Topics Surrounding
the Anabelian Geometry of Hyperbolic Curves

Shinichi Mochizuki

July 2000

Contents:

Section 0: Introduction

In this manuscript, we give an exposition of various ideas and results related to the fundamental results of [Tama1-2], [Mzk1-2] concerning *Grothendieck's Conjecture of Anabelian Geometry* (which we refer to as the "Grothendieck Conjecture" for short; cf. [Mzk2], Introduction, for a brief introduction to this conjecture). Many of these ideas existed prior to the publication of [Tama1-2], [Mzk1-2], but were not

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

discussed in these papers because of their rather elementary nature and secondary importance (by comparison to the main results of these papers). Nevertheless, it is the hope of the author that the reader will find the present manuscript useful as a supplement to [Tama1-2], [Mzk1-2]. In particular, we hope that *the discussion of the present manuscript will serve to clarify the meaning and motivation behind the main result of [Mzk2].*

Our main results are the following:

(1) In §1, we take the reverse point of view to the usual one (i.e., that the Grothendieck Conjecture should be regarded as a sort of (anabelian) Tate Conjecture) and show that in a certain case, *the Tate Conjecture may be regarded as a sort of Grothendieck Conjecture* (cf. Theorem 1.1, Corollary 1.2). In particular, Corollary 1.2 is interesting in that *it allows one to express the fundamental phenomenon involved in the Tate and Grothendieck Conjectures using elementary language that can, in principle, be understood even by high school students* (cf. the Introduction to §1; the Remarks following Corollary 1.2).

(2) In §2, we show how the main result of [Mzk2] gives rise to a purely *algebro-geometric* corollary (i.e., one which has nothing to do with Galois groups, arithmetic considerations, etc.) in characteristic 0 (cf. Corollary 2.1). Moreover, we give a partial generalization of this result to positive characteristic (cf. Theorem 2.2).

(3) In §3, we discuss *real analogues of anabelian geometry*. Not surprisingly, the real case is substantially easier than the case where the base field is p-adic or a number field. Thus, we are able to prove much stronger results in the real case than in the p-adic or number field cases (cf. Theorem 3.6, Corollaries 3.7, 3.8, 3.10, 3.11, 3.13, 3.14, 3.15). In particular, we are able to prove various *real analogues of the so-called Section Conjecture of anabelian geometry* (which has not been proven, at the time of writing, for any varieties over p-adic or number fields) — cf. [Groth], p. 289, (2); [NTM], §1.2, (GC3), for a discussion of the Section Conjecture. Also, we note that the real case is interesting relative to the *analogy* between the differential geometry that occurs in the real case and certain aspects of the p-adic case (cf. [Mzk4], Introduction, §0.10; the Introduction to §3 of the present manuscript). It was this analogy that led the author to the proof of the main result of [Mzk2].

(4) In §4, we show that a certain *isomorphism version* (cf. Theorem 4.12) of the main result of [Mzk2] can be proven over *"generalized sub-p-adic fields"* (cf. Definition 4.11), which form a somewhat larger class of fields than the class of "sub-p-adic fields" dealt with in [Mzk2]. This result is interesting in that it is *reminiscent of the main results of [Tama2], as well as of the rigidity theorem of Mostow-Prasad for hyperbolic manifolds of real dimension* 3 (cf. the Remarks following the proof of Theorem 4.12).

Although we believe the results of §4 to be essentially new, we make no claim of essential originality relative to the results of §1, 2, 3, which may be proven using well-known standard techniques. Nevertheless, we believe that it is likely that, even with respect to §1, 2, 3, *the point of view of the discussion is likely to be new* (and of interest relative to understanding the main result of [Mzk2]).

Finally, before beginning our exposition, *we pause to review the main result of [Mzk2]* (which is the central result to which the ideas of the present manuscript are related). To do this, we must introduce some notation. Let Σ be a nonempty set of *prime numbers*. If K is a field, then let us denote its *absolute Galois group* $\mathrm{Gal}(\overline{K}/K)$ (where $\overline{K}$ is some algebraic closure of K) by Γ_K. If X is a geometrically connected K-scheme, then let us recall that its algebraic fundamental group $\pi_1(X)$ (for some choice of base-point) fits into a natural exact sequence

$$1 \to \pi_1(X \otimes_K \overline{K}) \to \pi(X) \to \Gamma_K \to 1$$

Let us denote by Δ_X the *maximal pro-Σ quotient of* $\pi_1(X \otimes_K \overline{K})$ (i.e., the inverse limit of those finite quotients whose orders are products of primes contained in Σ). The profinite group Δ_X is often referred to as the *(pro-Σ) geometric fundamental group* of X. Note that since the kernel of $\pi_1(X \otimes_K \overline{K}) \to \Delta_X$ is a *characteristic subgroup* of $\pi_1(X \otimes_K \overline{K})$, it follows that it is normal *inside* $\pi_1(X)$. Denote the quotient of $\pi_1(X)$ by this normal subgroup by Π_X. The profinite group Π_X is often referred to as the *(pro-Σ) arithmetic fundamental group* of X. (When it is necessary to specify the set of primes Σ, we will write Δ_X^Σ, Π_X^Σ.) Thus, we have a natural exact sequence

$$1 \to \Delta_X \to \Pi_X \to \Gamma_K \to 1$$

In [Mzk2], the author proved the following result:

Theorem A. *Let K be a* **sub-p-adic field** *(i.e., a field isomorphic to a subfield of a finitely generated field extension of $\mathbf{Q}_p$), where $p \in \Sigma$. Let X_K be a smooth variety over K, and Y_K a hyperbolic curve over K. Let $\mathrm{Hom}_K^{\mathrm{dom}}(X_K, Y_K)$ be the set of dominant K-morphisms from X_K to Y_K. Let $\mathrm{Hom}_{\Gamma_K}^{\mathrm{open}}(\Pi_X, \Pi_Y)$ be the set of open, continuous group homomorphisms $\Pi_X \to \Pi_Y$ over Γ_K, considered up to composition with an inner automorphism arising from Δ_Y. Then the natural map*

$$\mathrm{Hom}_K^{\mathrm{dom}}(X_K, Y_K) \to \mathrm{Hom}_{\Gamma_K}^{\mathrm{open}}(\Pi_X, \Pi_Y)$$

is bijective.

Remark. Theorem A as stated above is a formal consequence of "Theorem A" of [Mzk2]. In [Mzk2], only the cases of $\Sigma = \{p\}$, and Σ equal to the set of all prime numbers are discussed, but it is easy to see that the case of arbitrary Σ containing p may be derived from the case $\Sigma = \{p\}$ by precisely the same argument as that used in [Mzk2] (cf. [Mzk2], the Remark following Theorem 16.5) to derive the case of Σ equal to the set of all prime numbers from the case of $\Sigma = \{p\}$.

Acknowledgements: The author would like to thank A. Tamagawa and T. Tsuji for stimulating discussions of the various topics presented in this manuscript. Also, the author greatly appreciates the advice given to him by Y. Ihara (orally) concerning the Remark following Corollary 1.2, and by M. Seppala and C. McMullen (by email) concerning the Teichmüller theory used in §3.

Section 1: The Tate Conjecture as a Sort of Grothendieