathbb{A}^\times} = \mu\nu^{-1}$, and
- χ_1 has prescribed, finite order restriction to $M_{\wp_1}^\times$, $M_{\wp_2}^\times$ and $\mathcal{O}_{M,l}^\times$, the latter compatible with $\mu\nu^{-1}|_{\mathbb{Z}_l^\times}$ (because $\overline{\mu}|_{\mathbb{Z}_l^\times}$ takes x to $(x \bmod l)^{2-k}$).

Note that $\mu\nu^{-1}$ has conductor dividing $\mathfrak{f}_M\mathfrak{f}_\mu\mathfrak{f}_0\mathfrak{f}_0^c$. Also note that for $i = 1, 2$ the unit $a_i = \alpha_i\chi_0(\varpi_{\wp_i})^{-1}$ satisfies $a_ia_i^c = 1$ for all complex conjugations c and so is a root of unity. Thus the specified restrictions have orders dividing $w_{E''M}$ in the first two cases and $\#(\mathcal{O}_M/l\mathfrak{f}_M\mathfrak{f}_\mu\mathfrak{f}_0\mathfrak{f}_0^c\mathcal{O}_M)^\times$ in the third case.
We can find a character
$$\chi_{1,S_0} : \prod_{q\in S_0} M_q^\times \longrightarrow (EM)^\times$$
with the desired restrictions to $\prod_{q\in S_0}\mathbb{Q}_q^\times$, $M_{\wp_1}^\times$, $M_{\wp_2}^\times$ and $\mathcal{O}_{M,l}^\times$, and with order dividing w. As
$$(\prod_{q\in S_0} M_q^\times \times \prod_{q\notin S_0}\mathcal{O}_{M,q}^\times)/M_{S_0}^\times \xrightarrow{\sim} \mathbb{A}_M^\times/M^\times M_\infty^\times,$$
it suffices to find a character
$$\chi_1^{S_0} : \prod_{q\notin S_0}\mathcal{O}_{M,q}^\times/\mathbb{Z}_q^\times \longrightarrow (EM)^\times$$
which coincides with χ_{1,S_0}^{-1} on $M_{S_0}^\times/\mathbb{Q}_{S_0}^\times$. One can choose such a character which is trivial on W_0 and so has order dividing w'. □

We remark that as $\chi(c\circ\chi)||\ ||(i_\infty\circ \mathrm{N}_{M/\mathbb{Q}})^{-1}$ has finite image contained in the totally positive elements of $E^\times$ we must have $\chi(c\circ\chi) = ||\ ||^{-1}(i_\infty\circ\mathrm{N}_{M/\mathbb{Q}})$.

If x is a place of EM above a place x' of M, let χ_x denote the character

$$\begin{array}{ccc} \mathbb{A}_M^\times/M^\times & \longrightarrow & (EM)_x^\times \\ a & \longmapsto & \chi(a)a_{x'}^{-1} \end{array}$$

where $a_{x'}$ denotes the x' component of a embedded in $(EM)_x^\times$ via the natural map $M_{x'} \to (EM)_x$.

Set $\mathfrak{b} = \lambda\wp_1\wp_2$ and $\mathfrak{b}_0 = \mathfrak{b} \cap E$, so that $\mathcal{O}_E/\mathfrak{b}_0 \cong \mathcal{O}_{EM}/\lambda \times \mathcal{O}_{EM}/\wp_1 \times \mathcal{O}_{EM}/\wp_2$. Let $W_{\mathfrak{b}_0,0}/\mathbb{Q}$ denote the finite free group scheme with $\mathcal{O}_E$-action which has

$$W_{\mathfrak{b}_0,0}(\mathbb{Q}^{ac}) \cong \mathcal{O}_E/\mathfrak{b}_0(1) \oplus \mathcal{O}_E/\mathfrak{b}_0.$$

By the standard pairing on $W_{\mathfrak{b}_0,0}$ we shall mean the map $W_{\mathfrak{b}_0,0} \otimes_{\mathcal{O}_E} \mathfrak{d}_E^{-1} \to W_{\mathfrak{b}_0,0}^\vee$ which corresponds to the pairing

$$\begin{array}{ccccc} (\mathcal{O}_E/\mathfrak{b}_0(1) \oplus \mathcal{O}_E/\mathfrak{b}_0) & \times & (\mathcal{O}_E/\mathfrak{b}_0(1) \oplus \mathcal{O}_E/\mathfrak{b}_0) & \longrightarrow & \mathcal{O}_E/\mathfrak{b}_0(1) \\ (x_1, y_1) & \times & (x_2, y_2) & \longmapsto & y_2x_1 - y_1x_2. \end{array}$$

We will let $X/\mathbb{Q}$ denote the moduli space for quadruples (A, i, j, α), where (A, i, j) is an E-HBAV and $\alpha : W_{\mathfrak{b}_0,0} \xrightarrow{\sim} A[\mathfrak{b}_0]$ takes the standard pairing on $W_{\mathfrak{b}_0,0}$ to the j-Weil pairing on $A[\mathfrak{b}_0]$. As $\mathfrak{b}_0$ is divisible by two primes with coprime residue characteristic we see that X is a fine moduli space. As in section 1 of [Rap] we see that X is smooth and geometrically connected (because of the analytic uniformization of its complex points by a product of copies of the upper half complex plane).

Let Γ denote the set of pairs

$$(\gamma, \varepsilon) \in GL_2(\mathcal{O}_E/\mathfrak{b}_0) \times \mathcal{O}_{E,\gg 0}^\times/(\mathcal{O}_{E,\equiv 1\ (\mathfrak{b}_0)}^\times)^2$$

such that

$$\varepsilon \det\gamma \equiv 1 \bmod \mathfrak{b}_0.$$

Here $\mathcal{O}_{E,\gg 0}^\times$ denotes the set of totally positive elements of $\mathcal{O}_E^\times$, and $\mathcal{O}_{E,\equiv 1\ (\mathfrak{b}_0)}^\times$ denotes the set of elements of $\mathcal{O}_E^\times$ which are congruent to 1 modulo $\mathfrak{b}_0$. The group Γ acts faithfully on X via

$$(\gamma, \varepsilon)(A, i, j, \alpha) = (A, i, j \circ \varepsilon^{-1}, \alpha \circ \gamma^{-1}).$$

The action of $G_\mathbb{Q}$ on the group of automorphisms of X preserves Γ and we have

$$\sigma(\gamma, \varepsilon) = \left(\begin{pmatrix} \epsilon(\sigma) & 0 \\ 0 & 1 \end{pmatrix} \gamma \begin{pmatrix} \epsilon(\sigma)^{-1} & 0 \\ 0 & 1 \end{pmatrix}, \varepsilon \right).$$

The set $H^1(G_\mathbb{Q}, \Gamma)$ is in bijection with the set of pairs (R, ψ) where $R : G_\mathbb{Q} \to GL_2(\mathcal{O}_E/\mathfrak{b}_0)$ is a continuous representation and $\psi : G_\mathbb{Q} \to \mathcal{O}_{E,\gg 0}^\times/(\mathcal{O}_{E,\equiv 1\ (\mathfrak{b}_0)}^\times)^2$ is a continuous homomorphism with

$$\epsilon^{-1} \det R \equiv \psi^{-1} \bmod \mathfrak{b}_0.$$

This pair corresponds to the cocycle

$$(R,\psi)(\sigma) = \left(R(\sigma) \left(\begin{array}{cc} \epsilon(\sigma)^{-1} & 0 \\ 0 & 1 \end{array} \right), \psi(\sigma) \right).$$

Thus to any such pair we can associated a twist $X_{R,\psi}/\mathbb{Q}$ of $X/\mathbb{Q}$.
Next we will give a description of the F-rational points of $X_{R,\psi}$ for any number field F. Let N' denote the splitting field of ψ. Let $W_R/\mathbb{Q}$ denote the finite free group scheme with an action of $\mathcal{O}_E$ such that

$$W_R(\mathbb{Q}^{ac}) \cong \mathcal{O}_E/\mathfrak{b}_0 \oplus \mathcal{O}_E/\mathfrak{b}_0$$

with Galois action via R. By the standard pairing on W_R/N' we shall mean the map $W_R \otimes_{\mathcal{O}_E} \mathfrak{d}_E^{-1} \to W_R^\vee$ (defined over N') which corresponds to the pairing

$$\begin{array}{ccccc} (\mathcal{O}_E/\mathfrak{b}_0 \oplus \mathcal{O}_E/\mathfrak{b}_0) & \times & (\mathcal{O}_E/\mathfrak{b}_0 \oplus \mathcal{O}_E/\mathfrak{b}_0) & \longrightarrow & \mathcal{O}_E/\mathfrak{b}_0 \\ (x_1, y_1) & \times & (x_2, y_2) & \longmapsto & y_2 x_1 - y_1 x_2. \end{array}$$

Then F-rational points of $X_{R,\psi}$ correspond to quadruples (A,i,j,β), where $(A,i,j)/N'F$ is an E-HBAV and where $\beta : W_R \xrightarrow{\sim} A[\mathfrak{b}_0]$ such that

- under β the standard pairing on W_R and the j-Weil pairing on $A[\mathfrak{b}_0]$ correspond, and
- for all $\sigma \in \mathrm{Gal}\,(N'F/F)$ there is an isomorphism

  $$\kappa_\sigma : \sigma(A,i) \xrightarrow{\sim} (A,i)$$

  such that $\sigma(j) = \kappa_\sigma^* \circ j \circ \psi(\sigma)^\sim$ for some lifting $\psi(\sigma)^\sim \in \mathcal{O}_E^\times$ of $\psi(\sigma)$ and such that for some lifting $\sigma^\sim \in G_F$ of σ

  $$\begin{tikzcd} \sigma A[\mathfrak{b}_0] \arrow[r, "\kappa_\sigma"] & A[\mathfrak{b}_0] \\ W_R \arrow[u] \arrow[r, "R(\sigma^\sim)"] & W_R \arrow[u] \end{tikzcd}$$

  commutes, where the left vertical arrow is $\sigma^\sim \circ \beta$ and the right one is β.

We will be particularly interested in two pairs (R,ψ) defined as follows. For $\sigma \in \mathrm{Gal}\,(N/\mathbb{Q})$ we can write $\mu(\sigma) = \zeta^{-2m_\sigma}$ for some integer m_σ. Define $\eta_\sigma = (\eta\zeta^{-1})^{m_\sigma} \in \mathcal{O}_{EM,\equiv 1\ (\mathfrak{b})}^\times$ and $\psi(\sigma) = \mathrm{N}_{EM/E}\eta_\sigma = \eta^{2m_\sigma}$. As

$$\eta^{2\#k^\times} = (-\eta^{\#k^\times})^2 \in (\mathcal{O}_{E,\equiv 1\ (\mathfrak{b}_0)}^\times)^2,$$

we see that

$$\psi : \mathrm{Gal}\,(N/\mathbb{Q}) \longrightarrow \mathcal{O}_{E,\gg 0}^\times/(\mathcal{O}_{E,\equiv 1\ (\mathfrak{b}_0)}^\times)^2$$

is a homomorphism. Let

$$R_{\overline{\rho}} = \overline{\rho} \oplus \mathrm{Ind}\,_{G_M}^{G_\mathbb{Q}} \chi_{\wp_1} \oplus \mathrm{Ind}\,_{G_M}^{G_\mathbb{Q}} \chi_{\wp_2}$$

and

$$R_{Dih} = \mathrm{Ind}\,_{G_M}^{G_{\mathbb{Q}}}\chi_\lambda \oplus \mathrm{Ind}\,_{G_M}^{G_{\mathbb{Q}}}\chi_{\wp_1} \oplus \mathrm{Ind}\,_{G_M}^{G_{\mathbb{Q}}}\chi_{\wp_2},$$

so that $\epsilon^{-1}\det R_\rho = \epsilon^{-1}\det R_{Dih} = \mu$. Then $(R_{\overline{\rho}}, \psi)$ and (R_{Dih}, ψ) define elements of $H^1(G_{\mathbb{Q}}, \Gamma)$ and we will denote the corresponding twists of X by $X_{\overline{\rho}}$ and X_{Dih} respectively. Note that $X_{\overline{\rho}}$ and X_{Dih} become isomorphic over $\mathbb{Q}_l$, $\mathbb{Q}_{p_1}$, $\mathbb{Q}_{p_2}$ and $\mathbb{R}$.

Lemma 4.4 *Suppose that F is a number field. If $X_{\overline{\rho}}$ has an F-rational point then there exists an abelian variety B/F of dimension $[EM : \mathbb{Q}]$, an embedding $i' : \mathcal{O}_{EM} \hookrightarrow \mathrm{End}\,(B/F)$, and an isomorphism β' between $B[\mathfrak{b}](F^{ac})$ and $R_{\overline{\rho}}$.*

Proof: Suppose that $(A, i, j, \beta)/FN$ is a quadruple corresponding to an F-rational point of $X_{\overline{\rho}}$ as above. Also, for $\sigma \in \mathrm{Gal}\,(NF/F)$ let $\kappa_\sigma : \sigma A \xrightarrow{\sim} A$ be the maps of the last but one paragraph. Set $B = A \otimes_{\mathcal{O}_E} \mathcal{O}_{EM}$ and let i' denote the natural map $\mathcal{O}_{EM} \to \mathrm{End}\,(B)$. Let β' denote the composite

$$W_{R_{\overline{\rho}}} \xrightarrow{\beta} A[\mathfrak{b}_0] \longrightarrow A[\mathfrak{b}_0] \otimes_{\mathcal{O}_E} \mathcal{O}_{EM}/\mathfrak{b} = B[\mathfrak{b}].$$

Define $f_0 : \mathcal{O}_{EM} \to \mathrm{Hom}\,_{\mathcal{O}_E}(\mathcal{O}_{EM}, \mathcal{O}_E)$ by $f_0(a)(b) = \mathrm{tr}\,_{EM/E}ab^c$ and set $f = j(1) \otimes f_0$ a polarisation of B. Also set

$$\kappa'_\sigma = \kappa_\sigma \otimes \eta_\sigma : \sigma B \longrightarrow B.$$

We see that κ'_σ commutes with the action of $\mathcal{O}_{EM}$, that $\sigma f = (\kappa'_\sigma)^\vee f \kappa'_\sigma$ and that for any lifting $\sigma^\sim \in G_F$ of σ

$$\begin{tikzcd}
\sigma B[\mathfrak{b}] \arrow[r, "\kappa'_\sigma"] & B[\mathfrak{b}] \\
W_{R_{\overline{\rho}}} \arrow[u] \arrow[r, "R_{\overline{\rho}}(\sigma^\sim)"] & W_{R_{\overline{\rho}}} \arrow[u]
\end{tikzcd}$$

commutes, where the left vertical arrow is $\sigma^\sim \circ \beta'$ and the right one is β'. As the quadruple (B, i', f, β') has no non-trivial automorphisms (because any automorphism of (B, i', f) has finite order and because $\mathfrak{b}$ is divisible by two primes with distinct residual characteristic), we see that $\kappa'_\sigma \sigma(\kappa'_\tau) = \kappa'_{\sigma\tau}$. Thus we can descend (B, i') to F in such a way that β' also descends to an isomorphism $\beta' : W_{R_{\overline{\rho}}} \xrightarrow{\sim} B[\mathfrak{b}]$ over F. □

Lemma 4.5 *X_{Dih} has a $\mathbb{Q}$-rational point and hence $X_{\overline{\rho}}$ has rational points over $\mathbb{Q}_l$, $\mathbb{Q}_{p_1}$, $\mathbb{Q}_{p_2}$ and over $\mathbb{R}$.*

Proof: Fix an embedding $\tau : M \hookrightarrow \mathbb{C}$ and let Φ denote the CM-type for EM consisting of all embeddings $EM \hookrightarrow \mathbb{C}$ which restrict to τ on M. Let $(\mathfrak{d}_{EM}^{-1})^-$ denote the ordered $\mathcal{O}_E$-module $\{d \in \mathfrak{d}_{EM}^{-1} :\ \mathrm{tr}\,_{EM/E}d = 0\}$ with $(\mathfrak{d}_{EM}^- \otimes_{E,\sigma} \mathbb{R})^+$ the subset with positive imaginary part under $\sigma \otimes \tau$. From the theory of complex multiplication (see [Lang], particularly theorem 5.1 of chapter 5) we see that there is

- an abelian variety A/M of dimension $[E:\mathbb{Q}]$;
- an embedding $i:\mathcal{O}_{EM}\hookrightarrow \mathrm{End}\,(A/M)$;
- an isomorphism $j:(\mathfrak{d}_{EM}^{-1})^{-}\xrightarrow{\sim}\mathcal{P}(A,i|_{\mathcal{O}_E})$; and
- for each prime $\mathfrak{q}$ of E a Galois invariant isomorphism $\alpha_{\mathfrak{q}}:\mathcal{O}_{EM,\mathfrak{q}}(\chi_{\mathfrak{q}})\xrightarrow{\sim} T_{\mathfrak{q}}A$

such that

- the action of EM on $Lie\,\tau A$ is $\bigoplus_{\sigma\in\Phi}\sigma$; and
- for any $d\in(\mathfrak{d}_{EM}^{-1})^{-}$ which is totally positive the $j(d)$-Weil pairing on $T_{\mathfrak{q}}A$ is given by
$$x\times y\longmapsto \mathrm{tr}\,_{EM/E}dxy^{c}.$$

(For the existence of j note that if f is a polarisation of $\tau A/\mathbb{C}$ such that the f-Rosati involution stabilises and acts trivially on E, then the f-Rosati involution also stabilises EM and acts on it via complex conjugation. This follows from the fact that EM is the centraliser of E in $\mathrm{End}\,(\tau A/\mathbb{C})$.) As $\chi(c\circ\chi)=(||\;||^{-1}i_\infty)\circ \mathrm{N}_{M/\mathbb{Q}}$, we see that for $\sigma\in G_M$ we have
$$\mathrm{tr}\,_{EM/M}d\alpha_{\mathfrak{q}}(\sigma x)\alpha_{\mathfrak{q}}(\sigma y)^{c}=\epsilon_q(\sigma)\mathrm{tr}\,_{EM/M}d\alpha_{\mathfrak{q}}(x)\alpha_{\mathfrak{q}}(y)^{c}.$$

Thus the quadruple $(A,i|_{\mathcal{O}_E},j,(\prod_{\mathfrak{q}}\alpha_{\mathfrak{q}})\bmod \mathfrak{b}_0)$ defines a point in $X_{Dih}(M)$. As $\chi(\chi\circ c)=(||\;||^{-1}i_\infty\mu)\circ \mathrm{N}_{M/\mathbb{Q}}$, we see that $c\circ\chi\circ \mathrm{N}_{NM/M}=\chi\circ c\circ \mathrm{N}_{NM/M}$ and so over NM there is an isomorphism between $(A,i,j,\{\alpha_{\mathfrak{q}}\})$ and $(cA,c\circ i\circ c,c\circ j,\{c\circ\alpha_{\mathfrak{q}}\circ c\})$. Thus the point in $X_{Dih}(M)\subset X_{Dih}(NM)$ defined by $(A,i|_{\mathcal{O}_E},j,(\prod_{\mathfrak{q}}\alpha_{\mathfrak{q}})\bmod \mathfrak{b}_0)$ is invariant under c and so lies in $X_{Dih}(\mathbb{Q})$. □

Combining the last two lemmas with a theorem of Moret-Bailly (see theorem G of [Tay4]) we see that we can find a Galois totally real field F of even degree in which l, p_1 and p_2 split completely, an abelian variety B/F of dimension $[EM:M]$ and an embedding $i:\mathcal{O}_{EM}\hookrightarrow\mathrm{End}\,(B/F)$ such that $B[\lambda]$ realises $\overline{\rho}$ and, for $i=1,2$, $B[\wp_i]$ realises $\mathrm{Ind}\,_{G_M}^{G_{\mathbb{Q}}}(\chi_{\wp_i}\bmod\wp_i)$. As $B[\lambda]$ is unramified at any prime above p_1 we see that the action of inertia at such a prime on $T_\lambda B$ has l-power order. As $B[\wp_2]$ is unramified at any prime above p_1 we see that the action of inertia at such a prime on $T_{\wp_2}B$ has p_2-power order. Hence the action of inertia at a prime above p_1 on $T_\lambda B$ has both l-power order and p_2-power order. We conclude that $T_\lambda B$ is unramified at primes above p_1 and hence B has semi-stable reduction at such primes. As p_1 splits completely in F and as $B[\wp_1]$ is reducible as a representation of the decomposition group of any prime of F above p_1, we see that $T_{\wp_1}B$ is an ordinary representation of the decomposition group at any prime of F above p_1. If x is a prime of F above l then I_x acts on both $B[\wp_1]$ and $B[\wp_2]$ via $\widetilde{\omega}_2^{k-(l+1)}\oplus\widetilde{\omega}_2^{lk-(l+1)}$ where $\widetilde{\omega}_2:I_x\to\mathcal{O}_{EM}^{\times}$ is tamely ramified and reduces mod λ to ω_2. Thus I_x acts on $T_{\wp_1}B$ by $\widetilde{\omega}_2^{k-(l+1)}\oplus\widetilde{\omega}_2^{lk-(l+1)}$. Because $\mathrm{Ind}\,_{G_{FM}}^{G_F}(\chi_{\wp_1})$ is modular, theorem 5.1

of [SW2] tells us that there is a algebraic, cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ of weight 2 and an embedding $M_\pi \hookrightarrow EM$ such that $\rho_{\pi,\wp_1}$ is equivalent to $T_{\wp_1}B$. (Alternatively one may appeal to the main theorem of [SW1], theorem 3.3 of this paper and a standard descent argument.) It follows that in addition $\rho_{\pi,\lambda}$ is equivalent to $T_\lambda B$. This completes the proof of proposition 4.1.

Using Langlands base change [Langl] we immediately obtain the following corollary.

Corollary 4.6 *Let $l > 2$ be a prime. Suppose that $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l^{ac})$ is a continuous odd representation with $\overline{\rho}|_{I_l} \sim \omega_2^{k-1} \oplus \omega_2^{l(k-1)}$ for some integer $2 \leq k \leq l$. Then there is a Galois totally real field F of even degree in which l splits completely, a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and an embedding $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ such that*

1. *$\overline{\rho}|_{G_F} \sim \overline{\rho}_{\pi,\lambda}$;*
2. *π_∞ has weight 2;*
3. *the central character of $\pi^{\infty,l}$ is unramified; and*
4. *for each place x of F above l, $\mathrm{WD}_\lambda(\pi_x)$ is tamely ramified and*
$$\mathrm{WD}_\lambda(\pi_x)|_{I_x} = \omega_2^{k-(l+1)} \oplus \omega_2^{lk-(l+1)}.$$

5 Change of weight

In this section we will prove various refinements of proposition 4.1, but first we shall discuss some results about congruences between modular forms.

Let F be a totally real field of even degree in which a prime $l > 3$ splits completely. Let $\mathfrak{n}$ denote an ideal of $\mathcal{O}_F$ coprime to l. Let $\psi : (\mathbb{A}_F^\infty)^\times/F^\times \to (\mathbb{Q}_l^{ac})^\times$ be a continuous character trivial on $\mathcal{O}_{F,x}^\times$ if $x \not| l$ and on $(1 + l\mathcal{O}_{F,x})$ if $x|l$. Suppose further that there exists $i \in (\mathbb{Z}/(l-1)\mathbb{Z})$ such that for $a \in \mathcal{O}_{F,l}^\times$, $\psi(a)$ is congruent to $(\mathrm{N}a)^{-i}$ modulo the maximal ideal of $\mathcal{O}_{\mathbb{Q}_l^{ac}}$.

Let D denote the division algebra with centre F ramified at exactly the infinite places of F. Let $\mathcal{O}_D$ be a maximal order in D and fix an isomorphism $\mathcal{O}_{D,x} \cong M_2(\mathcal{O}_{F,x})$ for each finite place x of F. We will write

- $U_0(\mathfrak{n}, l)$ for $U_{\{1\}}(\mathfrak{n}l)$, and
- $U_1(\mathfrak{n}, l)$ for $U_{(\mathcal{O}_F/l\mathcal{O}_F)^\times}(\mathfrak{n}l)$.

(See section 1, in particular the paragraph after corollary 1.2, for this notation.)

We will let $\overline{\eta}^i$ denote the character $U_0(\mathfrak{n}, l)/U_1(\mathfrak{n}, l) \to (\mathbb{F}_l^{ac})^\times$ which sends u, with
$$u_l = \begin{pmatrix} * & * \\ * & d \end{pmatrix},$$

to $(\mathrm{N}d \bmod l)^i$. We will also let η^i denote the Teichmüller lift of $\overline{\eta}^i$. For any $\mathcal{O}_{\mathbb{Q}_l^{ac}}$-algebra R, there is a natural embedding

$$S_{\eta^i\otimes R,\psi}(U_0(\mathfrak{n},l)) \hookrightarrow S_{\eta^i\otimes R,\psi}(U_1(\mathfrak{n},l)) = S_{2,R,\psi}(U_1(\mathfrak{n},l)),$$

which is equivariant for the action of T_x and S_x for all $x \not| l\mathfrak{n}$, and for $\mathbf{U}_{\varpi_x}$ for $x|\mathfrak{n}$. The image is the subset of $S_{2,R,\psi}(U_1(\mathfrak{n},l))$ where $\langle h\rangle = 1$ for all $h \in (\mathcal{O}_F/l\mathcal{O}_F)^\times$. If $\phi : h_{\eta^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l)) \to \mathbb{F}_l^{ac}$ has non-Eisenstein kernel then for $x|l$ we have

$$\det \overline{\rho}_\phi|_{I_x} = \omega^{1+i}.$$

The operators $\mathbf{U}_{\varpi_x}$ and $\mathbf{V}_{\varpi_x}$ on $S_{2,\mathbb{F}_l^{ac},\psi}(U_1(\mathfrak{n},l))$ commute with the action of $\langle h\rangle$ for $h \in (\mathcal{O}_F/l\mathcal{O}_F)^\times$ and hence preserve $S_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n},l))$. We will let $h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l))'$ (resp. $h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l))''$) denote the commutative subalgebra of the endomorphisms of $S_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n},l))$ generated by $h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l))$ and $\mathbf{U}_{\varpi_x}$ (resp. $\mathbf{V}_{\varpi_x}$) for all $x|l$. If $\phi : h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l))' \to \mathbb{F}_l^{ac}$ and $\phi(\mathbf{U}_{\varpi_x}) \neq 0$ then

$$\overline{\rho}_\phi|_{G_x} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

where χ_2 is unramified and $\chi_2(\mathrm{Frob}_x) = \phi(\mathbf{U}_{\varpi_x})$ (see [W1]).

If $f_1 \in S_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n},l))$ and $f_2 \in S_{\overline{\eta}^{-i},\psi^{-1}}(U_0(\mathfrak{n},l))$ then define (f_1, f_2) to be

$$\sum_{[x]\in D^\times\backslash(D\otimes_{\mathbb{Q}}\mathbb{A}^\infty)/U_0(\mathfrak{n},l)(\mathbb{A}_F^\infty)^\times} f_1(x)f_2(xw)(\#(U_0(\mathfrak{n},l)(\mathbb{A}_F^\infty)^\times \cap x^{-1}D^\times x)/F^\times)^{-1},$$

where

$$w_x = \begin{pmatrix} 0 & 1 \\ \varpi_x^{x(\mathfrak{n})} & 0 \end{pmatrix}$$

if $x \not| l$ and $w_x = 1_2$ if $x|l$. This is easily seen to be a perfect pairing. Moreover a standard calculation shows that the adjoint of S_x is S_x^{-1}, the adjoint of T_x is $S_x^{-1}T_x$, the adjoint of $\mathbf{U}_{\varpi_x}$ for $x|\mathfrak{n}$ is $S_{\varpi_x}^{-1}\mathbf{U}_{\varpi_x}$ and the adjoint of $\mathbf{U}_{\varpi_x}$ for $x|l$ is $S_{\varpi_x}^{-1}\mathbf{V}_{\varpi_x}$. Thus if $\phi : h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l)) \to \mathbb{F}_l^{ac}$ then there is also a homomorphism $\phi^* : h_{\overline{\eta}^{-i},\mathbb{F}_l,\psi^{-1}}(U_0(\mathfrak{n},l)) \to \mathbb{F}_l^{ac}$ satisfying $\phi^*(T_x) = \phi(S_x)^{-1}\phi(T_x)$ and $\phi^*(S_x) = \phi(S_x)^{-1}$. Moreover if ϕ extends to $h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l))''$ so that $\phi(\mathbf{V}_{\varpi_x}) \neq 0$ then ϕ^* extends to $h_{\overline{\eta}^{-i},\mathbb{F}_l,\psi^{-1}}(U_0(\mathfrak{n},l))'$ with $\phi^*(\mathbf{U}_{\varpi_x}) \neq 0$. We deduce that $\overline{\rho}_{\phi^*} = \overline{\rho}_\phi^\vee(1)$. Hence if $\phi : h_{\overline{\eta}^i,\mathbb{F}_l,\psi}(U_0(\mathfrak{n},l))'' \to \mathbb{F}_l^{ac}$ and $\phi(\mathbf{V}_{\varpi_x}) \neq 0$ then

$$\overline{\rho}_\phi|_{G_x} \sim \begin{pmatrix} \epsilon\chi_1 & * \\ 0 & \omega^i\chi_2 \end{pmatrix}$$

where χ_1 and χ_2 are unramified.

We will denote by I^i the induced representation from $U_0(\mathfrak{n},l)$ to $U_H(\mathfrak{n})$ of $\overline{\eta}^i$. It is a tesnor product $\bigotimes_{x|l} I_x^i$ where I_x^i is the induction from $U_0(\mathfrak{n},l)_x$ to $GL_2(\mathcal{O}_{F,x})$ of $\overline{\eta}^i$. We can realise I_x^i concretely as the space of functions

$$\theta : k(x)^2 - \{(0,0)\} \longrightarrow \mathbb{F}_l^{ac}$$

such that $\theta(a(x,y)) = a^i\theta(x,y)$ for all $a \in k(x)^\times$. The action of $GL_2(\mathcal{O}_{F,x})$ is via $(u\theta)(x,y) = \theta((x,y)u)$. We have an isomorphism

$$S_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n},l)) \cong S_{I^i,\psi}(U_H(\mathfrak{n}))$$

under which $f \in S_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n},l))$ corresponds to $F \in S_{I^i,\psi}(U_H(\mathfrak{n}))$ if

$$f(g) = F(g)((0,1)_x)$$

and

$$F(g)(a_x,b_x) = f(gu^{-1})$$

where $u \in GL_2(\mathcal{O}_{F,l})$ and

$$u \bmod x = \begin{pmatrix} * & * \\ a_x & b_x \end{pmatrix}$$

for all $x|l$.

Now suppose that $0 \leq i \leq l-2$. If x is a prime of F above l then we have an exact sequence

$$(0) \longrightarrow \mathrm{Symm}^i((\mathbb{F}_l^{ac})^2) \longrightarrow I_x^i \longrightarrow \mathrm{Symm}^{l-1-i}((\mathbb{F}_l^{ac})^2) \otimes \det{}^i \longrightarrow (0).$$

The first map is just the natural inclusion of homogeneous polynomials of degree i into the space of homogeneous functions of degree i. The second map sends a homogeneous function θ onto the polynomial

$$\sum_{(s,t)\in\mathbb{P}^1(k(x))} \theta(s,t)(tX-sY)^{l-1-i}.$$

Thus for any subset T of the set of places of F above l we have a submodule $I_T^i \subset I^i$ with

$$I_T^i \cong \bigotimes_{x\notin T} \mathrm{Symm}^i((\mathbb{F}_l^{ac})^2) \otimes \bigotimes_{x\in T} I_x^i.$$

These give rise to subspaces

$$S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n},l)) \subset S_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n},l))$$

with

$$S_{\overline{\eta}^i,\psi,\emptyset}(U_0(\mathfrak{n},l)) \cong S_{i+2,\mathbb{F}_l^{ac},\psi}(U_H(\mathfrak{n}))$$

as a module for the Hecke operators T_x and S_x for all $x \not| l\mathfrak{n}$ and for $\mathbf{U}_{\varpi_x}$ for all $x|\mathfrak{n}$.

The following lemma is a variant of an unpublished result of Buzzard (see [Bu]).

Lemma 5.1 *For any set T of places of F above l and for any place $x \notin T$ of F above l there is an injection*

$$\kappa_x : S_{\overline{\eta}^i,\psi,T\cup\{x\}}(U_0(\mathfrak{n},l))/S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n},l)) \hookrightarrow S_{\overline{\eta}^i,\psi,T\cup\{x\}}(U_0(\mathfrak{n},l))$$

which is equivariant for the actions of T_y *and* S_y *for all* $y \not| l$ *and for* $\mathbf{U}_{\varpi_x}$ *for* $x|\mathfrak{n}$*, and such that the composite*

$$S_{\overline{\eta}^i,\psi,T\cup\{x\}}(U_0(\mathfrak{n},l)) \xrightarrow{\kappa_x} S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n},l)) \hookrightarrow S_{\overline{\eta}^i,\psi,T\cup\{x\}}(U_0(\mathfrak{n},l))$$

coincides with $\mathbf{V}_{\varpi_x}$*.*

Proof: Define $U_0(T) \subset U_H(\mathfrak{n})$ by $U_0(T)_y = U_0(\mathfrak{n},l)_y$ if $y \in T$ and $U_0(T)_y = U_H(\mathfrak{n})_y$ otherwise. Let τ_T denote the representation

$$(\bigotimes_{y\in T} \overline{\eta}^i_y) \otimes (\bigotimes_{y\notin T} \mathrm{Symm}^{\,2+i}((\mathbb{F}_l^{ac})^2)$$

of $U_0(T)_l$. If $x \notin T$ is a place of F above l, let $\tau_{T,x}$ denote the representation

$$(\bigotimes_{y\in T} \overline{\eta}^i_y) \otimes (\bigotimes_{y\notin T\cup\{x\}} \mathrm{Symm}^{\,i+2}((\mathbb{F}_l^{ac})^2)) \otimes (\mathrm{Symm}^{\,l-1-i}((\mathbb{F}_l^{ac})^2) \otimes \det{}^i)$$

of $U_0(T)_l$. Then the exact sequence

$$\begin{aligned}(0) \longrightarrow S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n},l)) \longrightarrow S_{\overline{\eta}^i,\psi,T\cup\{x\}}(U_0(\mathfrak{n},l)) \longrightarrow \\ \longrightarrow S_{\overline{\eta}^i,\psi,T\cup\{x\}}(U_0(\mathfrak{n},l))/S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n},l)) \longrightarrow (0)\end{aligned}$$

is identified to the exact sequence

$$(0) \longrightarrow S_{\tau_T,\psi}(U_0(T)) \xrightarrow{\alpha} S_{\tau_{T\cup\{x\}},\psi}(U_0(T\cup\{x\})) \xrightarrow{\beta} S_{\tau_{T,x},\psi}(U_0(T)) \longrightarrow (0),$$

where

$$\alpha(f)(g) = f(g)(0,1)_x$$

and

$$\beta(f)(g)(X,Y)_x = \sum_{(s:t)\in\mathbb{P}^1(k(x))} f(gu(s,t)^{-1})(tX-sY)^{l-1-i}$$

with $u(s,t) \in GL_2(\mathcal{O}_{F,x})$ congruent to

$$\begin{pmatrix} * & * \\ s & t \end{pmatrix}$$

modulo x.
Now define

$$\kappa : S_{\tau_{T,x},\psi}(U_0(T)) \longrightarrow S_{\tau_{T\cup\{x\}},\psi}(U_0(T\cup\{x\}))$$

by

$$\kappa(f)(g) = f(g\gamma)(1,0)_x$$

where

$$\gamma = \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} \in GL_2(F_x).$$

To see this is well defined the only slightly subtle point is that if $u \in U_0(\mathfrak{n}, l)_x$ then

$$\begin{array}{rcl} \kappa(f)(gu) & = & f(g\gamma(\gamma^{-1}u\gamma))(1,0)_x \\ & = & (\det u)^i f(g\gamma)((1,0)_x(\gamma^{-1}u^{-1}\gamma)) \\ & = & (\det u)^i f(g\gamma)(\eta_x(u)/\det u, 0)_x \\ & = & \eta_x(u)^{-i} f(g\gamma)(1,0)_x \\ & = & \eta_x(u)^{-i}\kappa(f)(g). \end{array}$$

Moreover κ is clearly injective and equivariant for the action of T_y and S_y if $y \not| l\mathfrak{n}$ and for $\mathbf{U}_{\varpi_x}$ for $x|\mathfrak{n}$. Finally we have

$$\begin{array}{rcl} (\kappa \circ \beta)(f)(g) & = & \sum_{(s:t)\in\mathbb{P}^1(k(x))} f(g\gamma u(s,t)^{-1})t^{l-1-i} \\ & = & \sum_{s\in k(x)} f(g\gamma u(s,1)^{-1}) \\ & = & (\mathbf{V}_{\varpi_x} f)(g). \end{array}$$

as we can take

$$u(s,1) = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}.$$

□

Corollary 5.2 *There is a natural surjection*

$$h_{\overline{\eta}^i,\mathbb{F}_l^{ac},\psi}(U_0(\mathfrak{n}, l)) \twoheadrightarrow h_{i+2,\mathbb{F}_l^{ac},\psi}(U_H(\mathfrak{n}))$$

which takes T_y to T_y and S_y to S_y for all $y \not| l\mathfrak{n}$ and which takes $\mathbf{U}_{\varpi_x}$ to $\mathbf{U}_{\varpi_x}$ for all $x|\mathfrak{n}$. If $\mathfrak{m}$ is a maximal ideal of $h_{\overline{\eta}^i,\mathbb{F}_l^{ac},\psi}(U_0(\mathfrak{n}, l))$ such that for any $x|l$ and any maximal ideal $\mathfrak{m}_x''$ of $h_{\overline{\eta}^i,\mathbb{F}_l^{ac},\psi}(U_0(\mathfrak{n}, l))''$ extending $\mathfrak{m}$ one has $\mathbf{V}_{\varpi_x} \in \mathfrak{m}_x''$, then $h_{i+2,\mathbb{F}_l^{ac},\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}} \neq (0)$. This assumption will be verified if $\mathfrak{m}$ is non-Eisenstein and the kernel of a homomorphism $\phi : h_{\overline{\eta}^i,\psi}(U_0(\mathfrak{n}, l)) \to \mathbb{F}_l^{ac}$ such that for all $x|l$

$$\overline{\rho}_\phi|_{G_x} \not\sim \begin{pmatrix} \epsilon\chi_1 & * \\ 0 & \omega^i\chi_2 \end{pmatrix},$$

with χ_1 and χ_2 unramified.

Proof: Choose a minimal T such that $S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n}, l))_{\mathfrak{m}} \neq (0)$. If $T = \emptyset$ then $S_{k,\mathbb{F}_l^{ac},\psi}(U_H(\mathfrak{n}))_{\mathfrak{m}} \neq (0)$ and the corollary follows. Thus suppose that $x \in T$ and set $T' = T - \{x\}$. By our minimality assumption we see that

$$S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n}, l))_{\mathfrak{m}} \xrightarrow{\sim} (S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n}, l))/S_{\overline{\eta}^i,\psi,T'}(U_0(\mathfrak{n}, l)))_{\mathfrak{m}} \overset{\kappa_x}{\hookrightarrow} S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n}, l))_{\mathfrak{m}}$$

and the composite coincides with $\mathbf{V}_{\varpi_x}$. Thus $\mathbf{V}_{\varpi_x}$ is an isomorphism on the space $S_{\overline{\eta}^i,\psi,T}(U_0(\mathfrak{n}, l))_{\mathfrak{m}}$ and $\mathbf{V}_{\varpi_x}$ does not lie in some maximal ideal of $h_{\overline{\eta}^i,\mathbb{F}_l^{ac},\psi}(U_0(\mathfrak{n}, l))''$ above $\mathfrak{m}$, a contradiction. □

We also have the following lemma, which generalises results of Ash and Stevens [AS]. We write U_0 for $\prod_y GL_2(\mathcal{O}_{F,y})$.

Lemma 5.3 *If $k \in \mathbb{Z}_{\geq 2}$ and if $\phi : h_{k,\mathbb{F}_l^{ac},\psi}(U_0) \to \mathbb{F}_l^{ac}$ is a homomorphism, then there is a homomorphism $(D\phi) : h_{k+l+1,\mathbb{F}_l^{ac},\psi(\epsilon\circ \mathrm{Art}^{-1})}(U_0) \to \mathbb{F}_l^{ac}$ such that for all places $y \not| l$ we have $(D\phi)(T_y) = \phi(T_y)(\mathrm{N}y)$ and $(D\phi)(S_y) = \phi(S_y)(\mathrm{N}y)^2$.*

Proof: If $f \in S_{k,\mathbb{F}_l^{ac},\psi}(U_0)$ then the function

$$(Df)(g) = f(g)(||\mathrm{N}\det g||(\mathrm{N}\det g_l))^{-1},$$

where $||\ || : (\mathbb{A}^\infty)^\times \to \mathbb{Q}_{>0}^\times$ denotes the product of the usual p-adic absolute values, lies in $S_{\tau_{k,\mathbb{F}_l^{ac}}\otimes(\mathrm{N}\det),\psi(\epsilon\circ\mathrm{Art}^{-1})}(U_0)$. Moreover if $T_y f = af$ (resp. $S_y f = bf$) then $T_y(Df) = a(\mathrm{N}y)(Df)$ (resp. $S_y(Df) = b(\mathrm{N}y)(Df)$). Thus it suffices to exhibit an embedding

$$S_{\tau_{k,\mathbb{F}_l^{ac}}\otimes(\mathrm{N}\det),\psi(\epsilon\circ\mathrm{Art}^{-1})}(U_0) \hookrightarrow S_{k+l+1,\mathbb{F}_l^{ac},\psi(\epsilon\circ\mathrm{Art}^{-1})}(U_0)$$

compatible with the action of T_y and S_y for all $y \not| l$. By lemma 1.1 it suffices to exhibit a $GL_2(\mathcal{O}_{F,l})$-equivariant embedding

$$\bigotimes_x (\mathrm{Symm}^{k-2}(k(x)^2) \otimes \det) \hookrightarrow \bigotimes_x \mathrm{Symm}^{k+l-1}(k(x)^2),$$

or simply $GL_2(\mathcal{O}_{F,x})$-equivariant embeddings

$$\mathrm{Symm}^{k-2}(k(x)^2) \otimes \det \hookrightarrow \mathrm{Symm}^{k+l-1}(k(x)^2)$$

for all $x|l$. Because l splits completely in F such an embedding simply results from multiplication by $X^lY - XY^l$, as we see from the following calculation. For $a,b,c,d \in \mathbb{F}_l$ we have

$$\begin{array}{rl} & (aX+cY)^l(bX+dY) - (aX+cY)(bX+dY)^l \\ = & (aX^l+cY^l)(bX+dY) - (aX+cY)(bX^l+dY^l) \\ = & (ad-bc)(X^lY - XY^l). \end{array}$$

□

We now turn to our improvements to proposition 4.1. First we have the following lemma.

Lemma 5.4 *Let $l > 3$ be a prime. Suppose that $\overline{\rho} : G_\mathbb{Q} \to GL_2(\mathbb{F}_l^{ac})$ is a continuous odd representation with $\overline{\rho}|_{I_l} \sim \omega_2^{k-1} \oplus \omega_2^{l(k-1)}$ for some integer $2 \leq k \leq l$. Then there is a Galois totally real field F in which l splits completely, a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and an embedding $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ such that*

1. *$\overline{\rho}|_{G_F} \sim \overline{\rho}_{\pi,\lambda}$;*

2. *π_∞ has weight 2; and*

3. for each place x of F above l, π_x has conductor dividing x.

Proof: Let F, π, λ be as provided by corollary 4.6. Let $\psi_0 : (\mathbb{A}_F^\infty)^\times/F^\times \to (\mathbb{Q}_l^{ac})^\times$ be the character such that $\epsilon(\psi_0 \circ \mathrm{Art}^{-1})$ equals the determinant of $\rho_{\pi,\lambda}$. Thus ψ_0 is unramified away from l. Let $\mathfrak{n}_0$ denote the prime to l part of the conductor of π. Let D be the division algebra with centre F which is ramified at exactly the infinite places of F. Let $\mathcal{O}_D$ be a maximal order in D and fix an isomorphism $\mathcal{O}_{D,x} \cong M_2(\mathcal{O}_{F,x})$ for each finite place x of F. Let $\mathcal{O}$ denote the ring of integers of $\mathbb{Q}_l^{ac}$.
Let χ_k denote the character $\mathbb{F}_{l^2}^\times \to \mathcal{O}^\times$ which sends a to the Teichmüller lift of a^{k-l-1}. Let $\Theta(\chi_k)$ denote a model over $\mathcal{O}$ of the representation of $GL_2(\mathbb{Z}_l) \to \to GL_2(\mathbb{F}_l)$ denoted the same way in section 3.1 of [CDT]. Let Θ_k denote the representation $\bigotimes_{x|l} \Theta(\chi_k)$ of $GL_2(\mathcal{O}_{F,l})$. From proposition 4.1, lemma 1.3 and lemma 4.2.4 of [CDT] we see that there is a homomorphism

$$\phi_1 : h_{\Theta_k,\mathcal{O},\psi_0}(U_{H_0}(\mathfrak{n}_0)) \longrightarrow \mathbb{F}_l^{ac}$$

such that $\ker \phi_1$ is non-Eisenstein and $\overline{\rho}_{\phi_1} \sim \overline{\rho}|_{G_F}$.
By lemma 3.1.1 of [CDT] we see that $\Theta_k \otimes \mathbb{F}_l^{ac}$ has a Jordan-Hölder sequence with subquotients

$$R_T = \bigotimes_{x \notin T} \mathrm{Symm}^{k-2}((\mathbb{F}_l^{ac})^2) \otimes \bigotimes_{x \in T} (\mathrm{Symm}^{l-1-k}((\mathbb{F}_l^{ac})^2) \otimes \det{}^{k-1})$$

where T runs over sets of places of F above l, and where, if $k = l$, we only have one subquotient namely $T = \emptyset$. Thus for some T, ϕ_1 factors through $h_{R_T,\mathbb{F}_l^{ac},\psi_0}(U_{H_0}(\mathfrak{n}_0))$. It then follows from corollary 1.5 that for $x \in T$ we must have $\overline{\rho}|_{I_x} \sim \omega_2^{k-l} \oplus \omega_2^{kl-1}$ or

$$\begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}.$$

Thus in fact ϕ_1 must factor through $h_{R_\emptyset,\mathbb{F}_l^{ac},\psi_0}(U_{H_0}(\mathfrak{n}_0)) = h_{k,\mathbb{F}_l^{ac},\psi_0}(U_{H_0}(\mathfrak{n}_0))$. It follows from the first part of corollary 5.2 that ϕ_1 gives rise to a map

$$\phi_0 : h_{\eta^{k-2},\mathcal{O},\psi_0}(U_{H_0}(\mathfrak{n}_0)) \longrightarrow \mathbb{F}_l^{ac}$$

such that $\ker \phi_0$ is non-Eisenstein and $\overline{\rho}_{\phi_0} \sim \overline{\rho}|_{G_F}$. The proposition follows. □

Combining the lemma 5.4 with the main theorem of [SW1], we immediately obtain the following corollary.

Corollary 5.5 *Let $l > 3$ be a prime. Suppose that $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l^{ac})$ is a continuous odd representation with $\overline{\rho}|_{I_l} \sim \omega_2^{k-1} \oplus \omega_2^{l(k-1)}$ for some integer $2 \leq k \leq l$. Then there is a Galois totally real field F in which l splits completely, a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and an embedding $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ such that*

1. $\overline{\rho}|_{G_F} \sim \overline{\rho}_{\pi,\lambda}$;
2. π_∞ *has weight* 2;
3. *for each finite place* x *of* F *not dividing* l, π_x *is unramified; and*
4. *for each place* x *of* F *above* l, *the conductor of* π_x *divides* x.

Now we can use corollary 5.2 to obtain a further refinement of proposition 4.1.

Lemma 5.6 *Let* $l > 3$ *be a prime. Suppose that* $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l^{ac})$ *is a continuous odd representation with* $\overline{\rho}|_{I_l} \sim \omega_2^{k-1} \oplus \omega_2^{l(k-1)}$ *for some integer* $2 \leq k \leq l$. *Then there is a Galois totally real field* F *of even degree in which* l *splits completely, a regular algebraic cuspidal automorphic representation* π *of* $GL_2(\mathbb{A}_F)$ *and an embedding* $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ *such that*

1. $\overline{\rho}|_{G_F} \sim \overline{\rho}_{\pi,\lambda}$;
2. π_∞ *has weight* k; *and*
3. π_x *is unramified at every finite place* x *of* F.

Proof: Now let F, π, λ be as provided by corollary 5.5. Also denote by $\psi_0 : (\mathbb{A}_F^\infty)^\times / F^\times \to (\mathbb{Q}_l^{ac})^\times$ be the character such that $\epsilon(\psi_0 \circ \mathrm{Art}^{-1})$ equals the determinant of $\rho_{\pi,\lambda}$. Thus ψ_0 is unramified away from l. Note also that if $a \in \mathcal{O}_{F,l}^\times$ then $\psi_0(a)$ is the Teichmüller lift of $(\mathrm{N}a)^{2-k} \bmod l$. Let D be the division algebra with centre F which is ramified at exactly the infinite places of F. Let $\mathcal{O}_D$ be a maximal order in D and fix an isomorphism $\mathcal{O}_{D,x} \cong M_2(\mathcal{O}_{F,x})$ for each finite place x of F. Let $U_0 = \prod_y GL_2(\mathcal{O}_{F,y})$. There is a homomorphism

$$\phi_0 : h_{\overline{\eta}^{k-2}, \mathbb{F}_l^{ac}, \psi_0}(U_0(\mathcal{O}_F, l)) \longrightarrow \mathbb{F}_l^{ac}$$

with $\ker \phi_0$ non-Eisenstein and $\overline{\rho}_{\phi_0} \sim \overline{\rho}|_{G_F}$. By corollary 5.2 this factors through $h_{k,\mathbb{F}_l^{ac},\psi_0}(U_0)$ and the proposition follows. $\Box$

Finally we have the following version of our potential version of Serre's conjecture.

Theorem 5.7 *Let* $l > 3$ *be a prime. Suppose that* $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l^{ac})$ *is a continuous irreducible odd representation with* $\overline{\rho}|_{G_l}$ *irreducible. Then there is a Galois totally real field* F *of even degree in which* l *splits completely, a regular algebraic cuspidal automorphic representation* π *of* $GL_2(\mathbb{A}_F)$ *and an embedding* $\lambda : M_\pi \hookrightarrow \mathbb{Q}_l^{ac}$ *such that*

1. $\overline{\rho}|_{G_F} \sim \overline{\rho}_{\pi,\lambda}$;
2. π_∞ *has weight* $k_{\overline{\rho}}$, *where* $k_{\overline{\rho}}$ *is the weight associated to* $\overline{\rho}|_{G_l}$ *by Serre in [S2]; and*
3. π_x *is unramified for every finite place* x *of* F.

Proof: From the definition of $k_{\overline{\rho}}$ we see that there is an integer $0 \leq c < l-1$ such that $2 \leq k_{\overline{\rho}} - c(l+1) \leq l$ and $(\overline{\rho} \otimes \epsilon^{-c})|_{I_l} \sim \omega_2^{k_{\overline{\rho}}-1-c(l+1)} \oplus \omega_2^{l(k_{\overline{\rho}}-1)-c(l+1)}$. By lemma 5.6 we can find a Galois totally real field F of even degree in which l splits completely and a regular algebraic cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ such that

1. $(\overline{\rho} \otimes \epsilon^{-c})|_{G_F}$ is equivalent to $\overline{\rho}_{\pi,\lambda}$ for some prime $\lambda | l$ and some embedding $k(\lambda) \hookrightarrow \mathbb{F}_l^{ac}$;
2. π_∞ has weight $k_{\overline{\rho}} - c(l+1)$; and
3. π_x is unramified at every finite place x of F.

By lemma 1.3 we can find, for some character ψ, a homomorphism

$$\phi : h_{k_{\overline{\rho}}-c(l+1), \mathbb{F}_l^{ac}, \psi}(U_0) \to \mathbb{F}_l^{ac}$$

with non-Eisenstein kernel such that $\overline{\rho}_\phi \cong (\overline{\rho} \otimes \epsilon^{-c})|_{G_F}$. The theorem now follows from lemma 5.3. □

6 Applications

Combining theorem 2.1 of [Tay4], theorem 5.7, theorem 3.3 and a standard descent argument (see for example the proof of theorem 2.4 of [Tay3]) we obtain our main theorem.

Theorem 6.1 *Let $l > 3$ be a prime and let $2 \leq k \leq l-1$ be an integer. Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{\mathbb{Q}_l^{ac}})$ be a continuous irreducible representation such that*

- *ρ is ramifies at only finitely many primes,*
- $\det \rho(c) = -1$,
- *$\rho|_{G_l}$ is crystalline with Hodge-Tate numbers 0 and $1-k$.*

Let $\overline{\rho}$ denote the reduction of ρ modulo the maximal ideal of $\mathcal{O}_{\mathbb{Q}_l^{ac}}$. If $\overline{\rho}|_{G_l}$ is irreducible assume that $\overline{\rho}$ restricted to $\mathbb{Q}_l(\sqrt{(-1)^{(l-1)/2} l})$ is irreducible. (This will be the case if, for instance, $2k \neq l+3$.) Then there is a Galois totally real field F in which l is unramified with the following property. For each subfield $E \subset F$ with Gal (F/E) *soluble there is a regular algebraic cuspidal automorphic representation π_E of $GL_2(\mathbb{A}_E)$ and an embedding λ of the feild of coefficients of π_E into $\mathbb{Q}_l^{ac}$ such that*

- $\rho_{\pi_E,\lambda} \sim \rho|_{G_E}$,
- *$\pi_{E,x}$ is unramified for all places x of E above l, and*
- *$\pi_{E,\infty}$ has weight k.*

(We explain the parenthetical comment. In the case discussed in that comment $\overline{\rho}|_{I_l} = \omega_2^{k-1} \oplus \omega_2^{l(k-1)}$ and so $\overline{\rho}|_{I_{\mathbb{Q}_l(\sqrt{\pm l})}} = (\omega_2')^{2(k-1)} \oplus (\omega_2')^{2l(k-1)}$ where ω_2' is the fundamental character of level 2 of $I_{\mathbb{Q}_l(\sqrt{\pm l})}$. The assumption $k \neq (l+3)/2$ tells us that $(l+1) \nmid 2(k-1)$ so that $\overline{\rho}|_{G_{\mathbb{Q}_l(\sqrt{\pm l})}}$ is absolutely irreducible.) Combining this with the main theorem of [Bl] we deduce the following corollary.

Corollary 6.2 *Keep the assumptions of theorem 6.1. If ρ is unramified at a prime p and if α is an eigenvalue of $\rho(\mathrm{Frob}_p)$ then $\alpha \in \mathbb{Q}^{ac}$ and for any isomorphism $i : \mathbb{Q}_l^{ac} \stackrel{\sim}{\to} \mathbb{C}$ we have*

$$|i\alpha|^2 \leq p^{(k-1)/2}.$$

(We remark that we can deduce this corollary for all but finitely many primes p by appealing to theorem 3.4.6 of [BL] instead of the main theorem of [Bl].) Continue to assume that ρ satisfies the hypotheses of theorem 6.1. If $p \neq l$ and if $i : \mathbb{Q}_l^{ac} \stackrel{\sim}{\to} \mathbb{C}$ then we define

$$L_p(i\rho, X) = i \det(1 - \rho_{I_p}(\mathrm{Frob}_p)X) \in \mathbb{C}[X].$$

Corollary 6.2 tells us that

$$L^l(i\rho, s) = \prod_{p \neq l} L_p(i\rho, p^{-s})^{-1}$$

defines a meromorphic function in $\mathrm{Re}\, s > (k+1)/2$.

Choose a non-trivial additive character $\Psi = \prod \Psi_p : \mathbb{A}/\mathbb{Q} \to \mathbb{C}^\times$ with $\ker \Psi_l = \mathbb{Z}_l$ and $\Psi_\infty(x) = e^{2\pi\sqrt{-1}x}$. Also choose a Haar measure $dx = \prod dx_p$ on $\mathbb{A}_F$ with dx_∞ the usual measure on $\mathbb{R}$, with $dx_l(\mathbb{Z}_l) = 1$ and with $dx(\mathbb{A}_F/F) = 1$. If $p \neq l$ we will let $\mathrm{WD}(\rho|_{G_p})$ denote the Weil-Deligne representation associated to $\rho|_{G_p}$. Then we define

$$\epsilon(i\rho, s) = \sqrt{-1}^k \prod_{p \neq l} \epsilon(i\mathrm{WD}(\rho^\vee|_{G_p}) \otimes |\mathrm{Art}^{-1}|_p^{-s}, \Psi_p, dx_p).$$

(See [Tat].) Note that $\epsilon(i\rho, s) = WN^{k/2-s}$ where W is independent of s, and where N is the (prime to l) conductor of ρ. The proof of corollary 2.2 of [Tay4] then gives the following corollary.

Corollary 6.3 *Keep the assumptions of theorem 6.1 and let $i : \mathbb{Q}_l^{ac} \stackrel{\sim}{\to} \mathbb{C}$. There is a rational function $L_l(\rho, X)$ such that if we set*

$$L(i\rho, s) = L^l(i\rho, s) L_l(i\rho, l^{-s})^{-1}$$

then $L(i\rho, s)$ has meromorphic extension to the entire complex plane and satisfies the functional equation

$$(2\pi)^{-s}\Gamma(s)L(i\rho, s) = \epsilon(i\rho, s)(2\pi)^{s-k}\Gamma(k-s)L(i(\rho^\vee \otimes \epsilon^{k-1}), k-s).$$

The proof of corollary 2.4 of [Tay4] also gives us the following result.

COROLLARY 6.4 *Keep the assumptions of theorem 6.1 and if $k = 2$ further assume that for some prime $p \neq l$ we have*

$$\rho|_{G_p} \sim \begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}.$$

Then ρ occurs in the l-adic cohomology (with coefficients in some Tate twist of the constant sheaf) of some variety over $\mathbb{Q}$.

By a *rank d weakly compatible system of l-adic representations* $\mathcal{R}$ over $\mathbb{Q}$ we shall mean a 5-tuple $(M, S, \{Q_p(X)\}, \{\rho_\lambda\}, \{n_1, ..., n_d\})$ where

- M is a number field;
- S is a finite set of rational primes;
- for each prime $p \notin S$ of $\mathbb{Q}$, $Q_p(X)$ is a monic degree d polynomial in $M[X]$;
- for each prime λ of M (with residue characteristic l say)

  $$\rho_\lambda : G_\mathbb{Q} \longrightarrow GL_d(M_\lambda)$$

  is a continuous representation such that, if $l \notin S$ then $\rho_\lambda|_{G_l}$ is crystalline, if $p \notin S \cup \{l\}$ then ρ_λ is unramified at p and $\rho_\lambda(\mathrm{Frob}_p)$ has characteristic polynomial $Q_p(X)$; and
- $\{n_1, ..., n_d\}$ is a multiset (i.e. set with multiplicities) of integers such that for all primes λ of M (lying above a rational prime l) the representation $\rho_\lambda|_{G_l}$ is Hodge-Tate with numbers $\{n_1, ..., n_d\}$.

We will call $\{n_1, ..., n_d\}$ the *Hodge numbers* of $\mathcal{R}$. We will call $\mathcal{R}$ *strongly compatible* if for each rational prime p there is a Weil-Deligne representation $\mathrm{WD}_p(\mathcal{R})$ of $W_{\mathbb{Q}_p}$ such that for primes λ of M not dividing p, $\mathrm{WD}_p(\mathcal{R})$ is equivalent to the Frobenius semi-simplification of the Weil-Deligne representation associated to $\rho_\lambda|_{G_p}$. We will call a rank 2 weakly compatible system $\mathcal{R}$ *regular* if the Hodge numbers are distinct and for one, and hence all, primes λ of M we have $\det \rho_\lambda(c) = -1$.

We remark that whatever is meant by a "motive", the l-adic realisations of a "motive" would give rise to weakly compatible systems of l-adic representations which are generally expected to be strongly compatible. Moreover one can use the Hodge realisation to see that if the Hodge numbers of a rank 2 "motive" are distinct then the associated system of l-adic representations is regular in the above sense. This explains the perhaps somewhat unnatural definition of regularity given above.

The following lemma is an easy consequence of the characterisation of one dimensional Hodge-Tate representations of $G_\mathbb{Q}$.

Lemma 6.5 *If $\mathcal{R}/\mathbb{Q}$ is a rank 2 weakly compatible system of l-adic representations and if ρ_λ is absolutely reducible for one λ, then ρ_λ is absolutely reducible for all λ.*

We will call a rank 2 weakly compatible system of l-adic representations *reducible* if the hypothesis (and hence the conclusion) of the previous lemma holds. Otherwise we call it *irreducible.*

Theorem 6.6 *Suppose that $\mathcal{R} = (M, S, \{Q_x(X)\}, \{\rho_\lambda\}, \{n_1, n_2\})/\mathbb{Q}$ is a regular, irreducible, rank 2 weakly compatible system of l-adic representations with $n_1 > n_2$.*

1. *There is a Galois totally real field such that for any $i : M \hookrightarrow \mathbb{C}$ there is a regular algebraic cuspidal automorphic representation of $GL_2(\mathbb{A}_F)$ with $L(i\mathcal{R}|_{G_F}, s) = L(\pi, s)$.*
2. *For all rational primes $p \notin S$ and for all $i : M \hookrightarrow \mathbb{C}$ the roots of $i(Q_p(X))$ have absolute value $p^{-(n_1+n_2)/2}$.*
3. *$\mathcal{R}$ is strongly compatible.*
4. *Fix $i : M \hookrightarrow \mathbb{C}$. If we define*

$$L(i\mathcal{R}, s) = \prod_p L_p(i\mathrm{WD}_p(\mathcal{R})^\vee, s)^{-1}$$

and

$$\epsilon(i\mathcal{R}, s) = i^{1+n_1-n_2} \prod_p \epsilon(i\mathrm{WD}_p(\mathcal{R})^\vee \otimes |\mathrm{Art}^{-1}|_p^{-s}, \Psi_p, dx_p)$$

then the product defining $L(i\mathcal{R}, s)$ converges to a meromorphic function in $\mathrm{Re}\, s > 1 - (n_1 + n_2)/2$ and $L(i\mathcal{R}, s)$ has meromorphic continuation to the entire complex plane and satisfies a functional equation

$$(2\pi)^{-(s+n_1)}\Gamma(s + n_1)L(i\mathcal{R}, s) = \epsilon(i\mathcal{R}, s)(2\pi)^{s+n_2-1}\Gamma(1 - n_2 - s)L(i\mathcal{R}^\vee, 1 - s).$$

Proof: We may assume that $n_1 = 0$. For all but finitely many primes λ of M the representation ρ_λ satisfies the hypotheses of theorem 6.1. The first part follows immediately from that theorem and the second part from corollary 6.2. Choose one such prime λ and fix an embedding $M_\lambda \subset \mathbb{Q}_l^{ac}$. Let F be as in theorem 6.1 and write

$$1 = \sum_j m_j \mathrm{Ind}\,_{\mathrm{Gal}\,(F/E_j)}^{\mathrm{Gal}\,(F/\mathbb{Q})} \chi_j$$

where $m_j \in \mathbb{Z}$, $\mathrm{Gal}\,(F/E_j)$ is soluble and χ_j is a character of $\mathrm{Gal}\,(F/E_j)$. For each j we have a regular algebraic cuspidal automorphic representation π_j of

$GL_2(\mathbb{A}_{E_j})$ with field of coefficients M_j and an embedding $\lambda_j : M_j \hookrightarrow \mathbb{Q}_l^{ac}$ such that

$$\rho_{\pi_j,\lambda_j} \sim \rho_\lambda|_{G_{E_j}}.$$

We see in particular that $\lambda_j : M_j \hookrightarrow M$. Thus any embedding $\lambda' : M \hookrightarrow \mathbb{Q}_{l'}^{ac}$ gives rise to an embedding $\lambda_j' : M_j \hookrightarrow \mathbb{Q}_{l'}^{ac}$. From the Cebotarev density theorem we see that

$$\rho_{\pi_j,\lambda_j'} \sim \rho_{\lambda'}|_{G_{E_j}}$$

and hence that

$$\rho_{\lambda'} = \sum_j m_j \mathrm{Ind}_{\mathrm{Gal}\,(\mathbb{Q}^{ac}/E_i)}^{\mathrm{Gal}\,(\mathbb{Q}^{ac}/\mathbb{Q})} \rho_{\pi_j,\lambda_j'} \otimes \chi_j.$$

As the $\rho_{\pi_j,\lambda_j'}$ are strongly compatible (see [Tay1]), the same is true for the $\rho_{\lambda'}$. (To check compatibility of the nilpotent operators in the Weil-Deligne representations one notices that it suffices to check that they are equal after any finite base change.) Moreover we see that

$$L(i\mathcal{R}, s) = \prod_j L(\pi_j \otimes (\chi_j \circ \mathrm{Art} \circ \det), s)^{m_j}$$

and that

$$\epsilon(i\mathcal{R}, s) = \prod_j \epsilon(\pi_j \otimes (\chi_j \circ \mathrm{Art} \circ \det), s)^{m_j},$$

and the fourth part of the theorem follows. □

As an example suppose that $X/\mathbb{Q}$ is a rigid Calabi-Yau 3-fold. Let $\mathcal{X}/\mathbb{Z}$ denote a model for X. Also let $\zeta_X(s)$ denote the zeta function of X, so that

$$\zeta_X(s) = \prod_p \zeta_{X,p}(p^{-s})^{-1},$$

where $\zeta_{X,p}(T)$ is a rational function of T and for all but finitely many p we have

$$\zeta_{X,p}(T) = \prod_x (1 - T^{[k(x):\mathbb{F}_p]})$$

where x runs over closed points of $\mathcal{X} \times \mathbb{F}_p$. If we set

$$Z_X(s) = ((s-1)(s-3))^{-1}(2\pi)^{-s \dim H^2(X(\mathbb{C}),\mathbb{R})}\Gamma(s-1)^{\dim H^2(X(\mathbb{C}),\mathbb{R})^{c=1}}$$
$$\Gamma(s-2)^{\dim H^2(X(\mathbb{C}),\mathbb{R})^{c=-1}}\zeta_X(s),$$

then we have that

$$Z_X(s) = AB^{s-2}Z_X(4-s)$$

where B is a non-zero rational number and where $A = \pm 1$. (To see this note that

- $H^0(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l) = \mathbb{Q}_l$ and $H^6(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l) = \mathbb{Q}_l(-3)$;

- $H^1(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l) = H^5(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l) = (0)$;
- $H^{2,0}(X(\mathbb{C}), \mathbb{C}) = H^{0,2}(X(\mathbb{C}), \mathbb{C}) = (0)$ and so by Lefschetz's theorem there is finite dimensional $\mathbb{Q}$-vector space W with a continuous action of $G_{\mathbb{Q}}$ such that
$$H^2(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l) \cong W \otimes_{\mathbb{Q}} \mathbb{Q}_l(-1)$$
and
$$H^4(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l) \cong W^\vee \otimes_{\mathbb{Q}} \mathbb{Q}_l(-2)$$
for all rational primes l; and
- $\{H^3(X \times \mathbb{Q}^{ac}, \mathbb{Q}_l)\}$ forms a regular, rank two weakly compatible system in the above sense.

Thus it suffices to combine the above theorem with the functional equation for Artin L-series.)

Corrections to [Tay4].

We are extremely grateful to Laurent Clozel for raising the following points. All the references below are to [Tay4].

- The third bulleted point on page 130 should read $\det \overline{\rho} = \epsilon$. (Without this change the choice of a_λ at the top of page 136 becomes impossible.)
- It would be clearer if the parenthetical comment "(as $\beta_v - \beta_v^c$ is coprime to p)" read "(as $\beta_v \beta_v^c = \psi(\phi_v)\psi^c(\phi_v) = p$ and $\beta_v - \beta_v^c$ is coprime to p)".
- Before the "i.e." in the middle of page 135 it would be clearer to add a parenthetical explanation "(note that $\mathrm{End}_{\mathcal{O}_M}(A_1)$ is the centraliser of $\mathcal{O}_M$ in $M_{[N:\mathbb{Q}(\beta_v)]}(\mathcal{O}_{\mathbb{Q}(\beta_v)})$, which is just $\mathcal{O}_N$)".
- The superscript $\mathrm{Gal}\,(L/K)$ in the fourth displayed formula on page 135 should read $\mathrm{Gal}\,(\widetilde{F}_v/F_v)$.
- After the fourth displayed formula on page 135 it would be clearer to add the parenthetical comment: "(N.B. Because $[\widetilde{F}_v : F_v] | \#\chi_v(I_v) | \#k^\times$ and because N_0 contains a primitive $\#k^\times$ root of one, N contains a primitive $[\widetilde{F}_v : F_v]$ root of one.)".
- The proof of lemma 1.4 is wrong. A correct proof can be given as follows. "Choose $z \in (i\mathbb{R}_{>0})^{\mathrm{Hom}\,(M,\mathbb{R})}$. Let M act on $\mathbb{C}^{\mathrm{Hom}\,(M,\mathbb{R})}$ by acting via τ on the τ-component. Set $A = \mathbb{C}^{\mathrm{Hom}\,(M,\mathbb{R})}/(\mathfrak{d}_M^{-1} 1 + \mathcal{O}_M z)$ (where 1 denotes the vector $(1, ..., 1)$). This complex torus is an abelian variety with an action of $\mathcal{O}_M$, which is actually defined over $\mathbb{R}$ (in such a way that complex conjugation on $A(\mathbb{C})$ corresponds to complex conjugation

on $\mathbb{C}^{\mathrm{Hom}\,(M,\mathbb{R})}$). Moreover $\mathcal{P}(A,i) \cong \mathcal{O}_M^+$, where $\alpha \in \mathcal{O}_M$ corresponds to the alternating Riemannian form

$$E(x+yz, u+vz) = \mathrm{tr}_{\,M/\mathbb{Q}}\alpha(yu-xv)$$

for $x,y,u,v \in M \otimes_{\mathbb{Q}} \mathbb{R}$."

- At the end of the second sentence of the paragraph before theorem 1.6 add "and $\det \overline{\rho} = \epsilon$" after "the case that $\overline{\rho}$ has insoluble image".

- With the above changes, specifically adding $\det \overline{\rho} = \epsilon$ in two places, theorem 1.6 requires some further proof. The following will suffice: "We may assume that $\overline{\rho}$ has insoluble image. Choose a totally real quadratic extension F'/F in which all primes above l split and a finite extension k'/k and a character $\xi : G_{F'} \to (k')^\times$ such that $\det \overline{\rho}|_{G_{F'}} = \epsilon\xi^2$. (This is possible as the obstruction to taking the square root of a character lies in the two part of the Brauer group.) Now work with $\overline{\rho}' = \overline{\rho} \otimes \xi^{-1} : G_{F'} \to GL_2(k')$, and find p, N, M, λ, $\wp$, L, ψ, E'/F' and A' as above. Let E be the normal closure of E'/F. Then l and p split completely in E/F. Take $A = A' \times_{E'} E$ and argue as above."

References

[AS] A.Ash and G.Stevens, *Modular forms in characteristic l and special values of their L-functions*, Duke Math. J. 53 (1986), 849–868.

[BL] J.-L.Brylinski and J.-P.Labesse, *Cohomologie d'intersection et fonctions L de certaines variétés de Shimura*, Ann. Sci. ENS 17 (1984), 361-412.

[Bl] D.Blasius, *Hilbert modular forms and the Ramanujam conjecture*, preprint available at www.math.ucla.edu/~blasius/papers.html .

[Bu] K.Buzzard, *The levels of modular representations*, PhD thesis, Cambridge University, 1995.

[Ca1] H.Carayol, *Sur les représentations p-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. ENS (4) 19 (1986), 409-468.

[Ca2] H.Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, in "p-adic monodromy and the Birch and Swinnerton-Dyer conjecture", Contemp. Math. 165, Amer. Math. Soc., 1994.

[Cl] L.Clozel, *Motifs et formes automorphes: applications du principe de fonctorialité*, in "Automorphic forms, Shimura varieties, and L-functions, Vol. I,(Ann Arbor, MI, 1988)" eds. L. Clozel and J. S. Milne, Perspect. Math. 10, Academic Press, 1990.

[CDT] B.Conrad, F.Diamond and R.Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, JAMS 12 (1999), 521-567.

[DDT] H.Darmon, F.Diamond and R.Taylor, *Fermat's last theorem*, in "Elliptic curves, modular forms and Fermat's last theorem" Internat. Press, 1997.

[Dia] F.Diamond, *The Taylor-Wiles construction and multiplicity one*, Invent. Math. 128 (1997), 379-391.

[Ed] S.Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. 109 (1992), 563-594.

[Fa] G.Faltings, *Crystalline cohomology and p-adic Galois representations*, Algebraic Analysis, Geometry and Number Theory, Proc. JAMI Inaugural Conference, Johns-Hopkins Univ. Press (1989), 25-79.

[FL] J.-M.Fontaine and G.Laffaille, *Construction de représentations p-adiques*, Ann. Sci. Ecole Norm. Sup. (4) 15 (1982), 547–608.

[FM] J.-M.Fontaine and B.Mazur, *Geometric Galois representations*, in "Elliptic curves, modular forms and Fermat's last theorem", International Press 1995.

[Fu] K.Fujiwara, *Deformation rings and Hecke algebras in the totally real case*, preprint.

[HT] R.Taylor and M.Harris, *The geometry and cohomology of some simple Shimura varieties*, Annals of Math. Studies 151, PUP 2001.

[Lang] S.Lang, *Complex multiplication*, Springer 1983.

[Langl] R.Langlands, *Base change for $GL(2)$*, PUP 1980.

[Rap] M.Rapoport, *Compactifications de l'espace de modules de Hilbert-Blumental*, Comp. Math. 36 (1978), 255-335.

[S1] J.-P.Serre, *Abelian l-adic representations and elliptic curves*, W.A.Benjamin 1968.

[S2] J.-P.Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179-230.

[SW1] C.Skinner and A.Wiles, *Base change and a problem of Serre*, Duke Math. J. 107 (2001), 15–25.

[SW2] C.Skinner and A.Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse Math. 10 (2001), 185–215.

[Tat] J.Tate, *Number theoretic background*, in "Automorphic forms, representations and L-functions, part 2", Proc. Sympos. Pure Math. XXXIII, AMS 1979.

[Tay1] R.Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. 98 (1989), 265-280.

[Tay2] R.Taylor, *On Galois representations associated to Hilbert modular forms II*, in "Elliptic curves, modular forms and Fermat's last theorem" eds. J.Coates and S.T.Yau, International Press 1995.

[Tay3] R.Taylor, *On icosahedral Artin representations II*, Amer. J. Math. 125 (2003), 549–566.

[Tay4] R.Taylor, *On a conjecture of Fonatine and Mazur*, Journal of the Institute of Mathematics of Jussieu 1 (2002), 125-143.

[Tu] J.Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS 5 (1981), 173-175.

[TW] R.Taylor and A.Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553-572.

[W1] A.Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. 94 (1988), 529–573.

[W2] A.Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443-551.

Richard Taylor
Department of Mathematics
Harvard University,
Cambridge
MA 02138
USA
rtaylor@math.harvard.edu

Siegel Varieties and p-Adic Siegel Modular Forms

To John Coates for his sixtieth birthday

J. Tilouine

Received: November 30, 2005
Revised: August 10, 2006

Abstract. In this paper, we present a conjecture concerning the classicality of a genus two overconvergent Siegel cusp eigenform whose associated Galois representation happens to be geometric, and more precisely, given by the Tate module of an abelian surface. This conjecture is inspired by the Fontaine-Mazur conjecture. It generalizes known results in the genus one case, due to Kisin, Buzzard-Taylor and Buzzard. The main difference in the genus two case is the complexity of the arithmetic geometry involved. This is why most of the paper consists in recalling (mostly with proofs) old and new results on the bad reduction of parahoric type Siegel varieties, with some consequences on their rigid geometry. Our conjecture would imply, in certain cases, a conjecture posed by H. Yoshida in 1980 on the modularity of abelian surfaces defined over the rationals.

2000 Mathematics Subject Classification:
11F33, 11F46, 11F80, 11G18
Keywords and Phrases:
Arithmetic Siegel varieties, q-expansion, Bad reduction of Siegel varieties of parahoric level, Overconvergent Siegel modular forms, Galois representations

In a previous paper, we showed under certain assumptions (Theorem 4 of [26]) that a degree four symplectic Galois representation ρ with singular Hodge-Tate weights which is congruent to a cohomological modular Galois representation (we say then that ρ is residually cohomologically modular) is p-adically modular. The precise definitions of the expressions above can be found in [26] Sect.2 and 4. As a corollary, we obtain that certain abelian surfaces

$A_{/\mathbb{Q}}$ do correspond, if they are residually cohomologically modular, to overconvergent Siegel cusp forms of weight $(2,2)$ (see Theorem 8 of [26]), in the sense that their Galois representations coincide. This result fits a Generalized Shimura-Taniyama Conjecture due to H. Yoshida ([30], Section 8.2) according to which for any irreducible abelian surface A defined over $\mathbb{Q}$, there should exist a genus two holomorphic Siegel cusp eigenform g of weight $(2,2)$ such that $L(h^1(A),s) = L_{\mathrm{spin}}(g,s)$, where $L(h^1(A),s)$ is the Grothendieck L function associated to the motive $h^1(A)$ and $L_{\mathrm{spin}}(g,s)$ is the degree four automorphic L function associated to g (with Euler factors defined via Hecke parameters rather than Langlands parameters, for rationality purposes). One should notice that this conjecture presents a new feature compared to the genus one analogue. Namely, contrary to the genus one case, the weight $(2,2)$ occuring here is not cohomological; in other words, the Hecke eigensystem of g does not occur in the singular cohomology of the Siegel threefold (it occurs however in the coherent cohomology of this threefold). In particular, the only way to define the Galois representation $\rho_{g,p}$ associated to such a form g, either classical or overconvergent, is to use a p-adic limit process, instead of cutting a piece in the étale cohomology with coefficients of a Siegel threefold. This can be achieved in our case because g fits into a two-variable Hida family of p-nearly ordinary cusp eigenforms. Note that, more generally, for a classical cusp eigenform g of weight $(2,2)$ with (finite) positive slopes for its Hecke eigenvalues at p, one believes that two-variable Coleman families of cusp eigenforms passing through g in weight $(2,2)$ could also be constructed, and this would allow a similar construction of $\rho_{g,p}$.

For our p-nearly ordinary overconvergent g, Theorem 8 of [26] states that the associated Galois representation $\rho_{g,p}$ does coincide with the p-adic realization of a motive $h^1(A)$. Therefore, $\rho_{g,p}$ is geometric; several results in the analogue situation for genus 1 (see [18], [6] and [7]) lead us to conjecture that this g is actually classical.

The goal of the present paper is to generalize slightly and state precisely this conjecture (Sect.4.2). We also take this opportunity to gather geometric facts about Siegel threefolds with parahoric level p, which seem necessary for the study of the analytic continuation of such overconvergent cusp eigenforms to the whole (compactified) Siegel threefold; the rigid GAGA principle would then imply the classicity of such g. We are still far from fulfilling this program. However, we feel that the geometric tools presented here, although some of them can actually be found in the literature, may be useful for various arithmetic applications besides this one, for instance to establish the compatibility between global and local Langlands correspondence for cusp forms of parahoric level for $GSp(4,\mathbb{Q})$.

As a final remark, we should point out that there exist other Generalized Shimura-Taniyama Conjectures for submotives of rank 3 resp.4 of the motive $h^1(A)$ for certain abelian threefolds resp. fourfolds A (see [3]). For those, Theorem 8 of [26] seems transposable; the question of classicity for the resulting overconvergent cusp eigenforms for unitary groups $U(2,1)$ resp. $U(2,2)$ could then be posed in a similar way. It would then require a similar study of the (rigid) geometry of Shimura varieties of parahoric type for the corresponding groups.

Part of this paper has been written during visits at NCTS (Taiwan) and CRM (Montreal). The excellent working conditions in these institutions were appreciated. The author wishes to express his thanks to Professors Jing Yu and A. Iovita for their invitations, as well as the Clay Institute which financed part of the stay in Montreal. Discussions with H. Hida, A. Iovita, C.-F. Yu and especially A. Genestier were very useful to remove several falsities and add truths to an earlier draft (but the author alone is responsible for the remaining errors).

Contents

1 Notations

Let

$$G = \mathrm{GSp}(4) = \{X \in \mathrm{GL}_4; {}^tXJX = \nu \cdot J\}$$

be the split reductive group scheme over $\mathbb{Z}$ of symplectic simitudes for the antisymmetric matrix J, given by its 2×2 block decomposition: $J = \begin{pmatrix} 0 & -s \\ s & 0 \end{pmatrix}$ where s is the 2×2 antidiagonal matrix whose non zero entries are 1. This group comes with a canonical character $\nu : X \mapsto \nu(X) \in \mathbb{G}_m$ called the similitude factor. The center of G is denoted by Z, the standard (diagonal) maximal torus by T and the standard (upper triangular) Borel by B; U_B denotes its unipotent radical, so that $B = TU_B$. Let $\gamma_P = t_1/t_2$ resp. $\gamma_Q = \nu^{-1}t_2^2$ be the short, resp. the long simple root associated to the triple (G, B, T). The standard maximal parabolic $P = MU$, associated to γ_P, is called the Klingen parabolic, while the standard maximal parabolic $Q = M'U'$, associated to γ_Q, is the Siegel parabolic. The Weyl group of G is denoted W_G. It is generated by the two reflexions s_P and s_Q induced by conjugation on T by $\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix}$ resp. $\begin{pmatrix} 1 & & \\ & s & \\ & & 1 \end{pmatrix}$. Let us fix a pair of integers $(a, b) \in \mathbb{Z}^2$, $a \geq b \geq 0$; we identify it with a dominant weight for (G, B, T), namely the character

$$T \ni t = diag(t_1, t_2, \nu^{-1}t_2, \nu^{-1}t_1) \mapsto t_1^a t_2^b$$

Let $V_{a,b}$ be a generically irreducible algebraic representation of G associated to (a,b) over $\mathbb{Z}$.
Let $\mathbb{A} = \mathbb{A}_f \times \mathbb{Q}_\infty$ be the ring of rational adeles. Fix a compact open subgroup K of $G_f = G(\mathbb{A}_f)$; let $N \geq 1$ be an integer such that $K = K^N \times K_N$ with $K^N = G(\mathbb{Z}^N)$ maximal compact and $K_N = \prod_{\ell | N} K_\ell$ for local components K_ℓ to be specified later.
Let $\mathcal{H}^N$ be the unramified Hecke algebra outside N (that is, the tensor product algebra of the unramified local Hecke algebras at all prime-to-N rational primes); for each rational prime ℓ prime to N, one defines the abstract Hecke polynomial $P_\ell \in \mathcal{H}^N[X]$ as the monic degree four polynomial which is the minimal polynomial of the Hecke Frobenius at ℓ (see Remarks following 3.1.5 in [12]).
Let C_∞ be the subgroup of $G_\infty = G(\mathbb{Q}_\infty)$ generated by the standard maximal compact connected subgroup K_∞ and by the center Z_∞.
For any neat compact open subgroup L of $G(\mathbb{A}_f)$, the adelic Siegel variety of level L is defined as: $S_L = G(\mathbb{Q})\backslash G(\mathbb{A})/LC_\infty$; it is a smooth quasi-projective complex 3-fold. If $L \subset L'$ are neat compact open subgroups of G_f, we have a finite etale transition morphism $\phi_{L,L'} : S_L \to S_{L'}$.

2 Integral models and local models

Let K be a compact open subgroup of $G(\widehat{\mathbb{Z}})$ such that $K(N) \subset K$. For any integer $M \geq 1$, we write K_M resp. K^M for the product of the local components of K at places dividing M, resp. prime to M.
Let p be a prime not dividing N we denote by I, Π_P resp. Π_Q the Iwahori subgroup, Klingen parahoric, resp. Siegel parahoric subgroup of $G(\mathbb{Z}_p)$. We consider $K_B(p) = K \cap I \times K^p$, $K_P(p) = K \cap \Pi_P \times K^p$ and $K_Q(p) = K \cap \Pi_Q \times K^p$ and the corresponding Shimura varieties $S_B(p)$, $S_P(p)$ resp. $S_Q(p)$.
Let us consider the moduli problems

$$\mathcal{F}_\emptyset : \mathbb{Z}[\frac{1}{N}]-\mathrm{Sch} \to \mathrm{Sets}, \quad S \mapsto \{A, \lambda, \overline{\eta})_{/S}\}/\sim,$$

$$\mathcal{F}_B : \mathbb{Z}[\frac{1}{N}]-\mathrm{Sch} \to \mathrm{Sets}, \quad S \mapsto \{A, \lambda, \overline{\eta}, H_1 \subset H_2 \subset A[p])_{/S}\}/\sim,$$

$$\mathcal{F}_P : \mathbb{Z}[\frac{1}{N}]-\mathrm{Sch} \to \mathrm{Sets}, \quad S \mapsto \{A, \lambda, \overline{\eta}, H_1 \subset A[p])_{/S}\}/\sim$$

and

$$\mathcal{F}_Q : \mathbb{Z}[\frac{1}{N}]-\mathrm{Sch} \to Sets, \quad S \mapsto \{A, \lambda, \overline{\eta}, H_2 \subset A[p])_{/S}\}/\sim$$

where A/S is an abelian scheme, λ is a principal polarisation on A, $\overline{\eta}$ is a K-level structure (see end of Sect.6.1.1 of [12]), H_i is a rank p^i finite flat subgroup scheme of $A[p]$ with H_2 totally isotropic for the λ-Weil pairing.
As in Th.6.2.1 of [12] or [16] Prop.1.2, one shows

Theorem 1 *If K is neat, the functors above are representable by quasiprojective $\mathbb{Z}[\frac{1}{N}]$-schemes $X_\emptyset$, $X_B(p)$, $X_P(p)$ and $X_Q(p)$. The first one is smooth over $\mathbb{Z}[\frac{1}{N}]$ while the others are smooth away from p; the functors of forgetfulness of the level p structure provide proper morphisms $\pi_{B,\emptyset} : X_B(p) \to X_\emptyset$, $\pi_{P,\emptyset} : X_P(p) \to X_\emptyset$, and $\pi_{Q,\emptyset} : X_Q(p) \to X_\emptyset$ which are finite etale in generic fiber.*

We'll see that these morphisms are not necessarily finite hence not necessarily flat.
We'll also consider a moduli problem of level $\Gamma_1(p)$. Let U_B be the unipotent radical of the Borel B of G. Let $\mathcal{F}_{U_B}$ be the functor on $\mathbb{Q}-$Sch sending S to $\{A, \lambda, \overline{\eta}, P_1, P_2)_{/S}\}/\sim$ where P_1 is a generator of a rank p finite flat subgroup scheme H_1 of $A[p]$ while P_2 is a generator of the rank p finite flat group scheme H_2/H_1 for H_2 a lagrangian of $A[p]$. Over $\mathbb{Q}$, it is not difficult to show that it is representable by a scheme $X_{U_B}(p)_\mathbb{Q}$.
Following [14] and [12] Sect.6.2.2, we define the $\mathbb{Z}[\frac{1}{N}]$-scheme $X_{U_B}(p)$ as the normalisation of $X_B(p)$ in $X_{U_B}(p)_\mathbb{Q}$; it comes therefore with a morphism $\pi_{U_B,B} : X_{U_B}(p) \to X_B(p)$ which is generically finite Galois of group $T(\mathbb{Z}/p\mathbb{Z})$.

Remark: All schemes above have geometrically connected generic fibers if and only if $\nu(K) = \widehat{\mathbb{Z}}^\times$. However, in general, the morphisms $\pi_{*,\emptyset}$ induce bijections between the sets of geometric connected components of $X_*(p)$ and $X_\emptyset$; therefore the descriptions of irreducible components of the special fiber at p given below should be interpreted as relative to an arbitrary given connected component of the special fiber at p of $X_\emptyset$.
We still denote by $X_*(p)$ the base change to $\mathbb{Z}_p$ of $X_*(p)_{/\mathbb{Z}[\frac{1}{N}]}$ ($* = \emptyset, B, P, Q$).
The results that we will explain below are essentially due to de Jong [16], Genestier [11], Ngô-Genestier [22], Chai-Norman [9], C.-F. Yu [29]. As most of these authors, we make first use of the theory of local models [23], which allows to determine the local structure of $X_*(p)$; then, one globalizes using the surjectivity of the monodromy action due to [10]. This argument is sketched in [16] for $g = 2$ and developed for any genus and for any parahoric level structure in [29].
The determination of the local model and of its singularities has been done in case $* = B$ by de Jong [16], in case $* = P$ in [12] Sect.6.3 (inspired by [14]) and in case $* = Q$ in [12] Appendix. Let us recall the results.

2.1 The case $* = B$

We first recall the definition of the local model M_B of $X_B(p)$ over $\mathbb{Z}_p$.
Let $St_0 = \mathbb{Z}_p^4$, with its canonical basis (e_0, e_1, e_2, e_3), endowed with the standard unimodular symplectic form ψ: $\psi(x, y) = {}^t xJy$. We consider the standard diagram $St_2 \overset{\alpha_2}{\to} St_1 \overset{\alpha_1}{\to} St_0$ where α_{i+1} sends e_i to pe_i and e_j to e_j $(j \neq i)$. We endow St_2 resp. St_0 with the unimodular standard symplectic form ψ, which we prefer to denote ψ_2 resp. ψ_0. Let $\alpha^2 = \alpha_1 \circ \alpha_2$; then we have $\psi_0(\alpha^2(x), \alpha^2(y)) = p\psi_2(x, y)$.

Then, M_B is the scheme representing the functor from $\mathbb{Z}_p$–Sch to Sets sending a scheme S to the set of triples $(\omega_i)_{i=0,1,2}$, where ω_i is a direct factor of $St_i \otimes \mathcal{O}_S$, ω_0 and ω_2 are totally isotropic, and $\alpha_{i+1}(\omega_{i+1}) \subset \omega_i$ for $i = 0, 1$.
It is a closed subscheme of the flag variety over $\mathbb{Z}_p$ $G(St_2, 2) \times G(St_1, 2) \times G(St_0, 2)$. Let $\overline{\xi}_0 = (\overline{\omega}_2, \overline{\omega}_1, \overline{\omega}_0) \in M_B(\mathbb{F}_p)$ be the point given by $\overline{\omega}_2 = \langle e_0, e_1\rangle$, $\overline{\omega}_1 = \langle e_0, e_3\rangle$ and $\overline{\omega}_0 = \langle e_2, e_3\rangle$. Consider the affine neighborhood U of $\overline{\xi}_0$ in M_B given by $\omega_2 = \langle e_0 + c_{11}e_2 + c_{12}e_3, e_1 + c_{21}e_2 + c_{22}e_3\rangle$, $\omega_1 = \langle e_0 + b_{11}e_1 + b_{12}e_2, e_3 + b_{21}e_1 + b_{22}e_2\rangle$ and $\omega_0 = \langle e_2 + a_{11}e_0 + a_{12}e_1, e_3 + a_{21}e_0 + a_{22}e_1\rangle$.
We'll see below that it is enough to study the geometry of U because this open set is "saturating" in M_B (*i.e.* its saturation G_BU for the action of the group G_B of automorphisms of M_B is M_B). Let us first study the geometry of U.
The equations of U are $c_{11} = c_{22}$, $a_{11} = a_{22}$,
$pe_1 + c_{21}e_2 + c_{22}e_3 = c_{22}(e_3 + b_{21}e_1 + b_{22}e_2)$,
$e_0 + c_{11}e_2 + c_{12}e_3 = e_0 + b_{11}e_1 + b_{12}e_2 + c_{12}(e_3 + b_{21}e_1 + b_{22}e_2)$,
and similarly
$pe_0 + b_{11}e_1 + b_{12}e_2 = b_{12}(e_2 + a_{11}e_0 + a_{12}e_1)$,
$e_3 + b_{21}e_1 + b_{22}e_2 = e_3 + a_{21}e_0 + a_{22}e_1 + b_{22}(e_2 + a_{11}e_0 + a_{12}e_1)$.
Equating the coordinates of the two members, one gets the set of equations (2) of [16] Sect.5.
Putting $x = a_{11}$, $y = b_{12}$, $a = c_{12}$, $b = a_{12}$ and $c = b_{22}$, an easy calculation shows that $U = \operatorname{spec} \mathbb{Z}_p[x, y, a, b, c]/(xy - p, ax + by + abc)$. The special fiber $U_0 \subset M_B \otimes \mathbb{F}_p$ of U is an affine threefold given by the equations $xy = 0$ and $ax + by + abc = 0$; it is the union of its four smooth irreducible components $Z_{00} = V(x, b)$, $Z_{01} = V(x, y + ac)$, $Z_{10} = V(y, a)$ and $Z_{11} = V(y, x + bc)$.
Let $R = \mathbb{Z}_p^{ur}[x, y, a, b, c]/(xy - p, ax + by + abc)$; then $\overline{\xi}_0$ has coordinates $(0, 0, 0, 0, 0)$ in $U_0(\overline{\mathbb{F}}_p)$. Let $\overline{\zeta}_0 = (\overline{x}_0, \overline{y}_0, \overline{a}_0, \overline{b}_0, \overline{c}_0)$ be an arbitrary point of $U_0(\overline{\mathbb{F}}_p)$. Note that $\overline{x}_0\overline{y}_0 = 0$ and $\overline{a}_0\overline{x}_0 + \overline{b}_0(\overline{y}_0 + \overline{a}_0\overline{c}_0) = \overline{b}_0\overline{y}_0 + \overline{a}_0(\overline{x}_0 + \overline{b}_0\overline{c}_0) = 0$.
Let $\mathfrak{m}_0$ be the maximal ideal of R corresponding to $\overline{\zeta}_0$. The completion of R at $\mathfrak{m}_0$ is given by the following easy lemma ([16] Section 5).

Lemma 2.1

- *If $\overline{x}_0 + \overline{b}_0\overline{c}_0 \neq 0$, then if $\overline{y}_0 \neq 0$, $\widehat{R}_{\mathfrak{m}_0} \cong \mathbb{Z}_p^{ur}[[u, \beta, \gamma]]$,*
- *If $\overline{x}_0 + \overline{b}_0\overline{c}_0 \neq 0$ and $\overline{y}_0 = 0$, then $\widehat{R}_{\mathfrak{m}_0} \cong \mathbb{Z}_p^{ur}[[x, y, b, c]]/(xy - p)$,*
- *If $\overline{a}_0 \neq 0$, if $\overline{y}_0 = \overline{b}_0 = 0$ then $\widehat{R}_{\mathfrak{m}_0} \cong \mathbb{Z}_p^{ur}[[y, b, t, c]]/(ybt - p)$, and if $\overline{y}_0 \neq 0$ or $\overline{b}_0 \neq 0$, if $\overline{y}_0\overline{b}_0 = 0$ then $\widehat{R}_{\mathfrak{m}_0}$ is $\mathbb{Z}_p^{ur}[[y, b, t, c]]/(yt - p)$, or it is smooth if $\overline{y}_0\overline{b}_0 \neq 0$,*
- *If $\overline{c}_0 \neq 0$ and $\overline{x}_0 = \overline{b}_0 = \overline{a}_0 = \overline{y}_0 = 0$, if moreover $\overline{c}_0 \neq 0$, then $\widehat{R}_{\mathfrak{m}_0} \cong \mathbb{Z}_p^{ur}[[x, y, u, v, w]]/(xy - p, uv - p)$,*
- *If $\overline{x}_0 = \overline{b}_0 = \overline{a}_0 = \overline{y}_0 = \overline{c}_0 = 0$, that is, if $s_0 = x_0$ (defined above), then $\widehat{R}_{\mathfrak{m}_0} \cong \mathbb{Z}_p^{ur}[[x, y, a, b, c]]/(xy - p, ax + by + abc)$,*

The other cases are brought back to those by permuting the variables x and y resp. a and b.

Proof: If $\overline{x}_0+\overline{b}_0\overline{c}_0\neq 0$, and $\overline{y}_0\neq 0$, we choose liftings $x_0,a_0,b_0,c_0\in\mathbb{Z}_p^{ur}$ and $y_0\in\mathbb{Z}_p^{ur\times}$ and introduce new variables u,α,β,γ by putting $y=y_0+u$ and $a=a_0+\alpha$, $b=b_0+\beta$, $c=c_0+\gamma$ (in case $\overline{b}_0=0$ for instance, we choose $b_0=0$ so that $\beta=b$, and similarly for γ). Then, the relation $ax+by+abc=0$ in $\widehat{R}_{\mathfrak{m}_0}$ reads $a(x+bc)+by=0$, so that the image of the variable α can be expressed as a series of the images of the variables u,β,γ; similarly, the relation $xy=p$ allows to express x as a series of u; in conclusion, we have $\widehat{R}_{\mathfrak{m}_0}\cong\mathbb{Z}_p^{ur}[[u,\beta,\gamma]]$.
If $\overline{x}_0\neq 0=\overline{y}_0=0$, this reasoning shows that $\widehat{R}_{\mathfrak{m}_0}\cong\mathbb{Z}_p^{ur}[[x,y,\beta,\gamma]]/(xy-p)$.
If $\overline{a}_0\neq 0$, let us omit the centering at 0 of variables as above (needed for instance if $\overline{b}_0\neq 0$ or $\overline{y}_0\neq 0$). Let us write the relation $ax+by+abc=0$ as $x=-a^{-1}by-bc=b(-a^{-1}y-c)$. We introduce a new variable $t=-a^{-1}y-c$. Then we have $p=xy=bty$ so that $\widehat{R}_{\mathfrak{m}_0}\cong\mathbb{Z}_p^{ur}[[y,b,t,c]]/(ybt-p)$ unless, as mentioned, $\overline{b}_0\neq 0$ or $\overline{y}_0\neq 0$ where things become simpler.
If $\overline{x}_0=\overline{b}_0=\overline{a}_0=\overline{y}_0=0$ but $\overline{c}_0\neq 0$, then $(x+bc)(y+ac)=p+c(ax+by+abc)=p$; hence, putting $u=x+bc$ and $v=y+ac$, one defines a change of variables from the set of variables (x,y,a,b,c) to (x,y,u,v,c) (actually, as above, one should use $\gamma=c-c_0$ instead of c) and the conclusion follows.
The last case is clear.QED.

By the theory of local models, we have a diagram

$$\begin{tikzcd} & \mathcal{W}_B \arrow[dl, "\pi"'] \arrow[dr, "f"] & \\ X_B(p) & & M_B \end{tikzcd}$$

where $\mathcal{W}_B$ classifies quintuples $(A,\lambda,H_1,H_2;\phi: St.\otimes\mathcal{O}_S\cong D(A.))$ over a scheme S (see Sect.3 of [16], especially Prop.3.6, for the definition of ϕ). One sees easily that it is representable by a $X_B(p)$-scheme $\pi:\mathcal{W}_I\to X_B(p)$. The morphism f consists in transporting the Hodge filtration from the Dieudonné modules to $St.$ by ϕ and π consists in forgetting ϕ. Recall that those morphisms are smooth and surjective.
Given a point $z=(A_0\to A_1\to A_2,\lambda_0,\lambda_2;\phi)$ of $\mathcal{W}_B(\overline{\mathbb{F}}_p)$, the degree p isogenies $A_0\to A_1\to A_2$ (defined by quotienting $A=A_0$ by H_1 and H_2) give rise to morphisms of filtered Dieudonné modules (writing M_i for $D(A_i)_S$): $M_2\to M_1\to M_0$, sending ω_{i+1} into ω_i. Let us consider the rank p finite flat group schemes $G_0=H_1=\mathrm{Ker}\,(A_0\to A_1)$ and $G_1=H_2/H_1:\mathrm{Ker}\,(A_1\to A_2)$. Then, we have a canonical isomorphism
1) $\omega_i/\alpha(\omega_{i+1})\cong\omega_{G_i}$.
Recall that $\omega_{A_i^\vee}=\omega_i^\vee=M_i/\omega_i$, hence by Th.1, Sect.15 of [20]), if $G_i^\vee$ denotes the Cartier dual of G_i, we have
2) $\omega_{G_i^\vee}=M_i/(\omega_i+\alpha(M_{i+1}))$.
For $z\in\mathcal{W}_B(\overline{\mathbb{F}}_p)$ as above, let $x=\pi(z)=(A_0\to A_1\to A_2,\lambda_0,\lambda_2)$ and $s=f(z)=(\omega_2,\omega_1\omega_0)$.
We define $\sigma_i(s)=\dim\omega_i/\alpha(\omega_{i+1})$ and $\tau_i(s)=\dim M_i/(\omega_i+\alpha(M_{i+1}))$.
Then,

- if G_i is μ_p, $\sigma_i(s) = 1$ and $\tau_i(s) = 0$
- if G_i is $\mathbb{Z}/p\mathbb{Z}$, $\sigma_i(s) = 0$ and $\tau_i(s) = 1$
- if G_i is α_p, $\sigma_i(s) = 1$ and $\tau_i(s) = 1$

We define $M_B(\overline{\mathbb{F}}_p)^{\mathrm{ord}}$ as the set of points s such that $(\sigma_i(s), \tau_i(s)) \in \{(1,0),(0,1)\}$ for $i = 1,2$.

One determines its four connected components and we check their Zariski closures are the irreducible components of $M_B(\overline{\mathbb{F}}_p)$ as follows. The calculations of the lemma above show that $M_B(\overline{\mathbb{F}}_p) \cap U$ is the union of the loci

- (1) $x = b = 0$,
- (2) $x = y + ac = 0$,
- (3) $y = a = 0$,
- (4) $y = x + bc = 0$,

Then, let us check that the component $x = b = 0$ is the Zariski closure of the locus (m,m) where H_1 and H_2/H_1 are multiplicative. This component consists in triples $(\omega_2, \omega_1, \omega_0)$ such that the generators of ω_0 satisfy $a_{11} = a_{12} = 0$, that is, by equations (1) of U_0 in Sect.6 of [16], such that $\omega_0 = \langle e_2, e_3\rangle$. Then one sees that $\alpha(\omega_1) = \langle b_{12}e_2, e_3 + b_{22}e_2\rangle$ has codimension 1 in ω_0 if $b_{12} = 0$, and codimension 0 otherwise, while $\alpha(\omega_2) = \langle e_0 + c_{11}e_2 + c_{12}e_3, c_{21}e_2 + c_{22}e_3\rangle$ has codimension 1 if $c_{11} = 0$ and 0 otherwise.

On the other hand, $\alpha(M_1)$ is generated by (e_1, e_2, e_3) so $M_0/\alpha(M_1)$ is generated by the image of e_0; since $\omega_0 = \langle e_2, e_3\rangle$, we see that $\tau_0(s) = 1$ for any $s \in Z_{00}$, while $\alpha(M_2)$ is generated by (e_0, e_2, e_3) so that $M_1/\alpha(M_2)$ is generated by the image of e_1; since $\omega_1 = \langle e_0 + b_{12}e_2, e_3 + b_{22}e_2\rangle$, we see that $\tau_1(s) = 1$ also on Z_{00}. Hence the open dense locus defined by $b_{12} \neq 0$ and $c_{11} \neq 0$ is the ordinary locus of this component (that is, the set of points s such that $(\sigma_i(s), \tau_i(s)) = (0,1)$ $(i = 1,2)$.

One can do similar calculations for the other components; to obtain the table at bottom of page 20 of [16] (note however that our labeling of the components is different).

This calculation proves the density of the ordinary locus in each irreducible component in U_0 and provides at the same time the irreducible components of the non-ordinary locus and of the supersingular locus. We find

Lemma 2.2 *The open subset U_0 of $M_B \otimes \mathbb{F}_p$ is an affine scheme with four irreducible components*

- *(1) $x = b = 0$, Zariski closure of the locus (m,m) where H_1 and H_2/H_1 are multiplicative*
- *(2) $x = y + ac = 0$, Zariski closure of the locus (m,e) where H_1 is multiplicative and H_2/H_1 is étale*

- *(3) $y = a = 0$, Zariski closure of the locus (e, e) where H_1 and H_2/H_1 are étale*

- *(4) $y = x + bc = 0$, Zariski closure of the locus (e, m) where H_1 is étale and H_2/H_1 is multiplicative.*

The singular locus U_0^{sing} can be viewed as the union of two loci: "H_1 biconnected",whose equation is $x = y = 0$, and "H_2/H_1 biconnected", whose equation is $y + ac = x + bc = 0$. The intersection of those two is the supersingular locus U_0^{ssing}.
The locus "H_1 biconnected" is the union of U_0^{ssing} and two 2-dimensional irreducible components

- *(14) the locus $x = b = y = 0$,equation of the Zariski closure of the locus where H_1 is biconnected and H_2/H_1 is multiplicative,*

- *(23) the locus $y = x = a = 0$, equation of the Zariski closure of the locus where H_1 is biconnected and H_2/H_1 is étale,*

where the label (ij) denotes the irreducible 2-dimensional intersection of (i) and (j).
The supersingular locus U_0^{ssing} coincides with the intersection $(2) \cap (4)$ which is the union of one 2-dimensional component $x = y = c = 0$, which we denote by (24) and one 1-dimensional component $a = b = x = y = 0$.
The locus "H_2/H_1 biconnected" is the union of U_0^{ssing} and of two irreducible components

- *(12) $x = b = y + ac = 0$, equation of the Zariski closure of the locus where H_1 is multiplicative and H_2/H_1 is biconnected,*

- *(34) $y = a = x + bc = 0$, equation of the Zariski closure of the locus where H_1 is étale and H_2/H_1 is biconnected .*

with the same convention $(ij) = (i) \cap (j)$ (here, those are irreducible 2-dimensional components);
Finally, the three irreducible components of the one-dimensional stratum associated to the four irreducible components of U_0^{sing} are

- $x = y = a = b = 0$,

- $x = y = a = c = 0$,

- $x = y = b = c = 0$,

They are all contained in U_0^{ssing}. More precisely, the second and third are contained in (24), and U_0^{ssing} is the union of the first and of (24).
Thus, the supersingular locus of M_B is not equidimensional, it is union of a two-dimensional irreducible component, namely the Zariski closure of the locus (24), and a one-dimensional irreducible component, closure of $x = y = a = b = 0$.

Let us consider the Iwahori group scheme G_B; it is a smooth group scheme over $\mathbb{Z}_p$ representing the functor $S \mapsto \mathrm{Aut}_S(St. \otimes \mathcal{O}_S)$. Its generic fiber is the symplectic group G while its special fiber is extension of the upper triangular Borel B by the opposite unipotent radical.
The complete list of the G_B-orbits in $M_B \otimes \mathbb{F}_p$ follows from the analysis above. There are thirteen such orbits. There are four 3-dimensional orbits (whose Zariski closures are the irreducible components), five 2-dimensional orbits, three 1-dimensional orbits, and one 0-dimensional orbit, intersection of all the closures of the other orbits. These orbits can be detected from the irreducible components as complement in an irreducible component of the union of the other components of smaller dimension. In [13] p.594, they are described in terms of thirteen alcoves in an apartment of the Bruhat-Tits building.
Let us explain now the property of saturation of U: $G_B \cdot U = M_B$. To prove this, we note that U_0 meets all the orbits of G_B because it contains the smallest orbit, namely the point $\overline{\xi}_0$ defined above and that this point is in the closure of all the other orbits. (cf. the remark of [11] above Lemma 3.1.1). This observation, together with the previous lemma implies [16], [22]

Proposition 2.3 *The scheme M_B is flat, locally complete intersection over $\mathbb{Z}_p$. Its special fiber is the union of four smooth irreducible components. Its ordinary locus coincides with the regular locus and is dense; the singular locus has* 5 2*-dimensional irreducible components, all smooth, and two one-dimensional irreducible components, also smooth; the p-rank zero locus has* 3 *irreducible components, all smooth; one is* 2*-dimensional and two are* 1*-dimensional.*

The local and global geometry of $X_B(p)$ is mostly contained in the following:

Theorem 2 *The scheme $X_B(p)$ is flat, locally complete intersection over $\mathbb{Z}_p$. The ordinary locus in the special fiber coincides with the regular locus; it is therefore dense in the special fiber $X_B(p) \otimes \mathbb{F}_p$; this scheme is the union of four smooth irreducible components X^{mm}, X^{me}, X^{em}, X^{ee}. They are the Zariski closures of their ordinary loci, which are given respectively by the following conditions on the filtration $0 \subset H_1 \subset H_2 \subset A[p]$: H_2 is multiplicative, H_1 is multiplicative and H_2/H_1 étale, H_1 is étale and H_2/H_1 is multiplicative, H_2 is étale. The singular locus of $X_B(p) \otimes \mathbb{F}_p$ is therefore the locus where either H_1 or H_2/H_1 is étale-locally isomorphic to α_p.*
There exists a semistable model $\widetilde{X}_B(p)$ of $X_B(p)$ over $\mathbb{Z}_p$ with a proper morphism $h : \widetilde{X}_B(p) \to X_B(p)$ whose generic fiber $h \otimes \mathbb{Q}_p$ is an isomorphism and whose special fiber $h \otimes \mathbb{F}_p$ is an isomorphism over the ordinary locus.

Remark:
The stratification of the special fiber of M_B by the G_B-orbits (called the Kottwitz-Rapoport stratification) defines also a stratification of the special fiber of $X_B(p)$; the stratum X_S associated to the (irreducible) stratum S of M_B is defined as $\pi(f^{-1}(S))$. The four orbits corresponding to the irreducible

components are connected because of the monodromy theorem of [10] (due to C.-F. Yu [29]). It has been pointed out to the author by A.Genestier that for the 2-dimensional orbits, no such connexity result is available yet by a p-adic monodromy argument. However, C.F. Yu explained to us how to prove that the p-rank one stratum does consist of four 2-dimensional irrreducible components as listed above for M_B^{sing}. Indeed, for any p-rank one geometric closed point x of $X_B(p) \otimes \mathbb{F}_p$, we have $A_x[p] = G_{1,1}[p] \times \mu_p \times \mathbb{Z}/p\mathbb{Z}$ where $G_{1,1}$ denotes the p-divisible group of a supersingular elliptic curve; hence the possibilities for the pairs $(H_1, H_2/H_1)$ are (α_p, μ_p), $(\alpha_p, \mathbb{Z}/p\mathbb{Z})$, (μ_p, α_p), $(\mathbb{Z}/p\mathbb{Z}, \alpha_p)$. This shows that the p-rank one stratum has exactly four connected components, so that the components of each type are irreducible.

For the supersingular locus $X_B(p)^{\mathrm{ss}}$, it is known by Li-Oort that the number of irreducible components is in general strictly greater than 3 (which is the number of irreducible components of M_B^{ss}).

Proof: By [16] Sect.4, the morphisms $\pi : \mathcal{W}_B \to X_B(p)$ and $f : \mathcal{W}_I \to M_B$ are smooth and surjective and for any geometric point x of $X_B(p)$, there exists a geometric point $s \in f(\pi^{-1}(\{x\})$ of M_B and a local ring isomorphism

$$\widehat{\mathcal{O}}_{X_B(p),x} \cong \widehat{\mathcal{O}}_{M_B,s}$$

The description of the strictly henselian local rings $\widehat{\mathcal{O}}_{X_B(p),x}$ is therefore given by the list of Lemma 2.2. They are flat, complete intersection over $\mathbb{Z}_p^{ur}$.

The ordinary subcheme $X_B(p)^{\mathrm{ord}}$ of the special fiber $\mathbb{X}_B(p) \otimes \mathbb{F}_p$ is the locus where the connected component of $A[p]$ is of multiplicative type. By total isotropy of H_2 it follows easily that $X_B(p)^{\mathrm{ord}}(\overline{\mathbb{F}}_p) = \pi(f^{-1}(M_B^{\mathrm{ord}}))$. Therefore, $X_B(p)^{\mathrm{ord}}$ is the disjoint union of four open subsets $X^{mm,\mathrm{ord}}$, $X^{me,\mathrm{ord}}$, $X^{em,\mathrm{ord}}$, $X^{ee,\mathrm{ord}}$, defined by the conditions: "the type of the pair $(H_1, H_2/H_1)$ is (m, m) resp. (m, e), resp. (e, m), resp. (e, e), where m means multiplicative and e means étale". Let us denote by X^{mm}, X^{me}, X^{em}, X^{mm} their Zariski closures in $X_B(p) \otimes \mathbb{F}_p$. By density of the ordinary locus, one has $X_B(p) \otimes \mathbb{F}_p = X^{mm} \cup X^{me} \cup X^{em} \cup X^{mm}$. Let us show that these four subschemes are smooth irreducible. For $i, j \in \{0, 1\}$, let $M_B^{\alpha\beta}$ (α and β in $\{m, e\}$) be the irreducible components of $M_B \otimes \mathbb{F}_p$ such that $M_B^{\alpha\beta} \cap U_0$ is the component (α, β) in Lemma 2.2; then we have $\pi(f^{-1}(M_B^{\alpha\beta})) = X^{\alpha\beta}$. Thus, the smoothness of the components $M_B^{\alpha\beta}$ of $M_B \otimes \mathbb{F}_p$ yields the smoothness of $X^{\alpha\beta} \cap \mathcal{U}_0$ for all α and β in $\{m, e\}$. The connectedness of $X^{\alpha\beta}$ follows from a simple argument due to C.-F. Yu [29] which we repeat briefly, with a small correction (of the wrong statement (2.2) p.2595). let $A \to X_\emptyset$ be the universal abelian variety; let $X_\emptyset^o$ be the ordinary locus of $X_\emptyset \otimes \mathbb{F}_p$; then for any closed geometric point $\overline{x}$, by Sect.V.7 of [10] the monodromy representation $\pi_1(X_\emptyset^o, \overline{x}) \to GL_g(\mathbb{Z}_p)$ is surjective; this is equivalent to saying that the finite étale $X_\emptyset^o$-cover $Ig(p) = \mathrm{Isom}_{X_\emptyset^o}(\mu_p^2, A[p]^o)$ is connected. Consider the scheme $Ig_b(p) = \mathrm{Isom}_{X_\emptyset^o}((\mu_p^2 \times (\mathbb{Z}/p\mathbb{Z})^2, A[p])$ where the second member consists in symplectic isometries between the standard symplectic space (for the pairing given by the matrix J) and $A[p]$ endowed with the Weil pairing.

By extension of isomorphisms between lagrangians to symplectic isometries, we see that $Ig_b(p)$ is a purely inseparable torsor above $Ig(p)$ under the group scheme $\mu_p \otimes U(\mathbb{Z}/p\mathbb{Z})$ where U denotes the unipotent radical of the Siegel parabolic. Hence $Ig_b(p)$ is connected. Now, for each connected component $X^{\alpha\beta,\mathrm{ord}}$ of $X_B(p)^{\mathrm{ord}}$, one can define a finite surjective morphism $Ig_b(p) \to X^{o,\alpha\beta}$. For instance for $X^{me,\mathrm{ord}}$, we define a filtration inside $\mu_p^2 \times (\mathbb{Z}/p\mathbb{Z})^2$ by $H_1^{me} = \mu_p \times 1 \times 0 \times 0 \subset H_2^{me} = \mu_p \times 1 \times \mathbb{Z}/p\mathbb{Z} \times 0$, and we define f^{me} as sending $(A, \lambda, \xi) \in Ig(p)$ to $(A, \lambda, 0 \subset \xi(H_1^{me}) \subset \xi(H_2^{me}) \subset A[p]) \in X^{me,\mathrm{ord}}$. This shows the connectedness of $X^{me,\mathrm{ord}}$. A similar argument applies to the other components.

The construction of the G_B-equivariant semistable model $\widetilde{M}_B$ of M_B has been done first by de Jong [16] by blowing-up M_B along either of the irreducible components (m, m) or (e, e), while Genestier constructs a semistable scheme $\widetilde{\mathcal{L}}$ by three consecutive blowing-ups of the lagrangian grassmannian $\mathcal{L}$ in such a way that the resulting scheme has an action of G_B; then he shows that the isomorphism from the generic fiber of $\widetilde{\mathcal{L}}$ to that of M_B extends to a proper morphism $\widetilde{\mathcal{L}} \to M_B$. He also shows [11] Construction 2.4.1 that the two constructions coincide: $\widetilde{M}_B = \widetilde{\mathcal{L}}$.

Then, both authors define $\widetilde{X}_B(p)$ as $(\mathcal{W}_B \times_{M_B} \widetilde{M}_B)/G_B$ (for its diagonal action). QED

Remark: The previous calculations show also that the proper morphism $\pi_{B,\emptyset}$ is not finite over the supersingular locus C of $X_\emptyset$, for instance the inverse image $\pi_{B,\emptyset}^{-1}(CSS)$ of the (zero dimensional) superspecial locus $CSS \subset C$ coincides with the locus where the lagrangian H_2 coincides with the lagrangian $\alpha_p \times \alpha_p$ of $G_{1,1}[p] \times G_{1,1}[p]$, and $H_1 \subset H_2$; thus by [20] Sect.15, Th.2, the fiber of $\pi_{B,Q}$ at each superspecial point of $X_Q(p)$ is a projective line.

On the other hand, the morphism $\pi_{Q,\emptyset} : X_Q(p) \to X_\emptyset$ is finite.

2.1.1 The case $* = U_B$

Recall that U_B denotes the unipotent radical of B. The study of $X_{U_B}(p)$ can be deduced from that of $X_B(p)$ following the lines of [14] Sect.6, using Oort-Tate theory. More precisely, let $\mathcal{W}$ be the G_B-torsor considered above and $\mathcal{W}_U = f^{-1}(U)$ the inverse image of the affine open subset U of M_B (see beginning of 2.1). The locus where H_1 and H_2/H_1 are connected has equation $x = b = 0$. This locus can also be described by oort-Tate theory as follows. There exist two line bundles $\mathcal{L}_1$, $\mathcal{L}_2$ on $X_B(p)$ and two global sections $u_i \in H^0(X_B(p), \mathcal{L}_i^{\otimes(p-1)})$, $i = 1, 2$, together with scheme isomorphisms $H_1 \cong \mathrm{Spec}\,(\mathcal{O}_{X_B(p)}[T]/(T^p - u_1 T))$, resp. $H_2/H_1 \cong \mathrm{Spec}\,(\mathcal{O}_{X_B(p)}[T]/(T^p - u_2 T))$ such that the neutral sections correspond to $T = 0$; then the locus where H_1 and H_2/H_1 are connected is given by $u_1 = u_2 = 0$ in $X_B(p)$. Moreover, the (ramified) covering $X_{U_B}(p) \to X_B(p)$ is defined by $p-1$st roots t_i of u_i. More precisely, when $\mathcal{L}$ is a line bundle on a scheme X and u is a global section of $\mathcal{L}$, one defines the scheme $X[u^{1/n}]$ as the closed subscheme of $\underline{\mathrm{Spec}}_X(\mathrm{Symm}^\bullet \mathcal{L})$ given by the (well-defined) equation $t^n = u$; it is finite flat over X.

Hereafter, we pull back the line bundles and sections u_i to $\mathcal{W}_U$. The divisor $x = 0$ has two irreducible components: $x = b = 0$ and $x = y + ac = 0$ along which u_1 has a simple zero. Moreover, u_1/x is well defined and does not vanish on $\mathcal{W}_U$. Similarly, $u_2/(x + bc)$ is defined everywhere and does not vanish on $\mathcal{W}_U$. By extracting $p-1$st roots of these nowhere vanishing sections, one defines an etale covering $\mathcal{Z} \to \mathcal{W}_U$. Define $\mathcal{Z}_{U_B} = X_{U_B} \times_{X_B(p)} \mathcal{Z}$. On this scheme, the functions x and $x + bc$ admit $p - 1$st roots. Moreover, one has a diagram analogue to the local model theory:

$$X_{U_B}(p) \leftarrow \mathcal{Z}_{U_B} \to U' = U[f_1, f_2]/(f_1^{p-1} - x, f_2^{p-1} - (x + bc))$$

Lemma 2.4 *The two morphisms of the diagram above are smooth and surjective. The scheme U' is a local model of $X_{U_B}(p)$.*

Proof: The morphism $\mathcal{Z} \to X_B(p)$ is smooth since it is the composition of an étale and a smooth morphism; the same holds therefore for its base change $\mathcal{Z}_{U_B} \to X_{U_B}(p)$. The smoothness of the other morphism is proved in a similar way, noticing that one also has $\mathcal{Z}_{U_B} = \mathcal{Z} \times_U U'$.
The surjectivity of $\mathcal{W}_U \to X_B(p)$ (hence of $\mathcal{Z}_{U_B} \to X_{U_B}(p)$) follows because U is G_B-saturating. The surjectivity of $\mathcal{Z}_{U_B} \to U'$ comes from the surjectivity of $\mathcal{W} \to M_B$.

Corollary 2.5 *The singular locus of the reduced irreducible components of $X_{U_B}(p)$ is either empty or zero-dimensional.*

Let T' be the diagonal torus of the derived group G' of G.

Proposition 2.6 *The morphism $\pi_{U_B,B} : X_{U_B}(p) \to X_B(p)$ is finite flat, generically étale of Galois group $T'(\mathbb{Z}/p\mathbb{Z})$. The special fiber $X_{U_B}(p) \otimes \mathbb{F}_p$ of $X_{U_B}(p)$ has four irreducible components mapped by $\pi_{U_B,B}$ onto the respective irreducible components of $X_B(p) \otimes \mathbb{F}_p$; each irreducible component of $X_{U_B}(p) \otimes \mathbb{F}_p$ has prime to p multiplicities and the singular locus of the underlying reduced subscheme of each component is at most zero dimensional.*

One can also describe a local model of the quasisemistable scheme $\widetilde{X}_{U_B}(p) = X_{U_B}(p) \times_{X_B(p)} \widetilde{X}_B(p)$. Namely, recall that the map $\widetilde{M}_B \to M_B$ restricted to the affine subscheme $U \subset M_B$ as before, is described (in de Jong's approach) as the blowing-up of U along $x = b = 0$. It is the union of two charts V : $(b, [x/b])$ and $V' : (x, [b/x])$; the first is more interesting as it is G_B-saturating in the blowing-up. In V, one has $y = -([x/b] + c)$, hence after eliminating y, one finds a single equation for V in the affine space of $a, b, c, [x/b]$, namely: $p = -ab[x/b]([x/b] + c)$. Therefore the inverse image V_{U_B} of V in $\widetilde{X}_{U_B}(p)$ has equations

$$p = -ab[x/b]([x/b] + c), \quad f_1^{p-1} = b.[x/b], \quad f_2^{p-1} = b \cdot ([x/b] + c)$$

This scheme is not regular, but has toric, hence mild, singularities. The restriction of $\widetilde{\mathcal{Z}}_{U_B}$ above V provides again a diagram

$$\widetilde{X}_{U_B}(p) \leftarrow \widetilde{\mathcal{Z}}_{U_B,V} \rightarrow V_{U_B}$$

with smooth and surjective arrows (for the left one, the surjectivity comes from the G_B-saturating character of V). Therefore, V_{U_B} is a local model of $\widetilde{X}_{U_B}(p)$.

2.2 The case $* = P$

We follow the same method (see [12] Sect.6 for a slightly different proof). We keep the same notations (so p is prime to the level N of the neat group K). In order to study $X_P(p)$ over $\mathbb{Z}_p$, we consider the diagram of morphisms

$$\begin{tikzcd} & \mathcal{W}_P \arrow[dl, "\pi"'] \arrow[dr, "f"] & \\ X_P(p) & & M_P \end{tikzcd}$$

$\mathcal{W}_P$ is the $\mathbb{Z}_p$-scheme which classifies isomorphism classes of $(A, \lambda, \overline{\eta}, H_1, \phi)$ where $\phi : St. \otimes \mathcal{O}_S \to M.(A)$ is an isomorphism between two diagrams.
The first is $St. \otimes \mathcal{O}_S, \psi_0$ where $St_i = \mathbb{Z}_p^4$ $(i = 0, 1)$ and the diagram $St.$ consists in the inclusion $\alpha_1 : St_1 \to St_0$, $\alpha_1(e_0) = pe_0$ and $\alpha_1(e_i) = e_i$ $(i \neq 0)$, and as before, ψ_0 is the standard unimodular symplectic pairing on St_0 given by J.
The second is given by the inclusion of Dieudonné modules $D(A_1) \to D(A_0)$ associated to the p-isogeny $A_0 \to A_1$ where $A_0 = A$ and $A_1 = A/H_1$.
Let G_P be the group scheme representing the functor $S \mapsto \mathrm{Aut}_S(St. \otimes \mathcal{O}_S)$; is is a smooth group scheme of dimension 11 over $\mathbb{Z}_p$ whose generic fiber is G and the special fiber is an extension of the Klingen parahoric P by the opposite unipotent radical. Then $\pi : cW_P \to X_P(p)$ is a G_P-torsor .
The local model M_P is the projective $\mathbb{Z}_p$-scheme classifying isomorphism classes of pairs (ω_1, ω_0) of rank 2 direct factors $\omega_i \subset St_i$ $(i = 0, 1)$ such that $\alpha_1(\omega_1) \subset \omega_0$ and ω_0 is totally isotropic for ψ_0. The map f send a point of $\mathcal{W}_P$ to the pair obtained by transporting the Hodge filtrations to $St. \otimes \mathcal{O}_S$ via the isomorphism ϕ
We introduce again an open neighborhood U of the point $\xi_0 = (\overline{\omega}_1, \overline{\omega}_0)$ in M_P with $\overline{\omega}_1 = \langle e_0, e_3 \rangle$ and $\overline{\omega}_0 = \langle e_2, e_3 \rangle$. Its importance, as in the Iwahori case, stems from the fact that it is G_P-saturating $G_P U = M_P$ (same proof as above). It consists in the points (ω_1, ω_0) where $\omega_1 = \langle e_0 + b_{11}e_1 + b_{12}e_2, e_3 + b_{21}e_1 + b_{22}e_2 \rangle$ and $\omega_0 = \langle e_2 + a_{11}e_0 + a_{12}e_1, e_3 + a_{21}e_0 + a_{22}e_1 \rangle$.
The condition $\alpha_1(\omega_1) \subset \omega_0$ yields the relations $p = b_{12}a_{11}$, $b_{11} = b_{12}a_{12}$, $0 = a_{21} + b_{22}a_{11}$ and $b_{21} = a_{22} + b_{22}a_{12}$. The isotropy relation yields $a_{11} = a_{22}$. By putting $x = a_{11}$, $y = b_{12}$, $z = a_{12}$, $t = b_{22}$, we find that $U = \mathrm{spec}\, R$ where $R = \mathbb{Z}_p[x, y, z, t]/(xy - p)$, so that for any maximal ideal $\mathfrak{m}_0$ corresponding to $(\overline{x}_0, \overline{y}_0, \overline{z}_0, \overline{t}_0)$ of $U(\overline{\mathbb{F}}_p)$, the completion $\widehat{R}_{\mathfrak{m}_0}$ is $\mathbb{Z}_p^{ur}[[x, y, z, t]]/(xy - p)$, if $\overline{x}_0\overline{y}_0 = 0$, and smooth otherwise. In any case, the local rings are $\mathbb{Z}_p$-regular.

Via transitive action of G_P we conclude that M_P is semistable, with special fiber a union of two smooth irreducible components Z_0 (locally: $x = 0$) and Z_1 (locally: $y = 0$).
In this situation, it is natural to consider only the maps

$$\sigma_0 : s \mapsto \dim \omega_0(s)/\alpha_1(\omega_1(s)) \quad \text{and}\, \tau_0 : s \mapsto \dim M_0/\omega_0(s) + \alpha_1(M_1)$$

as above; the regular locus M_P^r of $M_P \otimes \mathbb{F}_p$ coincides with the locus where $(\sigma_0(s), \tau_0(s)) \in \{(0,1),(1,0)\}$.
As for $* = B$, we conclude that

Theorem 3 *The scheme $X_P(p)$ is flat, semistable over $\mathbb{Z}_p$. The ordinary locus in the special fiber is dense, strictly contained in the regular locus. The special fiber $X_B(p) \otimes \mathbb{F}_p$ is the union of two smooth irreducible components X^m and X^e where $X^m - X^e$ is the locus where H_1 is multiplicative, and $X^e - X^m$ is the locus where H_1 is étale. The singular locus of $X_P(p) \otimes \mathbb{F}_p$ is a smooth surface; it is the locus where H_1 is étale-locally isomorphic to α_p.*

The proof of the density of the ordinary locus is as follows. The forgetful morphism $X_B(p) \to X_P(p)$ sends the ordinary locus of $X_B(p)$ onto the one of $X_P(p)$; hence the density of the first implies that of of the second. The singular locus is the intersection of the two components; it is the locus where H_1 is étale-locally isomorphic to α_p.
Remark: We give an ad hoc proof of the density of the ordinary locus of $X_P(p) \otimes \mathbb{F}_p$ in[12] Prop.6.4.2.

2.3 The case $* = Q$

Again, the same method applies; however, in order to study $X_Q(p)$ over $\mathbb{Z}_p$ and find a semistable model $\widetilde{X}_Q(p) \to X_Q(p)$, we'll first perform calculations in the flavor of de Jong's method [16], as a motivation for Genestier's approach ([11] Sect.3.3.0 and 3.3.3 and [12] Appendix) which we will follow and further a little.
We consider the diagram of morphisms

$$\begin{tikzcd} & \mathcal{W}_Q \arrow[dl, "\pi"'] \arrow[dr, "f"] & \\ X_Q(p) & & M_Q \end{tikzcd}$$

where $\pi_Q : \mathcal{W}_Q \to X_Q(p)$ is the $X_Q(p)$-scheme classifying isomorphism classes of $(A, \lambda, \overline{\eta}, H_2, \phi)$ where $\phi : St. \otimes \mathcal{O}_S \to M.(A)$ is a symplectic isomorphism between two diagrams.
The first is $St. \otimes \mathcal{O}_S, \psi_0, \psi_2$ where $St_i = \mathbb{Z}_p^4$ $(i = 0, 2)$ and the diagram $St.$ consists in the inclusion $\alpha^2 : St_2 \to St_0$, $\alpha^2(e_i) = pe_i$ $(i = 0, 1)$ and $\alpha_1(e_i) = e_i$ $(i > 1)$, and as before, ψ_0 and ψ_2 both denote the standard unimodular symplectic pairing on $\mathbb{Z}_p^4$ given by J. Note that α^2 is a symplectic similitude of similitude factor p: $\psi_2(\alpha^2(x), \alpha^2(y)) = p \cdot \psi_0(x, y)$.

Let G_Q be the $\mathbb{Z}_p$-group scheme of automorphisms of M_Q. It acts on $\mathcal{W}_Q$ as well and π_Q is a G_Q-torsor.
Let $\mathcal{L}$ be the grassmannian of lagrangian direct factors in St_0 over $\mathbb{Z}_p$. Following [11] and [12] Appendix, we shall construct a G_Q-equivariant birational proper morphism $\mathcal{L}^{(2)} \to \mathcal{L}$ over $\mathbb{Z}_p$, composition of two blowing-up morphisms along closed subschemes of the special fiber such that $\mathcal{L}^{(2)}$ is semistable and is endowed with a canonical G_Q-equivariant proper morphism $h : \mathcal{L}^{(2)} \to M_Q$ (an isomorphism in generic fiber). We shall call h the Genestier morphism for (GSp_4, Q). For the easiest case (GSp_{2g}, P), see Prop.6.3.4. of [12].
As a motivation for the detailed construction below by two blowing-ups, we introduce the open subset U of M_Q consisting of pairs $(\omega_2, \omega_0) \in M_Q$ where ω_0 is spanned by $e_3 + a_{21}e_0 + a_{11}e_1$ and $e_2 + a_{22}e_0 + a_{12}e_1$ (with $a_{12} = a_{21}$) and $\omega_2 = \langle e_1 + c_{21}e_2 + c_{11}e_3, \alpha e_0 + c_{22}e_2 + c_{12}e_3 \rangle$ (with $c_{12} = c_{21}$), such that $\alpha^2(\omega_2) \subset \omega_0$; it is therefore isomorphic to the affine set of $\mathbf{A}^6_{\mathbb{Z}_p}$ consisting of pairs (A, C) of 2×2 symmetric matrices such that $AC = p1_2$ by the map

$$(A, C) \mapsto \begin{pmatrix} s \\ sC \end{pmatrix}, \begin{pmatrix} sA \\ s \end{pmatrix}$$

Its special fiber has three irreducible components, given by $A = 0$, $B = 0$ and the Zariski closure of the locally closed set: $\operatorname{rk} A = \operatorname{rk} B = 1$. One then defines $\widetilde{U}$ in $\widetilde{M}_Q$ as the quotient by $\mathbb{G}_m$ of the affine open set of triples (λ, A', μ) such that $A' \neq 0$ is symmetric and $\lambda\mu \det A' = p$, the action of $\mathbb{G}_m$ being given by $t \cdot (\lambda, A', \mu) = ((t\lambda, t^{-1}A', t\mu)$. The map $(\lambda, A', \mu) \mapsto (A, C)$ given by $A = \lambda A'$, $C = \mu^t com(A')$ is the blowing-up of U along the component $A = 0$.

Remark: One checks easily that $\widetilde{U}$ is also the blowing-up of U along $C = 0$. Hence the projection is invariant under the symmetry $(A, C) \mapsto (C, A)$. This allows the definition of an involution W on $\widetilde{U}$. This involution will extend to $\widetilde{M}_B$. See after Prop. below. Note however that the following construction is dyssymmetrical, and does not make explicit use of the open set U defined above.

The first blowing-up $\mathcal{L}^{(1)}$ of the lagrangian grassmannian $\mathcal{L}$ over $\mathbb{Z}_p$ along the closure of $Q \cdot \overline{\omega}_{23}$ where $\overline{\omega}_{23}$ is the $\mathbb{F}_p$-lagrangian spanned by e_2 and e_3.
Note that by functoriality of the blowing-up, $\mathcal{L}^{(1)}$ is endowed with a natural action of G_Q (which acts on $\mathcal{L}$ through the canonical morphism $G_Q \to G$ and leaves the center of blowing-up stable).
Namely, let us consider the affine open subset Ω_0 of $\mathcal{L}$ consisting of the lagrangian planes $\omega_0 = \langle e_3 + a_{11}e_0 + a_{12}e_1, e_2 + a_{21}e_0 + a_{22}e_1 \rangle$ (with $a_{12} = a_{21}$), the blowing-up $\mathcal{L}^{(1)}|\Omega_0$ is the closed $\mathbb{Z}_p$-subscheme of $\mathbb{A}^3 \times \mathbb{P}^3$ of points $(a_{11}, a_{12}, a_{22}; [A_{11}, A_{12}, A_{22}, S])$ such that

$$a_{11}A_{12} - a_{12}A_{11} = 0,\ a_{11}A_{22} - a_{22}A_{11} = 0, a_{12}A_{22} - a_{22}A_{12,} = 0$$

and

$$pA_{11} = a_{11}S,\ pA_{12} = a_{12}S,\ pA_{22} = a_{22}S.$$

The scheme $\mathcal{L}^{(1)}|\Omega_0$ can be described as the quotient by $\mathbb{G}_m$ of the locally closed $\mathbb{Z}_p$-subscheme T_1 of the affine space $\mathbb{A}^5$ defined in terms of the coordinates $(\lambda_0, P_0, A_{11}, A_{12}, A_{22})$ as the intersection of the closed subscheme $\lambda_0 P_0 = p$ with the complement of the closed subscheme $P_0 = A_{11} = A_{12} = A_{22} = 0$. The action of $\mathbb{G}_m$ is given by multiplication by λ^{-1} on the first variable and by λ on the rest.

Indeed, the quotient map $T_1 \to \mathcal{L}^{(1)}|\Omega_0$ is

$$(\lambda_0, P_0, A_{11}, A_{12}, A_{22}) \mapsto (a_{11}, a_{12}, a_{22}; [A_{11}, A_{12}, A_{22}, S])$$

where $a_{11} = \lambda_0 A_{11}$, $a_{12} = \lambda_0 A_{12}$, $a_{22} = \lambda_0 A_{22}$, $S = P_0$.

To take care of equation (1), following [11] Theorem, one forms the blow-up $\mathcal{L}^{(2)}$ of $\mathcal{L}^{(1)}$ along the strict transform $Z_{02}^{c,(1)}$ of the Zariski closure Z_{02}^c of $Z_{02} = Q \cdot \overline{\omega}_{02}$ where $\overline{\omega}_{02}$ is the lagrangian spanned by e_0 and e_2.

The equations of $\mathcal{L}^{(2)}|\Omega_0$ can be determined as follows. First, one notes that $Z_{02}^{c,(1)}|\Omega_0$ is given as a $\mathbb{Z}_p$-subscheme of $\mathcal{L}^{(1)}|\Omega_0$ by the equations $A_{11}A_{22} - A_{12}^2 = P_0 = 0$. Its inverse image in T_1 is given by the same equations (this time, viewed in an affine space). Let $\delta = A_{11}A_{22} - A_{12}^2$.

Then, the blowing-up $T^{(2)}$ of T_1 along this inverse image is the subscheme of $T_1 \times \mathbb{P}^1$ with coordinates $(\lambda_0, P_0, A_{11}, A_{12}, A_{22}, [P_1, \delta_1])$ given by the equation $\delta P_1 = \delta_1 P_0$ (with $(P_1, \delta_1) \neq (0, 0)$).

Introducing λ_1 such that $P_0 = \lambda_1 P_1$, and $\delta = \lambda_1 \delta_1$, one can rewrite $T^{(2)}$ as the quotient by $\mathbb{G}_m$ of the affine locally closed subscheme T_2 of $\mathbb{A}^7$ with affine coordinates $(\lambda_0, \lambda_1, P_1, A_{11}, A_{12}, A_{22}, \delta_1)$ and equations $\lambda_0 \lambda_1 P_1 = p$ and $\lambda_1 \delta_1 = A_{11}A_{22} - A_{12}^2$ in the open subset of $\mathbb{A}^7$ intersection of the locus $(\lambda_1 P_1, A_{11}, A_{12}, A_{22}) \neq (0, 0, 0, 0)$ with $(\delta_1, P_1) \neq (0, 0)$; the action of $\mu \in \mathbb{G}_m$ being the trivial one on λ_0 and A_{ij}, the multiplication by μ^{-1} on λ_1 and the multiplication by μ on P_1 and δ_1.

The quotient map is

$$(\lambda_0, \lambda_1, P_1, A_{11}, A_{12}, A_{22}, \delta_1) \mapsto (\lambda_0, P_0, A_{11}, A_{12}, A_{22}, [P_1, \delta_1])$$

with $P_0 = \lambda_1 P_1$.

We can thus write $\mathcal{L}^{(2)}|\Omega_0$ as a quotient $T_2/\mathbb{G}_m^2$, for the action of $(\lambda, \mu) \in \mathbb{G}_m^2$ on $(\lambda_0, \lambda_1, P_1, A_{11}, A_{12}, A_{22}, \delta_1) \in T_2$ by multiplication by λ^{-1} on λ_0, μ^{-1} on λ_1, by $\lambda\mu$ on P_1, by λ on A_{ij} and $\lambda^2\mu$ on δ_1.

The $\mathbb{Z}_p$-scheme T_2 is clearly semistable. It implies by Lemme 3.2.1 of [11] that $\mathcal{L}^{(2)}|\Omega_0$ is also semistable. Since $G_Q \cdot \mathcal{L}^{(2)}|\Omega_0 = \mathcal{L}^{(2)}$, the same holds for $\mathcal{L}^{(2)}$.

Let us consider the forgetful morphism $\pi_0 : M_Q \to \mathcal{L}$, $(\omega_2, \omega_0) \mapsto \omega_0$; the open subset $U'' = \pi^{-1}(\Omega_0) \subset M_Q$. This open set is not affine, it is dyssymmetrical, it contains the affine open set U defined above.

We can now define the Genestier morphism h on $\mathcal{L}^{(2)}|\Omega_0$. It is given by the $\mathbb{G}_m^2$-invariant map

$$T_2 \to U'', \quad (\lambda_0, \lambda_1, P_1, A_{11}, A_{12}, A_{22}, \delta_1) \mapsto (\omega_2, \omega_0)$$

where ω_0 is given by $a_{ij} = \lambda_0 A_{ij}$ and ω_2 is given in terms of its Plücker coordinates on the basis $(e_0 \wedge e_1, e_0 \wedge e_2, e_0 \wedge e_3, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3)$: $[\delta_1, P_1 A_{11}, -P_1 A_{12}, P_1 A_{12}, P_1 A_{22}, \lambda_1 P_1^2]$. This point of $\mathbb{P}^5$ is well defined because if $\delta_1 = 0$, we have $P_1 \neq 0$ and if $\lambda_1 = 0$, one of the $A_{ij} \neq 0$. It is invariant by the action of $\mathbb{G}_m^2$ hence factors through $\mathcal{L}^{(2)}|\Omega_0$. Moreover it corresponds to an isotropic plane because the third and fourth coordinates are opposite. By [11] Sect.3 before Lemme3.1.1, the saturation of Ω_0 under G_Q is $\mathcal{L}$, hence by G_Q equivariance, it is defined everywhere on $\mathcal{L}^{(2)}$. One sees easily the surjectivity of h restricted to $\mathcal{L}^{(2)}|\Omega_0$ onto U'' (which consists of points in $\mathbb{P}^5$ $[u_0, u_1, u_2, -u_2, u_3, u_4]$ such that $u_0 u_4 = u_1 u_3 - u_2^2$), hence by G_Q-equivariance, to the whole of M_Q.

Definition 2.7 *We put $\widetilde{M}_Q = \mathcal{L}^{(2)}$, it is a semistable $\mathbb{Z}_p$-scheme; its special fiber has three smooth irreducible components. We define $\widetilde{X}_Q(p) = (\mathcal{W}_Q \times \widetilde{M}_Q)/G_Q$; it is a semistable model of $X_Q(p)$ over $\mathbb{Z}_p$ with smooth irreducible components; their number is at least three. It comes with a proper birational morphism $h_X : \widetilde{X}_Q(p) \to X_Q(p)$ which we call the Genestier morphism which is an isomorphism on the generic fiber.*

What precedes is a developed version of [12] Appendix, which may be useful to non expert algebraic geometers. We give now some new information on h and h_X.

For any geometric point $s = (\omega_2, \omega_0)$ of the special fiber of M_Q, let $k = k(s)$ be the residue field; we define

$$\sigma(s) = \dim \omega_0/\alpha^2(\omega_2), \quad \tau(s) = \dim M_0/(\alpha^2(M_2) + \omega_0)$$

Let $x = (A, \lambda, H_2)$ be a geometric point of $X_Q(p)$ corresponding to s. Note that $\sigma(s)$ is the p-rank of the connected component H_2^0 of the group scheme H_2, while $\tau(s)$ is the p-rank of the connected component of the Cartier dual H_2^t of H_2. It can be identified by the Weil pairing to $A[p]/H_2$. From this it is easy to verify that the condition

$$\text{(Ord)} \qquad (\sigma(s), \tau(s)) \in \{(0,2), (2,0), (1,1)\}$$

is equivalent to the ordinarity of the point x. Let M_Q^{ord} be the locus where (Ord) is satisfied. Then the ordinary locus of $X_Q(p)^{\mathrm{ord}}$ of $X_Q(p) \times \mathbb{F}_p$ is equal to $\pi(f^{-1}(M_Q^{\mathrm{ord}})$.

We have a partition $M_Q^{\mathrm{ord}} = M_Q^{\mathrm{ee,ord}} \sqcup M_Q^{\mathrm{mm,ord}} \sqcup M_Q^{\mathrm{em,ord}}$. corresponding to the conditions $(\sigma(s), \tau(s)) \in \{(0,2)$, resp. $(\sigma(s), \tau(s)) \in \{(2,0)$, resp. $(\sigma(s), \tau(s)) \in \{(1,1)$.

Similarly, by taking the inverse images in $\widetilde{M}_Q$ by h, we can define a similar partition of $\overline{M}_Q^{\mathrm{ord}}$:

$$\widetilde{M}_Q^{\mathrm{ord}} = \widetilde{M}_Q^{\mathrm{ee,ord}} \sqcup \widetilde{M}_Q^{\mathrm{mm,ord}} \sqcup \widetilde{M}_Q^{\mathrm{em,ord}}.$$

Let $\widetilde{M}_Q^{\rm reg}$ resp. $\widetilde{M}_Q^{\rm sing}$ be the regular locus resp. singular locus of the special fiber of $\widetilde{M}_Q$.

Let us determine the locus $M_Q^{\rm ee,ord} \cap U''$ where $(\sigma(s), \tau(s)) = (0,2)$ in U'', together with its inverse image $\widetilde{M}_Q^{\rm ee,ord}|\Omega_0$ by h. The condition $\tau(s) = 2$ translates as $a_{11} = a_{12} = a_{22} = 0$; this implies $\lambda_0 = 0$. On the other hand, $\sigma(s) = 0$ implies, using Plücker coordinates, that $\lambda_1 P_1 \neq 0$. One checks easily that actually $(\sigma(s), \tau(s)) = (0,2)$ if and only if $\lambda_0 = 0$ and $\lambda_1 P_1 \neq 0$.

In particular,$\widetilde{M}_Q^{\rm ee,ord}|\Omega_0$ coincides with the (smooth) irreducible component $\lambda_0 = 0$ deprived from $\widetilde{M}_Q^{\rm sing}$; moreover, h induces an isomorphism between $\widetilde{M}_Q^{\rm ee,ord}|\Omega_0$ and $M_Q^{\rm ee,ord} \cap U''$.

Similarly for the locus $M_Q^{mm} \cap U''$ where $(\sigma(s), \tau(s)) = (2,0)$ in U''; the condition $\tau(s) = 0$ is given by the equation $a_{11}a_{22} - a_{12}^2 \neq 0$, that is, $\lambda_0^2 \lambda_1 \delta_1 \neq 0$; while $\sigma(s) = 2$ implies $P_1 = 0$. Conversely, one sees easily that $(\sigma(s), \tau(s)) = (2,0)$ if and only if $P_1 = 0$ and $\lambda_0 \lambda_1 \neq 0$.

Therefore,$\widetilde{M}_Q^{\rm mm,ord}|\Omega_0$ coincides with the smooth irreducible component $P_1 = 0$ minus $\widetilde{M}_Q^{\rm sing}$.

Finally, we consider the locus $M_Q^{em} \cap U''$ where $(\sigma(s), \tau(s)) \in \{(1,1)\}$ in U''. We see that $\tau(s) = 1$ is equivalent to $a_{11}a_{22} - a_{12}^2 = 0$ and $(a_{11}, a_{12}, a_{22}) \neq (0,0,0)$, that is, $\lambda_0^2 \lambda_1 \delta_1 = 0$ and $(\lambda_0 A_{ij} \neq (0,0,0)$. While $\sigma(s) = 1$ implies $\lambda_1 P_1^2 = 0$. Conversely, one sees easily that
$(\sigma(s), \tau(s)) \in \{(1,1)\}$ if and only if $\lambda_1 = 0$ and $\lambda_0 P_1 \neq 0$. In other words $\widetilde{M}_Q^{\rm em,ord}|\Omega_0$ coincides with the smooth irreducible component $\lambda_1 = 0$ minus $\widetilde{M}_Q^{\rm sing}$.

In the three cases, one deduces also from the previous calculations that h induces an isomorphism between $\widetilde{M}_Q^{\alpha\beta,\rm ord}|\Omega_0$ and $M_Q^{\alpha\beta,\rm ord} \cap U''$.

We define then the Zariski closures $M_Q^{\alpha\beta}$ of $M_Q^{\alpha\beta,\rm ord}$ and $\widetilde{M}_Q^{\alpha\beta}$ of $\widetilde{M}_Q^{\alpha\beta,\rm ord}$. Using G_Q-equivariance, we define $\widetilde{X}^{\alpha\beta}$ as $(\mathcal{W}_Q \times M_Q^{\alpha\beta})/G_Q$ for all $\alpha, \beta \in \{e, m\}$ (with the convention that $em = me$)

We can then conclude

Theorem 4 *The scheme $X_Q(p)$ is flat, locally complete intersection over $\mathbb{Z}_p$. The ordinary locus in the special fiber is dense in every irreducible component; it is contained in the regular locus. The special fiber $X_Q(p) \otimes \mathbb{F}_p$ is the union of three irreducible components X^{mm} and X^{me} and X^{em} which are the Zariski closures respectively of the locus where H_2 is of multiplicative type, the locus where, locally for the étale topology, $H_2 = \mu_p \times \mathbb{Z}/p\mathbb{Z}$ and the locus where H_2 is étale. The singular locus of $X_Q(p) \otimes \mathbb{F}_p$ is the locus where H_2 étale-locally contains α_p.*

There is a semistable model together with a blowing-up morphism $h_X : \widetilde{X}_Q(p) \to X_Q(p)$ whose center is in the special fiber; the special fiber of $\widetilde{X}_Q(p)$ consists of three smooth irreducible components $\widetilde{X}^{mm}$, $\widetilde{X}^{me}$ and $\widetilde{X}^{em}$

crossing transversally. The ordinary locus $\widetilde{X}_Q(p)^{\mathrm{ord}}$ *coincides with the regular locus* $\widetilde{X}_Q(p)^{\mathrm{reg}}$*.The restriction of* h_X *induces proper surjective morphisms* $\widetilde{X}^{\alpha\beta} \to X^{\alpha\beta}$ *(*$\alpha,\beta \in \{e,m\}$*) which are isomorphisms between the respective ordinary loci.*

The irreducibility of the components $X^{\alpha\beta}$ follows from [29] as explained above. This implies the irreducibility of the three components $\widetilde{X}^{\alpha\beta}$ because h_X is an isomorphism between the two dense open subsets $\widetilde{X}^{\alpha\beta,\mathrm{ord}}$ and $X^{\alpha\beta,\mathrm{ord}}$, the latter being irreducible.

Remark: Note that we have thus recovered part of the results of [9]; however, this paper contains extra informations: the singular locus of $X_Q(p)\otimes\mathbb{F}_p$ coincides with the finite set of superspecial abelian surfaces (that is, the cartesian products of supersingular elliptic curves); these isolated singularities are Cohen-Macaulay. The description of the intersections two by two and of the three components is given in Sect.6.2 there.

Finally, we introduce an involution W of the $\mathbb{Z}_p$-schemes $X_Q(p)$ and $\overline{X}_Q(p)$ compatible with h_X. The automorphism of the functor $\mathcal{F}_Q$ given by $(A,\lambda,\eta,H_2)\mapsto(\overline{A},\overline{\lambda},\overline{\eta},\overline{H}_2)$ where $\overline{A}=A/H_2$, $\overline{\lambda}$, resp. $\overline{\eta}$ is the quotient polarization resp. Γ-level structure on $\overline{A}$ deduced from λ resp. η and $\overline{H}_2=A[p]/H_2$, induces an involution of the $\mathbb{Z}[1/N]$-scheme $X_Q(p)$, hence of its pull-back to $\mathbb{Z}_p$. If one writes the test objects as $(\alpha : A_0\to A_2,\eta_0,\eta_2)$ where A_i's are principally polarized abelian varieties, α is an isogeny with lagrangian kernel in $A[p]$ respecting the polarizations and the Γ-level structures η_i on A_i, we see that the involution W can be written as the duality $\alpha\mapsto {}^t\alpha$ followed by the identifications of the dual abelian varieties ${}^tA_i$ to A_i; hence W maps $(\alpha : A_0\to A_2,\eta_0,\eta_2)$ to $({}^t\alpha : A_2\to A_0,\eta_2,\eta_0)$.

This involution W therefore extends to the torsor $\mathcal{W}_Q$ by replacing the diagram $M.(A)=(M(\alpha):M(A_2)\to M(A_0))$ by its dual $M({}^tA)=(M({}^t\alpha):M(A_0)\to M(A_2))$ and by interchanging the two isomorphisms ϕ_0 and ϕ_2 in the isomorphism of diagrams $\phi: St.\otimes\mathcal{O}_S\to M.(A)$ to obtain $\phi': St.\otimes\mathcal{O}_S\to M.(A)$.

The involution W on $\mathcal{W}_Q$ is compatible with the forgetful morphism $\mathcal{W}_Q\to M_Q$ where W on M_Q is given by taking the dual of $\alpha^2: St_2\to St_0$ with respect to the standard symplectic pairings ψ_0 and ψ_2, and exchanging ω_0 and ω_2.

Hence, the involution acts on the diagram $X_Q(p)\leftarrow\mathcal{W}_Q\to M_Q$.

Remark: By taking symplectic bases, its matricial interpretation is $\begin{pmatrix}0 & -s\\ p\cdot s & 0\end{pmatrix}$; note that this matrix normalizes the automorphism group G_Q of the diagram $St.$.

The involution W exchanges the two extreme irreducible components X^{ee} and X^{mm} of $X_Q(p)\otimes\mathbb{F}_p$ and it leaves the intermediate component X^{em} stable.

Remarks:

1) There is another construction of the morphism $h:\widetilde{M_Q}\to M_Q$ by noticing that the restriction of h above the open subset U introduced at the beginning of the present section coincides with the map $\widetilde{U}\to U$ defined above and is G_Q-equivariant. Since U, $\widetilde{U}$ and $h|\widetilde{U}$ is symmetric under $(A,C)\mapsto(C,A)$; W

extends by G_Q-action to an involution of $\widetilde{M_Q}$-still denoted W, compatible to h. We thus obtain an involution W of the $\mathbb{Z}_p$-scheme $\widetilde{X}_Q(p) = (\mathcal{W}_Q \times \widetilde{M_Q})/G_Q$ compatible to $h_X : \widetilde{X}_Q(p) \to X_Q(p)$; it exchanges the irreducible components $\widetilde{X}^{ee}$ and $\widetilde{X}^{mm}$ of $\widetilde{X}_Q(p) \otimes \mathbb{F}_p$ and leaves $\widetilde{X}^{em}$ stable.

2) Genestier's construction [11] of the semistable model $\widetilde{M_B}$ of the local model M_B of $X_B(p)$ in a way similar to that of $\widetilde{M_Q}$ implies that the forgetful morphism $M_B \to M_Q$, $(\omega_2, \omega_1, \omega_0) \mapsto (\omega_2, \omega_0)$ extends to the semistable models $\widetilde{M_B} \to \widetilde{M_Q}$; an easy argument provides then a canonical morphism between the Genestier models $\widetilde{X}_B(p) \to \widetilde{X}_Q(p)$. However, it should be noted that the morphism $M_B \to M_Q$ is NOT a local model of the morphism $X_B(p) \to X_Q(p)$. This is already false for the case of the classical modular curve $X_0(p)$ and the classical modular curve X of level prime to p.

Finally, note that as explained in the case $* = Q$, there is a Fricke-Weil involution W on $X_B(p)$; it extends to the semistable models and the forgetful morphism $\widetilde{\pi}_{B,Q}$ is compatible with W.

2.4 Rigid geometry of Siegel varieties

We gather here some informations concerning the rigid geometry of the Siegel varieties $X = X_\emptyset$ and $X_Q(p)$. Some (Prop.2.6, 2) are used in the formulation of the conjecture of Sect.4.3. We hope to develop them in another paper for studying analytic continuation of overconvergent Siegel cusp eigenforms.

Let X^{rig}, $X^{*,\mathrm{rig}}$ resp. $\overline{X}^{\mathrm{rig}}$ be the rigid analytic space associated to the p-adic completion of its corresponding $\mathbb{Z}_p$-scheme (for the toroidal compactification, we assume throughout this section that we fixed a fine Γ-admissible polyedral cone decomposition Σ).

Choosing a $\Gamma_Q(p)$-admissible refinement Σ' of Σ, one can define a smooth toroidal compactification $\overline{X}_Q(p)_{/\mathbb{Q}_p}$ of the $\mathbb{Q}_p$-scheme $X_Q(p) \otimes \mathbb{Q}_p$ (actually, by [10], it exists as a proper smooth scheme over $\mathbb{Z}[\frac{1}{Np}]$). Because of the compatibility of Σ and Σ', we see that the forgetful morphism $\pi = \pi_{Q\emptyset}$: $X_Q(p) \to X$ extends uniquely as a morphism $\overline{\pi} : \overline{X}_Q(p) \to \overline{X}$.

Let $\overline{X}_Q(p)^{\mathrm{rig}}$ be the rigid space over $\mathbb{Q}_p$ corresponding to the scheme $\overline{X}_Q(p)_{/\mathbb{Q}_p}$ (cf. Chapter 9, Ex.2 of [5]). Let $\overline{\mathcal{X}}$ be the formal completion of $\overline{X}$ along the special fiber. The ordinary locus $\overline{\mathcal{X}}^{\mathrm{ord}}$ is an open formal subscheme of $\overline{\mathcal{X}}$; let $\overline{X}^{\mathrm{rig,ord}}$ be the corresponding admissible rigid open subset of $\overline{X}^{\mathrm{rig}}$. Let $\overline{X}_Q(p)^{\mathrm{rig,ord}}$ be the inverse image of $\overline{X}^{\mathrm{rig,ord}}$ by $\overline{\pi}^{\mathrm{rig}}$.

We want to describe the connected components of this admissible rigid open set and strict neighborhoods thereof, in terms of a suitable model of $\overline{X}_Q(p)^{\mathrm{rig}}$. For this purpose, we write simply X_G for the semistable model $\widetilde{X}_Q(p)$ of $X_Q(p)$ over $\mathbb{Z}_p$. We briefly explain the construction of a "toroidal compactifcation of X_G" associated to Σ', by which we mean a proper regular $\mathbb{Z}_p$-scheme $\overline{X}_G$ together with a toroidal open immersion $X_G \hookrightarrow \overline{X}_G$ such that $\overline{X}_G \otimes \mathbb{Q}_p$ is the (smooth) toroidal compactification $\overline{X}_Q(p)_{/\mathbb{Q}_p}$ associated to Σ' mentioned above. Details on this construction, specific to the genus 2 case, should appear in the thesis of a student of A. Genestier. The model of $\overline{X}_Q(p)^{\mathrm{rig}}$ that we are looking for is then defined as the formal completion $\overline{\mathcal{X}}_G$ of $\overline{X}_G$ along the special fiber.

The construction is as follows. One first takes the normalization of the $\mathbb{Z}_p$-toroidal compactification $\overline{X}$ associated to Σ, in the finite étale morphism $X_Q(p)_{/\mathbb{Q}_p} \to X_{/\mathbb{Q}_p}$. Let $\overline{X}_Q(p)^\Sigma$ be this normalization. The morphism $X_G \to X_Q(p)$ is an isomorphism outside the supersingular locus $X_Q(p)^{\mathrm{ss}}$ and this locus is proper (because we are in genus 2). We can therefore glue the schemes $\overline{X}_Q(p)^\Sigma$ and X_G along their common open subscheme $X_Q(p)\backslash X_Q(p)^{\mathrm{ss}}$. We obtain a $\mathbb{Z}_p$-scheme denoted $\overline{X}_G^\Sigma$. Let $Z(\Sigma')_{/\mathbb{Q}_p}$ be the closed subscheme of $\overline{X}_Q(p)^\Sigma_{/\mathbb{Q}_p}$ which is the center of the blowing-up morphism

$$\overline{X}_Q(p)_{/\mathbb{Q}_p} = \overline{X}_Q(p)^{\Sigma'}_{/\mathbb{Q}_p} \to \overline{X}_Q(p)^{\Sigma}_{/\mathbb{Q}_p}$$

We consider the Zariski closure $Z(\Sigma')$ of $Z(\Sigma')_{/\mathbb{Q}_p}$ in the $\mathbb{Z}_p$-scheme $\overline{X}_G^\Sigma$. The blowing-up of $\overline{X}_G^\Sigma$ along $Z(\Sigma')$ is the desired scheme. It is denoted $\overline{X}_G$; by restricting the construction to the local charts of Faltings-Chai, it can be proven that $\overline{X}_G$ is regular over $\mathbb{Z}_p$ and that $X_G \hookrightarrow \overline{X}_G$ is toroidal, although the divisor at infinity doesn't have good reduction.

Remark: For the sake of completion, let us mention another abstract construction. Let $\mathcal{X}_G$ be the formal completion of X_G along the special fiber. One can apply the notion of normalization studied in[4] to define the "normalization" $\overline{\mathcal{X}}_G^{(\mathcal{U}_i)}$ of $\mathcal{X}_G$ along $\overline{X}_Q(p)^{\mathrm{rig}}$ associated to an admissible affinoid cover of $\overline{X}_Q(p)^{\mathrm{rig}}$ (we denote by $\mathcal{U}_i$ the formal scheme associated to the affinoid U_i). The $\mathbb{Z}_p$-formal scheme $\overline{\mathcal{X}}_G^{(\mathcal{U}_i)}$ is endowed with an open immersion of formal schemes $\mathcal{X}_G \to \overline{\mathcal{X}}_G^{(\mathcal{U}_i)}$. However, this construction does depend on the choice of the covering. This is why the specific construction described above is better suited for our purpose.

We still denote by $\overline{\pi}$ the morphism $\overline{X}_G \to \overline{X}$ as well as its p-adic completion $\overline{\mathcal{X}}_G \to \overline{\mathcal{X}}$. We define the ordinary locus $\overline{\mathcal{X}}_G^{\mathrm{ord}}$ as the inverse image in $\overline{\mathcal{X}}_G$ of the ordinary locus $\overline{\mathcal{X}}^{\mathrm{ord}}$ of $\overline{\mathcal{X}}$.

We observe that $\overline{\mathcal{X}}_G^{\mathrm{ord}}$ is smooth. Its underlying $\mathbb{F}_p$-scheme is denoted by $\overline{X}_G^{\mathrm{ord}}$. Let $\widetilde{X}^{\alpha\beta,\mathrm{ord}}$ $(\alpha,\beta \in \{e,m\})$ be the three connected components of $X_G \otimes \mathbb{F}_p$. We denote by $\overline{X}_G^{\alpha\beta,\mathrm{ord}}$ the Zariski closure of $\widetilde{X}^{\alpha\beta,\mathrm{ord}}$ in $\overline{X}_G^{\mathrm{ord}}$. We have a partition into three smooth open subschemes

$$\overline{X}_G^{\mathrm{ord}} = \overline{X}_G^{mm,\mathrm{ord}} \sqcup \overline{X}_G^{me,\mathrm{ord}} \sqcup \overline{X}_G^{ee,\mathrm{ord}}$$

Therefore, by taking the inverse image by the specialization map associated to the model $\overline{\mathcal{X}}_G$, we obtain three connected components of the open admissible subset $\overline{X}_Q(p)^{\mathrm{rig,ord}}$:

$$\overline{X}_Q(p)^{\mathrm{rig,ord}} =]\overline{X}_G^{mm,\mathrm{ord}}[\sqcup]\overline{X}_G^{me,\mathrm{ord}}[\sqcup]\overline{X}_G^{ee,\mathrm{ord}}[$$

We need to extend this to admissible quasi-compact neighborhoods of $\overline{X}_Q(p)^{\mathrm{rig,ord}}$. First we fix a lifting E of the Hasse invariant (see [15] Sect.3, or see next section below). Let $\mathcal{G}^{\mathrm{rig}} \to \overline{X}^{\mathrm{rig}}$ be the rigid analytification of the semi-abelian scheme $\mathcal{G} \to \overline{X}$ (as in Chap.9, ex.2 of [5]). By a Theorem of Abbès and Mokrane [1] Prop.8.2.3 (and [2] for an improved radius of convergence), the open subdomain $\overline{X}^{\mathrm{rig}}(p^{-a})$ of $\overline{X}^{\mathrm{rig}}$ defined as the locus where the lifting E of the Hasse invariant satisfies $|E|_p > p^{-a}$ ($a = \frac{1}{p(p-1)}$ for [1], and $a = \frac{p-1}{2p-1}$ for [2]) is endowed with a finite flat group scheme C_{can} of rank p^2 whose restriction to the ordinary locus is canonically isomorphic to $\mathcal{G}[p]^0$. For each $r \in]p^{-a}, 1[\cap p^{\mathbb{Q}}$, we define

$$\overline{X}\{r\} = \{x \in \overline{X}^{\mathrm{rig}}(L); |E|_p \geq r\}$$

These domains are admissible, quasi-compact relatively compact neighborhoods of $\overline{X}_Q(p)^{\mathrm{rig,ord}}$ (cf.[19] Sect.3.1.6). Let $\overline{X}_Q(p)\{r\}$ be the inverse image of $\overline{X}\{r\}$ by $\overline{\pi}^{\mathrm{rig}}$.

Proposition 2.8 *1) For any r sufficiently close to* 1, *the neighborhood $\overline{X}_Q(p)\{r\}$ has still three connected components denoted $\overline{X}_G^{\alpha\beta}\{r\}$ ($\alpha, \beta \in \{e, m\}$); $\overline{X}_G^{\alpha\beta}\{r\}$ is defined as the largest connected subset of $\overline{X}_Q(p)\{r\}$ containing $]\overline{X}_G^{\alpha\beta,\mathrm{ord}}[$.*
2) For any $r \in]p^{-a}, 1[$, the isomorphism $]\overline{X}_G^{mm,\mathrm{ord}}[\cong \overline{X}^{\mathrm{rig,ord}}$ induced by the forgetful morphism extends to an isomorphism $\overline{X}_G^{mm,\mathrm{rig}}\{r\} \cong \overline{X}\{r\}$ (the inverse morphism being given by the canonical subgroup).

Proof: Since we won't need the first part of the proposition, we won't prove it in this paper. For the second statement, which is crucial to our conjecture, we notice that by definition, the morphism $\overline{\pi}$ sends $\overline{X}_G^{mm}\{r\}$ into $\overline{X}\{r\}$ while the inverse map is provided by the canonical subgroup as in [1] Prop.8.2.3.
Finally, we note that the involution W extends to the toroidal compactifications hence defines an involution of $\overline{X}_Q(p)^{\mathrm{rig}}$ which exchanges $]\overline{X}_G^{mm,\mathrm{ord}}[$ and $]\overline{X}_G^{ee,\mathrm{ord}}[$ resp. $\overline{X}_G^{mm}\{r\}$ and $\overline{X}_G^{ee}\{r\}$ and leaves stable the middle component $]\overline{X}_G^{em,\mathrm{ord}}[$ resp. $\overline{X}_G^{em}\{r\}$.

Finally, we can consider in a similar way the extension to compatible toroidal compactifications $\overline{X}_{U_B}(p)$ and $\overline{X}_B(p)$ of the morphisms $\pi_{U_B,B}$ and $\pi_{B,Q}$. We shall consider the inverse image by

$$\pi_{B,Q} \circ \pi_{U_B,B} : \overline{X}_{U_B}(p)^{\mathrm{rig}} \to \overline{X}_Q(p)^{\mathrm{rig}}$$

of $\overline{X}_G^{mm}\{r\}$.

3 Siegel modular forms

3.1 Arithmetic Siegel modular forms and q-expansion

In [26], care has been taken to define the arithmetic Siegel varieties and modular forms adelically. However, here for simplicity, we restrict our attention to one connected component X corresponding to a discrete subgroup $\Gamma \subset Sp_4(\mathbb{Z})$. We assume that X has a geometrically connected model over $\mathbb{Z}[1/N]$. We also assume that Γ is neat, so that the problem of classifying principally polarized abelian surfaces with Γ-level structure is a fine moduli problem (if it is not the case, see [26] Section 3 where X is only a coarse moduli problem).
Let $f : A \to X$ be the universal principally polarized abelian surface with Γ-level structure η over $\mathbb{Z}[1/N]$. We put $\underline{\omega} = e^*\Omega_{A/X}$, where e denotes the unit section.
For any pair of integers $\kappa = (k, \ell)$ $(k \geq \ell)$, we consider the rational representation of $GL(2)$: $W_\kappa(\mathbb{Q}) = \mathrm{Sym}^{k-\ell} \otimes \det^\ell St_2$. Here, St_2 denotes the standard two-dimensional representation of $GL(2)$; the standard Levi M of the Siegel parabolic of Sp_4 is identified to $GL(2)$ by
(4.1.1) $U \mapsto \mathrm{diag}(U, s^tU^{-1}s)$
The twist by s occurs because our choice of the symplectic matrix J defining G involves the matrix s instead of 1_2. We use (4.1.1) to identify M to $GL(2)$. Let $B_M = TN_M$ be the Levi decomposition of the standard Borel of M (corresponding to the group of upper triangular matrices in $GL(2)$). In order to define integral structures on the space of Siegel modular forms, it will be useful to consider an integral structure of $W_\kappa(\mathbb{Q})$. Since there is in general an ambiguity for such an integral structure, we need to make our choice explicit: following [15] Sect.3, we take it to be the induced $\mathbb{Z}$-module $W_\kappa = \mathrm{Ind}_{B_M}^M \kappa$. For any ring R, we put $W_\kappa(R) = W_\kappa \otimes R$.
Let $\mathcal{T} = \mathrm{Isom}_X(\mathcal{O}_X^2, \underline{\omega})$ be the right $GL(2)$-torsor over X of isomorphisms $\phi : \mathcal{O}_X^2 \to \underline{\omega}$. By putting $\omega_1 = \phi((1,0))$ and $\omega_1 = \phi((0,1))$, it can also be viewed as the moduli scheme classifying quintuples $(A, \lambda, \eta, \omega_1, \omega_2)$ where A, λ is a principally polarized abelian varieties with a Γ level structure η over a base S, endowed with a basis (ω_1, ω_2) of $\underline{\omega}_{A/S}$. One writes $\pi : \mathcal{T} \to X$ for the structural map. Note that $\pi_*\mathcal{O}_\mathcal{T}$ carries a left action (by right translation) of $GL(2)$.
Then, for any $\kappa = (k, \ell) \in \mathbb{Z}^2$, one defines the locally free sheaf $\underline{\omega}^\kappa$ over X as $(\pi_*\mathcal{O}_\mathcal{T})^{N_M}[\kappa^{-1}]$. Its sections are functions on $\mathcal{T}$ such that for any $\phi \in \mathrm{Isom}_X(\mathcal{O}_X^2, \underline{\omega})$, for any $t \in T$ and any $n \in N_M$, $f(A, \lambda, \eta, \phi \circ tn) = \kappa(t)^{-1} f(A, \lambda, \eta, \phi)$.
One sees easily that $\pi^*\underline{\omega}^\kappa = W_\kappa(\mathcal{O}_\mathcal{T})$, so that $\underline{\omega}^\kappa$ is a locally free sheaf which is non zero if and only if $k \geq \ell$.

We briefly recall some notations concerning toroidal compactifications, canonical extensions of sheaves and q-expansions. It will allow us in particular to define the cuspidal subsheaf $\underline{\omega}_\kappa$ of the canonical extension of $\underline{\omega}^\kappa$.
For any ring R, let $S_2(R)$ be the module of symmetric 2×2-matrices with

entries in R. Recall that the bilinear form $Tr : S_2(\mathbb{R}) \times S_2(\mathbb{R}) \to \mathbb{R}$ identifies the dual of $S_2(\mathbb{Z})$ to the module $\mathcal{S}$ of matrices $\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$, $a, b, c \in \mathbb{Z}$.

Let $S_2(\mathbb{R})^+$ be the cone of definite positive matrices in $S_2(\mathbb{R})$ and $\widetilde{S}_2$ the cone of semi-definite positive matrices whose kernel is $\mathbb{Q}$-rational.

A standard rational boundary component of level N is a pair $(Z, \phi : \frac{1}{N}Z/Z \to (\mathbb{Z}/N\mathbb{Z})^r)$ where Z is a free non zero quotient of $\mathbb{Z}^2$ (of rank r) and ϕ is an isomorphism. Let us view $\mathbb{Z}^2$ as the standard lagrangian $\langle e_1, e_2\rangle$ of $\mathbb{Z}^4$ endowed with the symplectic pairing ${}^t xJy$, Then, a general rational boundary component of level N is the image of a standard one by the action of $Sp_4(\mathbb{Z})$ on the space of lagrangians and on the projective space of $\mathbb{Z}^4$.

We denote by RBC_1, RBC_N, resp. $SRBC_1$, $SRBC_N$, the set of rational boundary components, resp. the set of standard rational boundary components. We can partition $\widetilde{S}_2 \cap S_2(\mathbb{Z})$ as $\sqcup_{Z \in SRBC_1} S(Z)^+$ where $S(Z)^+$ denotes the set of semidefinite symmetric matrices of $S_2(\mathbb{Z})$ which induce a positive definite quadratic form on Z.

Let $\Sigma = \{\Sigma_Z\}_{Z \in RBC_1}$ be an $Sp_4(\mathbb{Z})$-admissible family of rational polyhedral cone decompositions Σ_Z of $S(Z)^+$ (see [8] Chapt.I Def.5.8.2). As explained in [10] p.126, this decomposition can be used for any level N congruence subgroup Γ, since it is *a fortiori* Γ-admissible. To Σ, one can associate a toroidal compactification $\overline{X}$ over $\mathbb{Z}[\frac{1}{N}]$ of X as in [10] IV.6.7; it is smooth if Σ is sufficiently fine; this is assumed in the sequel.

The compactification $\overline{X}$ carries a degenerating semi-abelian scheme $\mathcal{G}$ extending A (see [10] Th.IV.5.7 and IV.6.7). One still denotes by $\underline{\omega}$ the sheaf $e^*\Omega_{\mathcal{G}/\overline{X}}$ where e is the unit section of $\mathcal{G} \to \overline{X}$.

Recall that $\overline{X}$ is a projective smooth, geometrically connected scheme over $\mathbb{Z}[\frac{1}{N}]$. It is endowed with a projection map b to the minimal compactification $X^*_{\mathbb{Z}[\frac{1}{N}]}$. Let $D = \overline{X} \backslash X = b^{-1}(\partial X^*)$; it is a relative Cartier divisor with normal crossings; its irreducible components are smooth.

The rank two vector bundle $\underline{\omega}$ over $\overline{X}$ does not descend as a vector bundle on X^*; however its determinant $\omega = \det \underline{\omega}$ descends as an ample line bundle.

The $GL(2)$-torsor $\overline{\mathcal{T}} = \mathrm{Isom}_{\overline{X}}(\mathcal{O}^2_{\overline{X}}, \underline{\omega})$ (with structural map $\overline{\pi} : \overline{\mathcal{T}} \to \overline{X}$) allows to define "the canonical extension" of the vector bundles $\underline{\omega}^\kappa$ to $\overline{X}$: one can either define this extension as

$$\underline{\omega}^\kappa = (\overline{\pi}_* \mathcal{O}_{\overline{\mathcal{T}}})^{N_M}[\kappa^{-1}]$$

$(k \geq \ell)$. Or one can also use the $\mathbb{Z}$-structure $W_\kappa = \mathrm{Ind}_{B_M}^M \kappa$ of the rational representation $W_\kappa(\mathbb{Q})$ of $GL(2)$ in order to give an equivalent definition of $\underline{\omega}^\kappa$ as the sections of the $\overline{X}$-vector bundle $\overline{\mathcal{T}} \overset{GL_2}{\times} W_\kappa$; here, as usual, the contraction product is the quotient of the product by the equivalence relation $(\phi \circ g, w) \sim (\phi, g \cdot w)$ for any $\phi \in \overline{\mathcal{T}}$, $g \in GL_2$ and $w \in W_\kappa$. For details see [10] Chapter 4 and 6, [21] Sect.4 and [15] Sect.3.

Let $\underline{\omega}_\kappa = \underline{\omega}^\kappa(-D)$ the sub-vector bundle of $\underline{\omega}^\kappa$ on $\overline{X}$ whose sections vanish along D. Recall the Koecher principle: $H^0(\overline{X}\otimes\mathbb{C},\underline{\omega}^\kappa) = H^0(X\otimes\mathbb{C},\underline{\omega}^\kappa)$. We define

Definition 3.1 *For any $\mathbb{Z}[1/N]$-algebra R one defines the R-module of arithmetic Siegel modular forms resp. cusp forms, as $H^0(X\otimes R,\underline{\omega}^\kappa)$ resp. $H^0(\overline{X}\otimes R,\underline{\omega}_\kappa)$ which we write also $H^0(X\otimes R,\underline{\omega}_\kappa)$ by convention.*

For $R=\mathbb{C}$, these vector spaces canonically identify to the corresponding spaces of classical Siegel modular forms of level Γ and weight κ (see [15] Th.3.1).
The arithmetic q-expansion (at the ∞ cusp) is defined as follows.
Let $\eta = (Z,\phi)\in SRBC_N$ with $Z=\mathbb{Z}^2$ and with ϕ the canonical identification $\frac{1}{N}\mathbb{Z}^2/\mathbb{Z}^2 = \mathbb{Z}/N\mathbb{Z}^2$ (it is called the infinity cusp).
Consider the rational polyhedral cone decomposition (RPCD) Σ_η of $S_2(\mathbb{R})^+$ corresponding to η. Let $D_\eta = D\cap b^{-1}(\{\eta\})$. By definition, the completion of $\overline{X}$ along D_η admits an open cover by affine formal schemes $\mathcal{U}_\sigma$ ($\sigma\in\Sigma_\eta$) with a canonical surjective finite etale cover $\phi_\sigma : \mathcal{S}_\sigma\to\mathcal{U}_\sigma$ where $\mathcal{S}_\sigma = \mathrm{Spf}\,\mathbb{Z}[1/N][[q^T; T\in\mathcal{S}\cap\sigma^\vee]]$. The morphism ϕ_σ is Galois; its group is the stabilizer $\overline{\Gamma}_\sigma$ of σ in the image $\overline{\Gamma}$ of $\Gamma\cap Q$ by the projection $Q\to Q/U = M$. Recall that $M(\mathbb{Z}) = GL(2,\mathbb{Z})$ acts on $S_2(\mathbb{Z})^+$ by $g\cdot S = gS^tg$. Moreover, ϕ_σ is uniquely determined by the property that the pull-back by ϕ_σ of the restriction of $\mathcal{G}$ to $\mathcal{U}_\sigma$ is the canonical Mumford family

$$f_\sigma : \mathcal{G}_\sigma\to\mathcal{S}_\sigma$$

deduced by Mumford's construction (see [10] p.54) from the canonical degenerescence data in $\mathrm{DD}_{\mathrm{ample}}$ on the global torus $\tilde{G}_\sigma = \mathbf{G}_m^2$ over $\mathcal{S}_\sigma$, together with the standard level N structure $\mu_N^2\times(\mathbb{Z}/N\mathbb{Z})^2\to\tilde{G}_\sigma[N]$;
Given $f\in H^0(\overline{X},\omega^\kappa)$, for any rational polyedral cone σ, we restrict f to $\mathcal{U}_\sigma$ and pull it back to $\mathcal{S}_\sigma$ by ϕ_σ. The bundle $\underline{\omega}_{\mathcal{G}_\sigma/\mathcal{S}_\sigma}$ of the Mumford family is trivial, hence the pull-back of the torsor $\overline{\mathcal{T}}$ to $\mathcal{S}_\sigma$ is trivial too; it is isomorphic to $\mathcal{S}_\sigma\times GL(2)$. In consequence, $\phi_\sigma^*\underline{\omega}^\kappa$ is the trivial bundle $W_\kappa\otimes\mathcal{S}_\sigma$. Hence ϕ_σ^*f yields a series in $W_\kappa[[q^T; T\in\mathcal{S}\cap\sigma^\vee]]$ which is invariant by $\overline{\Gamma}$ where the action of $\gamma\in\overline{\Gamma}$ is given by $\gamma\cdot(\sum_T a_Tq^T) = \sum_T\rho_\kappa(\gamma)(a_T)q^{\gamma T^t\gamma}$. These series are compatible when one varies the cone σ either by restricting to its faces of by letting $\overline{\Gamma}$ act (this action permutes the cones in Σ_η); recall that $\bigcap_{\sigma\in\Sigma_\eta}\sigma^\vee = \widetilde{S}_2$; this implies that there exists one well-defined series which belongs to the intersection $W_\kappa[[q^T; T\in\mathcal{S}\cap\widetilde{S}_2]]$ of the rings $W_\kappa[[q^T; T\in\mathcal{S}\cap\sigma^\vee]]$ and which is fixed by $\overline{\Gamma}$. It is called the q-expansion or Fourier expansion (at the infinity cusp) of f:

$$FE(f)\in W_\kappa[[q^T; T\in\mathcal{S}\cap\widetilde{S}_2]]^{\overline{\Gamma}}$$

For any $\mathbb{Z}[1/N]$-algebra R and any form $f\in H^0(X\times R,\omega^\kappa)$ defined over R, one defines an analogue series $FE_R(f)$ with coefficients in $W_\kappa(R) = W_\kappa\otimes R$.

Proposition 3.2 *1) (q-expansion principle) If f is any form defined over R, if the coefficients of its q-expansion vanish in $W_\kappa(R)$, then $f = 0$.*
2) The map FE sends the submodule of cusp forms over any ring R to the submodule of $W_\kappa(R)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]^{\overline{\Gamma}}$ of series whose coefficients $a_T \in W_\kappa(R)$ vanish unless $T \in \mathcal{S} \cap S_2(\mathbb{R})^+$.

The first point follows from the irreducibility of the modular scheme; the second from the examination of $\phi_\sigma^*(f)$ along $\phi_\sigma^* D$.

Remark: By comparing the two definitions of ω^κ given above, one sees that

$$W_\kappa[[q^T; T \in \mathcal{S} \cap \sigma^\vee]] = (\overline{\pi}_* \mathcal{O}_{\overline{T}})^{N_M}[\kappa^{-1}] \otimes_{\mathcal{O}_{\overline{X}}} \mathbb{Z}[[q^T; T \in \mathcal{S} \cap \sigma^\vee]]$$

We shall use this when comparing q-expansion of classical forms to q-expansion of p-adic forms.

3.2 p-adic Siegel modular forms and q-expansion

Let X as in the previous subsection. We fix a fine Γ-admissible family of rational polyedral cone decompositions Σ_ξ; we denote by For any integer $m \geq 1$, let X_m be the pull-back of X to $\mathbb{Z}/p^m\mathbb{Z}$. Let S_m be the ordinary locus and for each $n \geq 1$, consider $T_{m,n} = \mathrm{Isom}_{S_m}(\mu_{p^n}^2, A[p^n]^0) = \mathrm{Isom}_{S_m}(A[p^n]^{et}, (\mathbb{Z}/p^n\mathbb{Z})^2)$; for any $n \geq 1$, $T_{m,n}$ is a connected Galois cover of S_m of Galois group $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ (see [10] Prop.7.2).
Let $V_{m,n} = H^0(T_{m,n}, \mathcal{O}_{T_{m,n}})$, $V_{m,\infty} = \bigcup_{n \geq 1} V_{m,n}$. One can define the Σ-"toroidal compactification" $\overline{S}_m$ of S_m as the locus of $\overline{X}_m$ over which $\mathcal{G}[p]^0$ is of multiplicative type; similarly, define $\overline{T}_{m,n}$ as

$$\mathrm{Isom}_{\overline{X} \otimes \mathbb{Z}/p^m\mathbb{Z}}(\mu_{p^n}^2, \mathcal{G}[p^n]^0)$$

We still denote by D the pull-back to $\overline{T}_{m,n}$ of the divisor at ∞. We can now define $V_{!,m,n} = H^0(\overline{T}_{m,n}, \mathcal{O}_{\overline{T}_{m,n}}(-D))$ and $V_{!,m,\infty} = \bigcup_m V_{!,m,n}$. We also consider the corresponding p-adic limits: $S_\infty = \varinjlim S_m$, $T_{\infty,\infty} = \varinjlim T_{m,\infty}$, $V = \varprojlim V_{m,\infty}$ and $V_! = \varprojlim V_{!,m,\infty}$. These last two spaces are respectively the space of generalized p-adic modular forms resp. cusp forms.
Let $\mathbf{M}$ resp. $\mathbf{N_M}$ be the group of $\mathbb{Z}_p$-points of $M = GL_2$ resp. N_M the unipotent radical of the standard Borel B_M of M. Then, $T_{\infty,\infty} \to S_\infty$ is a right $\mathbf{M}$ étale torsor, hence $\mathbf{M}$ acts on the left (by right translations) on V (and $V_!$) by $m \cdot f(\psi) = f(\psi \circ m)$. Let $LC(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}/p^m\mathbb{Z})$ resp. $\mathcal{C}(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}_p)$ be the ring of $\mathbb{Z}/p^m\mathbb{Z}$-valued locally constant, resp. $\mathbb{Z}_p$-valued continous functions on $\mathbf{M}/\mathbf{N_M}$, viewed as a left $\mathbf{M}$-module via the left translation action. In particular, these modules are $\overline{\Gamma}$-modules. Note that $\mathcal{C}(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}_p) = \mathrm{projlim}\, LC(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}/p^m\mathbb{Z})$.
Let us define now the p-adic q-expansion map. It is a ring homomorphism

$$\mathrm{FE} : V^{\mathbf{N_M}} \to \Big(\mathcal{C}(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]\Big)^{\overline{\Gamma}}$$

given as follows.
For the infinity cusp η defined above, and for any $\sigma \in \Sigma_\eta$, we consider the base change $\phi_{\sigma,m}$ of the morphism $\phi_\sigma : \mathcal{S}_\sigma \to \mathcal{U}_\sigma$ to $\mathbb{Z}/p^m\mathbb{Z}$. As noticed above, the canonical Mumford family $f_\sigma : \mathcal{G}_\sigma \to \mathcal{S}_\sigma$ admits a canonical rigidification $\psi_{can} : \mu_{p^\infty}^2 \cong \mathcal{G}_\sigma[p^\infty]^0$ induced from the tautological rigidification of $\widetilde{G}_\sigma = \mathbf{G}_m^2$. This provides a canonical lifting $\Phi_{\sigma,m} : \mathcal{S}_\sigma \to \overline{T}_{m,\infty}$ of $\phi_{\sigma,m}$. These liftings are compatible when m grows, this gives rise to a lifting $\Phi_\sigma : \mathcal{S}_{\sigma\widehat{(p)}} \to \overline{T}_{\infty,\infty}$ of $\phi_\sigma : \mathcal{S}_{\sigma\widehat{(p)}} \to \mathcal{U}_{\sigma\widehat{(p)}}$ (the hat means p-adic completion).
For $f \in V$, one can therefore take the pull-back of $f \bmod p^m$ by $\Phi_{\sigma,m}$ (resp. of f by Φ_σ). The resulting series belongs to $\mathcal{O}_{\mathcal{S}_\sigma} \otimes \mathbb{Z}/p^m\mathbb{Z} = \mathbb{Z}/p^m\mathbb{Z}[[q^T; T \in \mathcal{S} \cap \sigma^\vee]]$ resp. $\mathcal{O}_{\mathcal{S}_\sigma} \otimes \mathbb{Z}_p = \mathbb{Z}_p[[q^T; T \in \mathcal{S} \cap \sigma^\vee]]$. It is however useful for further use to view it as belonging to $\mathcal{O}_{\mathcal{S}_\sigma} \otimes LC(\mathbf{M}, \mathbb{Z}/p^m\mathbb{Z})$ resp. to $\mathcal{O}_{\mathcal{S}_\sigma} \widehat{\otimes} \mathcal{C}(\mathbf{M}, \mathbb{Z}_p) = \mathcal{C}(\mathbf{M}, \mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \sigma^\vee]]$ in the following way: the map $x \in \mathbf{M} \mapsto \Phi_{\sigma,m}^*(x \cdot f)$ is an $\mathcal{O}_{\mathcal{S}_\sigma} \otimes \mathbb{Z}/p^m\mathbb{Z}$-valued locally constant map on $\mathbf{M}$. The evaluation of this function at $1 \in \mathbf{M}$ gives the $\mathbb{Z}/p^m\mathbb{Z}[[q^T; T \in \mathcal{S} \cap \sigma^\vee]]$-valued q-expansion mentioned above. By taking the inverse limit over m, one gets the desired q-expansion with coefficients in $\mathcal{C}(\mathbf{M}, \mathbb{Z}_p)$. Both $\mathbb{Z}_p$-coefficient and $\mathcal{C}(\mathbf{M}, \mathbb{Z}_p)$-coefficient q-expansions are compatible to restriction to faces; however, only the $\mathcal{C}(\mathbf{M}, \mathbb{Z}_p)$-coefficient expansion is compatible to the action of $\overline{\Gamma}$; we conclude that the functions $x \in \mathbf{M} \mapsto \Phi_\sigma^*(x \cdot f)$ for all σ's give rise to an element of the submodule $H^0(\overline{\Gamma}, \mathcal{C}(\mathbf{M}, \mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]])$ of $\overline{\Gamma}$- invariants of $\mathcal{C}(\mathbf{M}, \mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]$. We finally restrict our attention to $f \in V^{\mathbf{N_M}}$; thus we obtain a q-expansion in

$$\mathcal{C}(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]$$

We list below some well-known facts for which we refer to [15].

Proposition 3.3 *1) (p-adic q-expansion principle) For any $\sigma \in \Sigma_\eta$, for any $m \geq 1$, $V/p^mV \subset V_{m,\infty} \hookrightarrow \mathbb{Z}/p^m\mathbb{Z}[[q^T; T \in \mathcal{S} \cap \sigma^\vee]]$ is injective with flat cokernel. In particular, the ring homomorphism* FE *is injective.*
2) The restriction of FE to the ideal $V_!$ of cusp forms takes values in the ideal generated by q^T for $T \in \mathcal{S} \cap S_2(\mathbb{R})^+$. and the q-expansion principle holds for cusp forms for any cone σ and any $m \geq 1$ as above.

We simply recall that the first point results from the irreducibility of $\overline{T}_{m,\infty}$ (Igusa irreducibility theorem, [10] V.7.2) and the second from direct examination of $\Phi_\sigma^*(f)$.

It remains to compare the classical and p-adic modular forms resp. q-expansions. The embedding of classical forms into V comes from the canonical morphism $\iota : T_{\infty,\infty} \to \mathcal{T}|S_\infty$ given by the fact that for an abelian variety A (of dimension 2) over a base S where p is nilpotent, any rigidification $\psi : \mu_{p^\infty}^2 \cong A[p^\infty]^0$ gives rise to an isomorphism $\mathcal{O}_S^2 \cong \underline{\omega}_{A/S}$. One checks easily that $\iota^* : H^0(X, \underline{\omega}^\kappa) \to V^{\mathbf{N_M}}[\kappa]$ and $\iota^* : H^0(X, \underline{\omega}_\kappa) \to V_!^{\mathbf{N_M}}[\kappa]$.

Thus given a classical form, we first view it as a section of $(\pi_*\mathcal{O}_\mathcal{T})^{N_M}$, then one restricts it to the ordinary locus and one takes its pull-back by the morphism ι.

The comparison of the two definitions of $\underline{\omega}^\kappa$ provides a commutative square expressing the compatibility of classical and p-adic q-expansions:

$$\begin{tikzcd}
V^{\mathbf{N_M}} \arrow[r] & H^0(\overline{\Gamma}, \mathcal{C}(\mathbf{M}/\mathbf{N_M}, \mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]) \\
H^0(X, \underline{\omega}^\kappa) \arrow[u] \arrow[r] & H^0(\overline{\Gamma}, W_\kappa(\mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]) \arrow[u]
\end{tikzcd}$$

In the case where κ is diagonal so that $W_\kappa(\mathbb{Z}_p)$ is free of rank one, one can formulate more simply the diagram by composing both horizontal maps by the evaluation of functions on $\mathbf{M}/\mathbf{N_M}$ at 1, sending $f : \mathbf{M}/\mathbf{N_M} \to \mathbb{Z}_p$ to $f(1)$. We thus get a commutative square

$$\begin{tikzcd}
V^{\mathbf{N_M}} \arrow[r] & \mathbb{Z}_p[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]) \\
H^0(X, \underline{\omega}^\kappa) \arrow[u] \arrow[r] & H^0(\overline{\Gamma}, W_\kappa(\mathbb{Z}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]) \arrow[u]
\end{tikzcd}$$

Let $H \in H^0(X_1, \det^{p-1}\underline{\omega})$ be the Hasse invariant on X_1. We fix an integer $t \geq 1$ sufficiently large such that H^t lifts to X over $\mathbb{Z}_p$. This can be achieved because $\det \underline{\omega}$ is ample. We denote by E such a lifting. Recall that $\mathrm{FE}(E) \equiv 1 \pmod p$; this is because $\mathrm{FE}(H) = 1$ in $\mathbb{Z}/p\mathbb{Z}[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]$.

By [15] Sect.3.6, the Hecke operators $U_{p,1} = [\mathbf{N_M}\mathrm{diag}(1,1,p,p)\mathbf{N_M}]$ and $U_{p,2} = p^{-3}[\mathbf{N_M}\mathrm{diag}(1,p,p,p^2)\mathbf{N_M}]$ do act on $V_!^{\mathbf{N_M}}$. Let $e = \lim (U_{p,1}U_{p,2})^{n!}$ be the corresponding idempotent of $\mathrm{End}_{\mathbb{Z}_p} V_!^{\mathbf{N_M}}$. The module $eV_!^{\mathbf{N_M}}$ is called the module of ordinary p-adic cusp forms (with strict Iwahori p-level). Hida's control theorem [15] Th.1.1 says that for any weight κ (not necessarily cohomological), the cokernel of the inclusion $eH^0(S_\infty, \underline{\omega}_\kappa) \subset eV_!^{\mathbf{N_M}}[\kappa]$ is finite.
Comment: Actually, Th.1.1 of [15] also contains a "classicity statement", but only for very regular weights. Since we need in [26] an analogue of this statement including all cohomological weights (including those such that $k = \ell$), we prove it there for all cohomological weights after localisation to a non-Eisenstein maximal ideal of the Hecke algebra.
This theorem is crucial for us in [26] in order to produce overconvergent cusp forms g satisfying
(LIM) The q-expansion of g is the p-adic limit of q-expansions of cusp eigenforms of cohomological weight.
This condition provides the framework for the conjecture stated in the present paper. On the other hand, it would be very interesting to generalize Hida theorem to p-adic forms with finite slope for $U_{p,1}$ different from 0. Such a generalization would produce new overconvergent forms satisfying (LIM).

3.3 Overconvergence

We endow $\mathbb{C}_p$ with the p-adic norm such that $||_p = p^{-1}$. For any extension L of $\mathbb{Q}_p$ contained in $\mathbb{C}_p$ and for any real number $r \in]0,1[$, we consider the L-vector space of r-overconvergent Siegel modular forms

$$S_\kappa(\Gamma; r) = H^0(\overline{X}\{r\} \times L, \underline{\omega}_\kappa)$$

If r is in $|L^\times|_p$, this is a Banach space for the norm $|f| = \sup_{x\in\overline{X}\{r\}(L)}|f(x)|_p$ by [5] Th.4.1.6. In particular, for any $r < r'$ in $]p^{-a}, 1[\cap|L^\times|_p$, the inclusions

$$\mathrm{res}_{r,r'} : S_\kappa(K; r) \hookrightarrow S_\kappa(K; r')$$

are completely continuous by [19] 2.4.1.
It should be noted that the above fact does not require the assumption that the weight κ be cohomological (that is $k_1 \geq k_2 \geq 3$). In [26], we indeed apply this to $\kappa = (2, 2)$.

Let a be either the Abbès-Mokrane bound ($a = \frac{1}{p(p-1)}$) or the Andreatta-Gasbarri's bound ($a = \frac{p-1}{2p-1}$). By [1] Lemma 8.2.1 and [2], for any $r \in]p^{-a}, 1[$, the canonical lifting F_{can} of the Frobenius endomorphism is defined as a rigid morphism $\overline{X}\{r\} \to \overline{X}^{\mathrm{rig}}$.
The following two results are contained in [26] Sect.4.5

Proposition 3.4 *There exists $r \in]p^{-a}, 1[\cap p^{\mathbb{Q}}$ such that F_{can} maps $\overline{X}\{r\}$ into $\overline{X}\{r^p\}$ and is finite flat of degree p^3. It yields a continous homomorphism of Banach spaces $\phi = F^*_{can} : S_\kappa(\Gamma; r^p) \to S_\kappa(K; r)$ and a trace homomorphism $Tr_\phi : S_\kappa(\Gamma; r) \to S_\kappa(\Gamma; r^p)$.*

Corollary 3.5 *There exists $r \in]p^{-a/p}, 1[\cap|L^\times|_p$, the composition $\psi = \mathrm{res}_{r^p,r} \circ Tr_\phi$ defines a completely continuous endomorphism of the Banach space $S_\kappa(\Gamma; r)$.*

The evaluation on the rigid Mumford families $\mathcal{G}_\eta^{rig} \to \mathcal{S}_\sigma$ (for all polyedral cones σ in Σ_η as above) defines a L-linear homomorphism

$$\mathrm{FE} : S_\kappa(K; r) \hookrightarrow L[[q^T; T \in \mathcal{S} \cap S_2(\mathbb{R})^+]].$$

The overconvergent q-expansion principle says that FE is injective. It follows directly from the connectedness of $\overline{X}^{rig}$.
We define $U_{p,1}$ as $p^{-3}\psi$ the operator corresponding to the weight $\kappa = (2, 2)$. We denote by $S_2(\Gamma; r)$ the L-Banach space of r-overconvergent forms of weight $(2, 2)$. Then it follows immediately from Cor.3.3 that

Corollary 3.6 *There exists $r \in]p^{-a/p}, 1[\cap|L^\times|_p$ such that the operator $U_{p,1}$ is completely continuous on the Banach space $S_2(\Gamma; r)$ of weight 2 overconvergent p-adic cusp forms.*

Recall that by [24] Prop.7, one can define a Fredholm determinant $P(t) = \det(1 - tU_{p,1})$ which is a p-adic entire function of t and such that $\lambda \in \overline{\mathbb{Q}}_p$ is a non-zero eigenvalue of $U_{p,1}$ if and only if $P(\lambda^{-1}) = 0$; so that the non-zero eigenvalues of $U_{p,1}$ form a sequence decreasing to 0. By Prop.12 and Remark 3 following this proposition in [24], each spectral subspace associated to a non-zero eigenvalue is finite dimensional (its dimension being equal to the multiplicity of the root λ^{-1} of P) and there is a direct sum decomposition of the Banach space as the sum of the (finite dimensional) spectral subspace and the largest closed subspace on which $U_{p,1} - \lambda$ is invertible.

In particular, for any positive number α, the set of eigenvalues $\lambda_i \in \overline{\mathbb{Q}}_p$ of $U_{p,1}$ such that $ord_p(\lambda_i) \leq \alpha$ is finite. Moreover one has a direct sum decomposition of the Banach space $S_2(\Gamma, r)$ as $S_2(\Gamma, r)^{\leq \alpha} \oplus S_2(\Gamma, r)^{>\alpha}$, where the first space is finite dimensional, defined as the direct sum of the spectral subspaces for all eigenvalues λ_i with $ord_p(\lambda_i) \leq \alpha$, and the second is the (closed) largest subspace on which all the operators $U_{p,1} - \lambda_i$ are invertible.

4 Galois representations of low weight and overconvergent modular forms

4.1 Eichler-Shimura maps

Let $\kappa = (k, \ell)$ be a cohomological weight, that is, a pair of integers such that $k \geq \ell \geq 3$. Let $k = a + 3$, $\ell = b + 3$. Then, (a, b), $a \geq b \geq 0$ is a dominant weight for (G, B, T); let $V_{a,b}$ be the local system on the Siegel variety associated to the irreducible representation of G of highest weight (a, b); recall that the central character of this representation is $z \mapsto z^{a+b}$. For any (neat) compact open subgroup L of G_f, for $a' \geq b' \geq 0$ and $k' = a' + 3$, $\ell' = b' + 3$, there is a canonical Hecke-equivariant linear injection

$$H^0(S_L, \underline{\omega}_\kappa) \hookrightarrow H^3(S_L, V_{a,b}(\mathbb{C}))$$

See Section 3.8 of [15] where it is explained how to make it canonical, and where it is called the Eichler-Shimura map. Actually the image is contained in $H^3_! = \mathrm{Im}(H^3_c \to H^3)$. It follows for instance from Th.5.5, Chapter VI of [10].

4.2 Galois representation associated to a cohomological cusp eigenform

Let f be a cusp eigenform of cohomological weight $\kappa = (k, \ell)$. Let $k = a + 3$, $\ell = b + 3$. By the EIchler-Shimura injection, the Hecke eigensystem associated to f occurs in $H^3(X(\mathbb{C}), V_{a,b}(\mathbb{C}))$. For any prime q prime to N, let $P_{f,q} \in \mathbb{C}[X]$ be the degree four Hecke polynomial at q for the eigensystem of f (see [26]).

Let E be the number field generated by the eigenvalues of the Hecke operators outside N. We fix a p-adic embedding ι_p of $\overline{\mathbb{Q}}$; let $F \subset \overline{\mathbb{Q}}_p$ be a p-adic field containing $\iota_p(E)$ (big enough but of finite degree).

The Galois representation $W_f = H^3(S_K, V_{a,b}(F)))_f$ (largest subspace where Hecke acts as on f) is E-rational and pure of Deligne weight $\mathbf{w} = 3 + a + b$.
Let S be the set of prime divisors of N, and Γ be the Galois group of the maximal algebraic extension of $\mathbb{Q}$ unramified outside S and p. By a series of papers (due to R. Taylor, Laumon and Weissauer) there exists a degree four Galois representation $R_{f,p} : \Gamma \to GL_4(\overline{\mathbb{Q}}_p)$ such that for any $\ell \notin S \cup \{p\}$, $\det(X \cdot 1_4 - R_{f,p}(Fr_\ell)) = P_{\pi,\ell}(X)$.
Its relation to W_f is: $W_f^4 = R_{f,p}^m$, where $m = \dim W_f$.
We take F big enough for $R_{f,p}$ to be defined over it.
Remark: Let $\epsilon : \Gamma \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character. With the convention above, we have $\nu \circ \rho_{\pi,p} = \epsilon^{-\mathbf{w}} \cdot \omega_f$, where ω_f is a finite order character modulo N, given as the Galois avatar of the companion character of f (this can viewed using Poincaré duality for W_f, see for instance [25], beginning of Sect.2).
Remark: Given a classical cusp eigenform $g \in H^0(X, \omega_{(2,2)})$, there is no geometric construction of an associated Galois representation (there is no Eichler-Shimura map to transport the eigensystem to the étale cohomology). See below for a p-adic construction, if the q-expansion of g is a p-adic limit of q-expansions of cohomological weight cusp eigenforms.

4.3 A conjecture

Let $g \in H^0(\overline{X}\{r\}, \omega_{(2,2)})$ be an overconvergent cusp eigenform of weight $(2,2)$ and auxiliary level group K (unramified at p). By Prop.2.6, 2, since $\overline{X}\{r\}$ is canonically identified to $\overline{X}_G^{mm}\{r\} \subset \overline{X}_Q(p)^{\mathrm{rig}}$, one can view g as an element of $H^0(\overline{X}_G^{mm}\{r\}, \omega_{(2,2)})$, where $\overline{X}_G^{mm}\{r\}$ is a strict neighborhood of $]\overline{X}_G^{mm}[$ in $\overline{X}_Q(p)^{\mathrm{rig}}$. We shall actually need to consider the pull-back of g by $\pi_{B,Q} \circ \pi_{U_B,B}$ as a section of $\underline{\omega}_{2,2}$ over the quasi-compact relatively compact rigid open

$$(\pi_{B,Q} \circ \pi_{U_B,B})^{-1}(\overline{X}_G^{mm}\{r\})$$

in $\overline{X}_{U_B}(p)^{\mathrm{rig}}$.
Assume that

(LIM-EIG) there exists a sequence (g_i) of classical cusp eigenforms $g_i \in H^0(\overline{X}_{U_B}(p), \omega_{\kappa_i})$ with cohomological weights $\kappa_i = (k_i, \ell_i)$ and level K (that is, prime to p, equal to the auxiliary level of g) such that the q-expansions of the g_i's converge p-adically to that of g.

Let Π_{U_B} be the subgroup of matrices in $G(\mathbb{Z}_p)$ whose reduction modulo p belongs to $U_B(\mathbb{Z}/p\mathbb{Z})$.

Comments: 1) Note that the key-point in this assumption is that the forms g_i are eigenforms. If we insist that the sequence of p-adic weights satisfies $\kappa_i \equiv (2,2) \pmod{p-1)p^i}$, we cannot assume in general that the level of the g_i's is prime to p; then we simply need to replace $K_p = G(\mathbb{Z}_p)$ by Π_{U_B} as

p-component of the level group in (LIM-EIG). We can motivate the choice of the p-level group Π_{U_B} by recalling that both in the proof of the main theorem of [6] and in the Control Theorem for the Iwahori levels for $GSp(4)$ of [27], it has been natural to consider the pull-back of g by $\pi_{B,Q} \circ \pi_{U_B,B}$ as a section of $\underline{\omega}_{2,2}$ over the strict neighborhood

$$(\pi_{B,Q} \circ \pi_{U_B,B})^{-1}(\overline{X}_G^{mm}\{r\})$$

in $\overline{X}_{U_B}(p)^{\mathrm{rig}}$. This is the analogue of Hida's p-stabilization for p-adic modular forms.
2) Note also that it is a well-known theorem [15] that any p-adic cusp form is the p-adic limit (in the sense of q-expansions) of prime-to-p level classical cusp forms of weights κ_i satisfying $\kappa_i \equiv (2,2) \pmod{p-1}$, where however, the forms g_i's are not necessarily eigen even if g is.

Recall then that for any weight κ, there is a q-expansion map (always at the infinity cusp)

$$H^0((\pi_{B,Q} \circ \pi_{U_B,B})^{-1}(\overline{X}_G^{mm}\{r\}), \underline{\omega}_\kappa) \to W_\kappa(\mathbb{Q}_p)[[q^T; T \in \mathcal{S} \cap \widetilde{S}_2]]^{\overline{\Gamma}}$$

These maps are compatible with the p-adic q-expansion map via the canonical injection of $H^0((\pi_{B,Q} \circ \pi_{U_B,B})^{-1}(\overline{X}_G^{mm}\{r\}), \underline{\omega}_\kappa)$ into the space of p-adic cusp forms.
We give below a conjectural criterion for the analytic continuation of g to $\overline{X}_{U_B}(p)^{\mathrm{rig}}$.
Let $\rho_{g,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_4(\overline{\mathbb{Q}}_p)$ be the Galois representation associated to the limit of the pseudo-representations of the g_i's. We call it the Galois representation associated to g. Note that by Sen theory (Bull. Soc. Math. de France 1999), if the κ_i converge to $(2,2)$ in $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ and if $\rho_{g,p}$ is Hodge-Tate, its p-adic Hodge-Tate weights should be $0, 0, 1, 1$. Our conjecture reads as follows.

Conjecture: *Let $g \in S_{2,2}(K, r)$ be an overconvergent cusp eigenform satisfying* (LIM-EIG)*; assume that there exists an abelian surface A defined over $\mathbb{Q}$ such that $\rho_{g,p}$ is isomorphic to the contragredient $\rho_{A,p}^\vee$ of the representation on the p-adic Tate module of A. Then, g extends to a global section $g \in H^0(\overline{X}_{U_B}(p)^{\mathrm{rig}}, \omega_{(2,2)})$ thus defining by the rigid GAGA principle a classical cusp form of weight $(2,2)$ and level $K^p \times \Pi_{U_B}$.*
If the abelian variety has good reduction at p, the cusp eigenform has level prime to p.

Remark: The minimal level group $\Pi_{g,p}$ at p of the classical cusp eigenform g satisfies $\Pi_{U_B} \subset \Pi_{g,p} \subset G(\mathbb{Z}_p)$; the compatibility between gobal and local Langlands correspondences predicts that the (local) Weil-Deligne representation associated to $D_{pst}(\rho_{g,p})$ determines $\Pi_{g,p}$.

The main result (Theorem 4) of [26] provides under certain assumptions (primarily the assumption of near ordinarity) such pairs of an overconvergent cusp eigenform g with a converging sequence (g_i) of cusp eigenforms, together with an abelian surface A defined over $\mathbb{Q}$ with potential good ordinary reduction at p.

Actually one starts there from an abelian surface satisfying certain condition, the most stringent being that the Galois representation $\rho_{A,p}^\vee$ must be congruent modulo p to the representation $\rho_{f,p}$ associated to a cusp eigenform of level K prime to p, ordinary at p with cohomological weight. Then Hida theory ([26] Lemma 4.2) yields a sequence (g_i) converging to a limit g which is overconvergent of weight $(2,2)$ and auxiliary level K.

Note that once a generalization of Coleman Families Theory to the Siegel case is available, there might be new examples of such forms g.

In the situation treated in [26], the representation $\rho_{g,p} = \rho_{A,p}^\vee$ is potentially crystalline but not crystalline, which implies that the eigenforms g_i are indeed p-new of p-level Π_{U_B}, hence the presence of Π_{U_B} as conjectural p-level group of g.

The conjecture above would imply that the L function of the motive $h^1(A)$ is automorphic: $L(h^1(A),s) = L_{\rm spin}(g,s)$, hence, by a classical theorem of Piatetskii-Shapiro, it would have analytic continuation and functional equation.

References

[1] A. Abbès, A. Mokrane: *Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes*, Publ. Math. IHES 99, 2004, pp.117-162.

[2] F. Andreatta, M. Gasbarri: *The canonical subgroup for families of abelian varieties*, preprint.

[3] D. Blasius: *A rank* 3 *gneralization of the Conjecture of Shimura and Taniyama*, Comp. Math.142 (2006), 1151-1156.

[4] S. Bosch: *Zur kohomologietheorie rigid analytischen Raüme*, Manuscr. Math. 20 (1977).

[5] S. Bosch, U. Güntzer, R. Remmert: Non-archimedean Analysis. A systematic approach, Grundlehren der Mathematischen Wissenschaften, Bd 261, Springer Verlag 1984.

[6] K. Buzzard, R. Taylor : *Companion forms and weight one forms*, Ann. of Math., 149 (1999), 905-919.

[7] K. Buzzard: *Analytic continuation of overconvergent eigenforms*, J. Amer. Math. Soc. 16 (2003), 29-55.

[8] C.-L. Chai : Compactification of Siegel moduli schemes, LMS Lect. Notes Series 107, C.U.P. 1985.

[9] C.-L. Chai, P. Norman : *Bad reduction of the Siegel moduli space of genus two with $\Gamma_0(p)$-level structure*, Amer. Journal of Math. 112 (1990), 1003-1071.

[10] G. Faltings, C.L. Chai : Degeneration of Abelian Varieties, Erg. Math. Wiss. 3.folge, 22, Springer Verlag, 1990.

[11] A. Genestier : *Un Modèle semistable de la variété de Siegel de genre* 3 *avec structures de niveau* $\Gamma_0(p)$, Comp. Math. 123, 303-328, 2000.

[12] A. Genestier, J. Tilouine: *Systèmes de Taylor-Wiles pour* $GSp(4)$, to appear in: Formes Automorphes II: le cas $GSp(4)$, Astérisque 302, Soc. Math. France 2005.

[13] T. J. Haines: *Introduction to Shimura varieties with bad reduction of parahoric type*, to appear in Clay Mathematics Proceedings volume 4 (2005), pp.583-642.

[14] M. Harris, R. Taylor : *Regular models of certain Shimura varieties*, Asian J. Math.6 (2002), no.1, 61-94.

[15] H. Hida : *Control theorems of coherent sheaves on Shimura varieties of PEL type*. J. Inst. Math. Jussieu 1 (2002), no. 1, 1–76.

[16] J. de Jong : *The moduli space of principally polarized abelian varieties with* $\Gamma_0(p)$*-level structure*, J. Alg. Geom. 2 (1993), 667-688.

[17] N. Katz: *p-adic properties of modular schemes and modular forms*,*in* Modular Forms of One Variable III, pp.69-189, Springer Lect. Notes 350, Springer 1972.

[18] M. Kisin : *Overconvergent modular forms and the Fontaine-Mazur conjecture*, Inv. Math.153 (2003), 374-454.

[19] M. Kisin, K.-F. Lai: *Overconvergent Hilbert modular forms*, Amer. J. Math.127, n^{0}4,2005, 735-783.

[20] D. Mumford : Abelian Varieties, Oxford Univ. Press 1970.

[21] A. Mokrane, J. Tilouine : *Cohomology of Siegel varieties with p-adic integral coefficients and Applications*, Astérisque 280, 2002.

[22] B.-C. Ngô, A. Genestier : *Alcôves et p-rang des variétés abéliennes*, Ann. Inst. Fourier (Grenoble) 52 (2002), 1665-1680.

[23] M. Rapoport, T. Zink: Period spaces for p-divisible groups, Ann. of Math. Studies 141, 1996, Princeton Univ.Press.

[24] J.-P. Serre: *Endomorphismes complètement continus des espaces de Banach p-adiques*, Publ. Math. de l'I.H.E.S., tome 12,(1962), p.69-85.

[25] R. Taylor : *On the ℓ-adic cohomology of Siegel threefolds*, Inv. Math. 114, 289-310 (1993).

[26] J. Tilouine : *Nearly ordinary degree four symplectic Galois representations and p-adic Siegel modular forms*, with an Appendix by D. Blasius, Comp. Math. 142 (2006), 1122-1156.

[27] J. Tilouine, E. Urban : *Several variable p-adic families of Siegel-Hilbert cusp eigensystems and their Galois representations*, Ann. Sci. Ec. Norm.Sup.(4), t.32 (1999), p.499-574.

[28] E. Urban : *Sur les représentations p-adiques associées aux représentations cuspidales de $GSp(4)_{\mathbb{Q}}$*, to appear in: Formes Automorphes II: le cas $GSp(4)$, Astérisque 302, Soc. Math. France 2005.

[29] C.-F. Yu : *Irreducibility of the Siegel Moduli Spaces with Parahoric Level Structures*,Int. Math. Res. Not. 2004 (48), p.2593-2597.

[30] Yoshida H.: *Siegel's Modular Forms and the Arithmetic of Quadratic Forms*, Inv. Math. 60, 193-248 (1980).

J. Tilouine
Département de Mathématiques
UMR 7539
Institut Galilée
Université de Paris 13
93430 Villetaneuse
France
tilouine@math.univ-paris13.fr

On p-Adic Geometric Representations of $G_{\mathbb{Q}}$

To John Coates

J.-P. Wintenberger

Received: August 30, 2005
Revised: September 15, 2006

Abstract. A conjecture of Fontaine and Mazur states that a geometric odd irreducible p-adic representation ρ of the Galois group of $\mathbb{Q}$ comes from a modular form ([10]). Dieulefait proved that, under certain hypotheses, ρ is a member of a compatible system of ℓ-adic representations, as predicted by the conjecture ([9]). Thanks to recent results of Kisin ([15]), we are able to apply the method of Dieulefait under weaker hypotheses. This is useful in the proof of Serre's conjecture ([20]) given in [11], [14],[12],[13].

2000 Mathematics Subject Classification: : 11R32, 11R39

1 Introduction.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. For L a finite extension of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}$, we write G_L for the Galois group of $\overline{\mathbb{Q}}/L$. For ℓ a prime number, we write $\mathbb{Q}_\ell$ for the field of ℓ-adic numbers and $\overline{\mathbb{Q}_\ell}$ for an algebraic closure of $\mathbb{Q}_\ell$.
An ℓ-adic representation ρ of G_L of dimension d is a continuous morphism ρ from G_L to $\mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$. In fact, ρ has values in $\mathrm{GL}_d(M)$, for M a finite extension of $\mathbb{Q}_\ell$ contained in $\overline{\mathbb{Q}_\ell}$ (lemma 2.2.1.1. of [6]). Such a representation ρ is said to be *geometric* if it satisfies the following two conditions ([10]):
- for $\mathcal{L}$ a prime of L above ℓ, the restriction of ρ to the decomposition subgroup $D_{\mathcal{L}}$ satisfies the potentially semi-stable condition of Fontaine's theory (exp. 8 of [1]) ;
- there exists a finite set S of primes of L such that ρ is unramified outside S and the primes above ℓ.
A geometric ℓ-adic Galois representation defines for each prime $\mathcal{L}$ of L an isomorphy class of representations of the Weil-Deligne group $\mathrm{WD}_{\mathcal{L}}$ in $\mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$

([8], exp. 8 of [1], [10]). We call $r_{\mathcal{L}}(\rho)$ its F-semisimplification. It is attached to the restriction of ρ to the decomposition group $D_{\mathcal{L}}$. When $\mathcal{L}$ is of characteristic ℓ, in order to define $r_{\mathcal{L}}$, one needs to use the action of $\mathrm{WD}_{\mathcal{L}}$ on the filtered Dieudonné module attached to the restriction of ρ to $D_{\mathcal{L}}$ via Fontaine's theory (see remark 1 of section 4).

Let E be a finite extension of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}$. By a *compatible system of geometric representations of* G_L *with coefficients in* E of dimension d, we mean the following data :

- for each ℓ and for each embedding ι of E in $\overline{\mathbb{Q}_\ell}$, a geometric representation $\rho_\iota : G_L \to \mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$,

- a finite set S of primes of L, and for each prime $\mathcal{L}$ of L, an F-semisimple representation $r_{\mathcal{L}}$ of $\mathrm{WD}_{\mathcal{L}}$ in $\mathrm{GL}_d(E)$, such that :

  - $r_{\mathcal{L}}$ is unramified if $\mathcal{L} \notin S$;
  - for each ι as above, $\iota \circ r_{\mathcal{L}}$ is isomorphic to $r_{\mathcal{L}}(\rho_\iota)$.

We fix a prime p. Let ρ be a p-adic geometric irreducible odd representation of dimension 2 of $G_{\mathbb{Q}}$. By odd, we mean that $\rho(c)$ has eigenvalues 1 et -1, for c a complex conjugation. We suppose that ρ has Hodge-Tate weights $(0, k-1)$, where k is an integer ≥ 2 : we shall say that ρ is of weight k. It is conjectured by Fontaine and Mazur that ρ comes from a modular form of weight k.

More precisely, let $k \geq 2$ and $N \geq 1$ be integers. Let $f = q + \ldots + a_n q^n + \ldots$ be a primitive modular form on $\Gamma_1(N)$ of weight k. Let $E(f)$ be its coefficient field, *i.e.* the field generated by the coefficients of f and the values of the character of f. The field $E(f)$ is a finite extension of $\mathbb{Q}$. It is classical that one can associate a p-adic representation $\rho(f)_\iota : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ to f and an embedding ι of $E(f)$ in $\overline{\mathbb{Q}_p}$. The representation $\rho(f)_\iota$ is unramified at ℓ if ℓ is $\neq p$ and does not divide N and is characterized by :

$$\mathrm{tr}(\rho(f)_\iota(\mathrm{Frob}_\ell)) = \iota(a_\ell),$$

for these ℓ. Furthermore, $\rho(f)_\iota$ is absolutely irreductible, odd, geometric, of conductor N and of weight k (Hodge-Tate weights $(0, k-1)$). The conjecture of Fontaine and Mazur states that ρ is isomorphic to $\rho(f)_\iota$ for an f and a ι.

A consequence of the conjecture of Fontaine and Mazur is that ρ is a member of a compatible system of Galois representations. Dieulefait proved that it is the case under certain hypotheses ([9]). Using a recent result of Kisin ([15]), we give weaker hypotheses under which the result of Dieulefait is true.

The main tool of the proof is a theorem of Taylor ([26] and [25]). There exists a totally real number field F which is Galois over $\mathbb{Q}$ and such that $\rho_{|G_F}$ comes from an cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of parallel weight k (or a Hilbert modular form for F). By Arthur-Clozel ([2]), for each F' such that the Galois group of F/F' is solvable, $\rho_{|G_{F'}}$ comes from an automorphic representation $\pi_{F'}$ for $\mathrm{GL}_2(\mathbb{A}_{F'})$. Using Brauer's theorem, we put together the compatible systems associated to the automorphic representations $\pi_{F'}$, and we obtain the compatible system of representations of $G_{\mathbb{Q}}$.

2 Taylor's theorem.

Let ρ be an odd irreducible geometric p-adic representation of $G_{\mathbb{Q}}$ of dimension 2 of weight k, k an integer ≥ 2.
We say that ρ is *potentially modular* if there exists a Galois totally real finite extension F of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}$ such that the restriction of ρ to G_F comes from a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of parallel weight k. The theorem of Taylor states in many cases that ρ is potentially modular. In fact, Taylor proves that the reduction $\overline{\rho}$ of ρ is potentially modular, with F unramified (resp. split) at p if the restriction of $\overline{\rho}$ to D_p is reducible (resp. irreducible). Then, the modularity of $\rho_{|G_F}$ follows from modularity theorems. According to which modularity theorem one applies, one get different statements. We write the following statement which is needed for our work with Khare on Serre's conjecture.

Théorème 1 *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be a p-adic representation, absolutely irreducible, odd, unramified outside a finite set of primes. One supposes that the reduction $\overline{\rho}$ of ρ has non solvable image and, if $p \neq 2$, that $\overline{\rho}$ has Serre's weight $k(\overline{\rho})$ in the range $[2, p+1]$. Then ρ is potentially modular in the following cases :*
- a1) $p \neq 2$ and $\rho_{|D_p}$ is crystalline of weight $k = k(\overline{\rho})$;
- a2) $p = 2$, $k(\overline{\rho}) = 2$ and $\rho_{|D_2}$ is Barsotti-Tate ;
- b) $p \neq 2$ and $k(\overline{\rho}) \neq p+1$, $\rho_{|D_p}$ is potentially Barsotti-Tate, Barsotti-Tate after restriction to $\mathbb{Q}_p(\mu_p)$, and the restriction of the representation of the Weil-Deligne group WD_p to inertia is $(\omega_p^{k-2} \oplus 1)$, where ω_p is the Teichmuller lift of the cyclotomic character modulo p ;
- c) $p \neq 2$ and $k(\overline{\rho}) = p+1$ or $p = 2$ and $k(\overline{\rho}) = 4$ and $\rho_{|D_p}$ is semistable of weight 2.

The theorem follows from the potential modularity of $\overline{\rho}$ ([26], [25]) and the modularity theorem stated in 8.3. of [13].
Remark. Using Skinner-Wiles modularity theorem ([22]), Taylor gives a variant of this statement in a lot of ordinary cases.

3 Field of coefficients of ρ.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be as in the preceeding section. Furthermore, we suppose that ρ is potentially modular.

Proposition 1 *There is a finite extension E of $\mathbb{Q}$ and an embedding $\iota_p : E \hookrightarrow \overline{\mathbb{Q}_p}$ and for each prime ℓ, a F-semisimple representation r_ℓ of the Weil-Deligne group WD_ℓ with values in $\mathrm{GL}_2(E)$ such that for each ℓ, the F-semisimplification $r_\ell(\rho)$ of the representation of the Weil-Deligne group WD_ℓ associated to ρ is isomorphic to $\iota_p \circ r_\ell$.*

Proof. Let F and π as in the theorem of Taylor. Let F' be a subfield of F such that F/F' has solvable Galois group. By Arthur and Clozel, we know that the restriction of ρ to $G_{F'}$ is also associated to a cuspidal representation $\pi_{F'}$ of $\mathrm{GL}_2(\mathbb{A}_{F'})$ ([2]). It follows that there exists a finite extension $E_{F'}$ of $\mathbb{Q}$ such that the F-semisimplification of the representation of the Weil-Deligne group $\mathrm{WD}_{\mathcal{L}}$ associated to the restriction of ρ to $G_{F'}$ can be realized in $E_{F'}$ for each prime $\mathcal{L}$ of F'. The rationality properties of $\pi_{F'}$ follows from Shimura for the unramified primes and from Rogawski-Tunnell for the ramified primes ([21], see also [19] ; [18]). The compatiblity of global and local Langlands correspondances follows for $\mathcal{L}$ of characteristic $\neq p$ from Carayol completed by Taylor ([7],[23]) and for $\mathcal{L}$ of characteristic p from Saito and Kisin ([19],[15]).

Take for E an extension of $\mathbb{Q}$ containing the images by all embeddings in $\overline{\mathbb{Q}}$ of the fields $E_{F'}$. Let $\mathcal{L}$ be a prime of F. Let $F'_{\mathcal{L}}$ be the subfield of F which is fixed by the decomposition subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ for $\mathcal{L}$. Let $\mathcal{L}'$ be the restriction of $\mathcal{L}$ to $F'_{\mathcal{L}}$. The representation of the Weil-Deligne group $\mathrm{WD}_{\mathcal{L}'}$ defined by the restriction of ρ to $F'_{\mathcal{L}}$ can be realized in $E_{F'_{\mathcal{L}}}$. As the Weil-Deligne groups WD_{ℓ} and $\mathrm{WD}_{\mathcal{L}'}$ coincide, the proposition follows.

Remark. Particular cases of the compatibility between global and local Langlands correspondences for the primes dividing the characteristic follows from Breuil, Berger and Taylor ([5],[3],[24]).

4 Construction of the compatible system.

Théorème 2 *Let ρ be as in the preceeding section. Then, there exists a compatible system (ρ_ι) of geometric representations of $G_{\mathbb{Q}}$ with coefficients in a number field E such that there exists an embedding $\iota_p : E \hookrightarrow \overline{\mathbb{Q}_p}$ with ρ_{ι_p} isomorphic to ρ. The ρ_ι are irreducible, odd and of weight k.*

Proof. If ρ is induced from the p-adic representation associated to a Hecke's character Ψ of an imaginary quadratic field, then one takes for (ρ_ι) the compatible system induced from the one defined by the Hecke character. Otherwise, ρ remains absolutely irreducible after restriction to any open subgroup of $G_{\mathbb{Q}}$. We suppose this from now.

Let F, π, $E(\pi)$ and ι_p such that $\rho_{|G_F}$ is isomorphic to the Galois representation $\rho(\pi)_{\iota_p}$ attached to π, and the embedding ι_p of the coefficient field $E(\pi)$ of π in $\overline{\mathbb{Q}_p}$. As in Taylor's 5.3.3. of [27], one applies Brauer's theorem to the trivial representation of $\mathrm{Gal}(F/\mathbb{Q})$. There exist fields $F_i \subset F$, such that each F/F_i has a solvable Galois group, integers $m_i \in \mathbb{Z}$ and characters Ψ_i of $\mathrm{Gal}(F/F_i)$ such that the trivial representation of $\mathrm{Gal}(F/\mathbb{Q})$ equals :

$$\sum_i m_i \mathrm{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} \Psi_i.$$

One has :

$$\rho = \sum_i m_i \mathrm{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} (\rho_{|G_{F_i}} \otimes \Psi_i).$$

As in the proof of proposition 1, it follows from the theorems of Taylor and Arthur-Clozel that $\rho_{|G_{F_i}}$ is the Galois representation $\rho(\pi_i)$ attached to an automorphic representation π_i of $\mathrm{GL}_2(\mathbb{A}_{F_i})$ whose coefficient field is embedded in E.

Let ι be an embedding of E in $\overline{\mathbb{Q}_q}$ for a prime q. We enlarge E such that it contains the values of the characters Ψ_i. One defines the virtual representation R_ι in the Grothendieck group of irreducible representations of $G_{\mathbb{Q}}$ with coefficients in $\overline{\mathbb{Q}_q}$ by :

$$R_\iota = \sum_i m_i \mathrm{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} (\rho(\pi_i)_\iota \otimes \Psi_i).$$

Let us prove that R_ι is a true representation. For i and j, let $\{\tau_k\}$, $\tau_k \in G_{\mathbb{Q}}$ be a set of representatives of the double classes $G_{F_i} \backslash G_{\mathbb{Q}} / G_{F_j}$. Let us call F_{ijk} the compositum of F_i and $\tau_k(F_j)$. One has :

$$\mathrm{Ind}_{G_{F_j}}^{G_{\mathbb{Q}}} (\rho(\pi_j)_\iota \otimes \Psi_j)_{|G_{F_i}} = \sum_k \mathrm{Ind}_{G_{F_{ijk}}}^{G_{F_i}} \left(((\rho(\pi_j)_\iota \otimes \Psi_j) \circ \mathrm{int}(\tau_k^{-1}))_{|G_{F_{ijk}}} \right).$$

It follows that the scalar product $< R_\iota, R_\iota >$ in the Grothendieck group is equal to the sum over i, j, k of :

$$m_i m_j \ < \left((\rho(\pi_j)_\iota \otimes \Psi_j) \circ \mathrm{int}(\tau_k^{-1})\right)_{|G_{F_{ijk}}}, (\rho(\pi_i)_\iota \otimes \Psi_i)_{|G_{F_{ijk}}} > .$$

We see that the scalar product of R_ι with itself is $\sum_{i,j,k} m_i m_j t_{ijk}$ with $t_{ijk} = 1$ or 0 depending whether

$$\left((\rho(\pi_j)_\iota \otimes \Psi_j) \circ \mathrm{int}(\tau_k^{-1})\right)_{|G_{F_{ijk}}} \simeq (\rho(\pi_i)_\iota \otimes \Psi_i)_{|G_{F_{ijk}}}$$

or not. One has a similar calculation for the scalar product of ρ with itself in the Grothendieck group of irreducible representations of $G_{\mathbb{Q}}$ with coefficients in $\overline{\mathbb{Q}_p}$. The calculation gives $\sum_{ijk} m_i m_j t'_{ijk}$, with $t'_{ijk} = 1$ or 0 depending whether

$$\left((\rho \otimes \Psi_j) \circ \mathrm{int}(\tau_k^{-1})\right)_{|G_{F_{ijk}}} \simeq (\rho \otimes \Psi_i)_{|G_{F_{ijk}}}$$

or not. As $\rho(\pi_i)_\iota$ and $\rho_{|G_{F_i}}$ are irreducible and have the same characteristic polynomial of Frobenius outside a finite set of primes, one has $t_{ijk} = t'_{ijk}$. As $< \rho, \rho >= 1$, it follows that the scalar product of R_ι with itself is 1. As the dimensions of R_ι and ρ are both $\sum 2m_i[G_{\mathbb{Q}} : G_{F_i}]$, we have $\dim(R_\iota) = 2$. We see that R_ι is a true representation of dimension 2. We call it ρ_ι.

It follows from the formula defining R_ι that the restriction of ρ_ι to G_F is associated to π. By Blasius-Rogawski ([4]), $(\rho_\iota)_{|G_F}$ comes from a motive, except perhaps if $k = 2$. It then follows by Tsuji that the restriction of ρ_ι to the decomposition group for the characteristic q of ι is potentially semi-stable of weight k ([28]). The case $k = 2$ and ρ_ι is constructed as a limit of q-adic representations attached to automorphic forms with one local component discrete series is taken care by Kisin ([23],[15]).

The F-semisimple representation of the Weil-Deligne group WD_ℓ on ρ_ι is isomorphic to :

$$\sum_i m_i \left(\sum_{\mathcal{L}} \mathrm{Ind}_{D_{\mathcal{L}}}^{D_\ell} (r_{\mathcal{L}}(\pi_i) \otimes \Psi_i) \right),$$

where $\mathcal{L}$ describes the set of primes of F_i over ℓ. The compatibility follows from the fact that $\pi_i \mapsto \rho(\pi_i)$ is compatibility with local Langlands correspondance (see the references quoted in the proof of proposition 1).

By an argument of Ribet, it follows from compatibility that ρ_ι is absolutely irreducible ([17]). As the restriction of ρ_ι to G_F is associated to π, it is odd and ρ_ι is odd. This finishes the proof of the theorem.

Remarks.

1) Let M be a finite extension of $\mathbb{Q}_p$ contained in $\overline{\mathbb{Q}_p}$ and let $\gamma : G_M \to \mathrm{GL}_d(E)$ be a potentially semistable representation of the Galois group G_M with coefficients in a finite extension E of $\mathbb{Q}_p$. Let WD_M be the Weil-Deligne group. Let M_0 be the maximal unramified extension of $\mathbb{Q}_p$ contained in M. Fontaine has defined a representation of WD_M on the filtered Dieudonné D module attached to γ (exp. 8 of [1]). Let us recall how it defines, up to conjugacy, a representation r of WD_M in $\mathrm{GL}_d(\overline{\mathbb{Q}_p})$. The filtered Dieudonné module D is a $L \otimes_{\mathbb{Q}_p} E$-module D, L a finite unramified extension of M_0 in $\overline{\mathbb{Q}_p}$, with an action of WD_M commuting with the action of $L \otimes_{\mathbb{Q}_p} E$. One knows that the $E \otimes_{\mathbb{Q}_p} L$-module D is free. Let us briefly recall why. Let us choose such an embedding of E in $\overline{\mathbb{Q}_p}$, and let us call $E_1 = E \cap L$. For each element τ of the Galois group of $E_1/\mathbb{Q}_p$, let D_τ be the sub-module of the elements x of D such that $(e \otimes 1)x = (1 \otimes \tau(e))x$ for every $e \in E_1$. As the Frobenius ϕ of D acts semi-linearly relatively to the action of L and commutes with the action of E, ϕ transitively permutes the D_τ, and the D_τ have the same dimension. This implies the freeness. As the action of the Weil-Deligne group WD_M on D commutes with the action of $E \otimes_{\mathbb{Q}_p} L$, it follows that WD_M acts on each D_τ. One defines r as the F-simplification of the action of WD_M on D_{id}.

2) One can describe the projective representation associated to ρ_ι as in [29]. Let F and π as in Taylor's theorem. Let ρ_ι the Galois-representation associated to π and ι. The multiplicity one theorem ([16]) implies that for $\sigma \in G_{\mathbb{Q}}$, the automorphic representations π and ${}^\sigma\pi$ are isomorphic. It follows that the Galois representations ρ_ι and $\rho_\iota \circ \mathrm{int}(\sigma)$ are isomorphic. That means that there exists $\overline{g_\sigma} \in \mathrm{PGL}_2(\overline{\mathbb{Q}}_q)$ such that :

$$\rho_\iota \circ \mathrm{int}(\sigma) \simeq \mathrm{int}(\overline{g_\sigma}) \circ \rho_\iota.$$

This characterizes $\overline{g_\sigma}$ as $\rho_{F,q}$ is absolutely irreducible. Then, $\sigma \mapsto g_\sigma$ defines a projective representation which is the projective representation associated to ρ_ι. As in [29], one can show directly that this projective representation lifts to a representation in $\mathrm{GL}_2(\overline{\mathbb{Q}}_q)$.

References

[1] *Périodes p-adiques.* Société Mathématique de France, Paris, 1994. Papers from the seminar held in Bures-sur-Yvette, 1988, Astérisque No. 223 (1994).

[2] James Arthur and Laurent Clozel. *Simple algebras, base change, and the advanced theory of the trace formula*, volume 120 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1989.

[3] Laurent Berger. Limites de représentations cristallines. Compositio Mathematica, 140 (6), 2004, 1473–1498.

[4] Don Blasius and Jonathan D. Rogawski. Motives for Hilbert modular forms. *Invent. Math.*, 114(1):55–87, 1993.

[5] Christophe Breuil. Une remarque sur les représentations locales p-adiques et les congruences entre formes modulaires de Hilbert. *Bull. Soc. Math. France*, 127(3):459–472, 1999.

[6] Christophe Breuil and Ariane Mézard, Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbf{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ en $l = p$. Duke Mathematical Journal, 115 (2), 205–310, 2002.

[7] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[8] Deligne, P. Les constantes des équations fonctionnelles des fonctions L. Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, 1972) : 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin 1973.

[9] Luis V. Dieulefait. Existence of families of Galois representations and new cases of the Fontaine-Mazur conjecture. *J. Reine Angew. Math.*, 577:147–151, 2004.

[10] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 41–78. Internat. Press, Cambridge, MA, 1995.

[11] C Khare and J.-P Wintenberger. On Serre's reciprocity conjecture for 2-dimensional mod p representations of the Galois group $G_{\mathbb{Q}}$. *arXiv math.NT/0412076*, 2004.

[12] C Khare and J.-P Wintenberger. Serre's modularity conjecture : the odd conductor case (1). Preprint 2006.

[13] C Khare and J.-P Wintenberger. Serre's modularity conjecture : the odd conductor case (2). Preprint 2006.

[14] Chandrashekhar Khare. Serre's modularity conjecture : The level one case. *Duke Mathematical Journal*, 134 (3) : 557–589, 2006.

[15] Mark Kisin. Potentially semi-stable deformation rings. Preprint 2006.

[16] I. I. Piatetski-Shapiro. Multiplicity one theorems. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, pages 209–212. Amer. Math. Soc., Providence, R.I., 1979.

[17] Kenneth A.Ribet. Galois representations attached to eigenforms with Nebentypus. Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976. 17–51. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

[18] J. D. Rogawski and J. B. Tunnell. On Artin L-functions associated to Hilbert modular forms of weight one. Inventiones Mathematicae, 74, 1983, 1, 1–42.

[19] Takeshi Saito. Hilbert modular forms and p-adic hodge theory. *Preprint.*

[20] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de Gal$(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Mathematical Journal, 54, 1987, 1, 179–230.

[21] Goro Shimura. The special values of the zeta functions associated with Hilbert modular forms. Duke Mathematical Journal, 45, 1978, 3, 637–679.

[22] C. M. Skinner and A. J. Wiles. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.*, (89):5–126 (2000), 1999.

[23] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[24] Richard Taylor. On Galois representations associated to Hilbert modular forms. II. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 185–191. Internat. Press, Cambridge, MA, 1995.

[25] Richard Taylor. On the meromorphic continuation of degree two L-functions. *Preprint*, pages 1–53, 2001.

[26] Richard Taylor. Remarks on a conjecture of Fontaine and Mazur. *J. Inst. Math. Jussieu*, 1(1):125–143, 2002.

[27] Richard Taylor. Galois representations. *Ann. Fac. Sci. Toulouse Math. (6)*, 13(1):73–119, 2004.

[28] Takeshi Tsuji. p-adic Hodge theory in the semi-stable reduction case, Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998). Documenta Mathematica, 1998, Extra Vol. II, 207–216.

[29] J.-P Wintenberger. Sur les représentations p-adiques géométriques de conducteur 1 et de dimension 2 de $g_{\mathbb{Q}}$. *arXiv math.NT/0406576*, 2004.

Jean-Pierre Wintenberger
Université Louis Pasteur
Département de Mathématiques
IRMA
7, rue René Descartes
67084 Strasbourg Cedex
France
wintenb@math.u-strasbg.fr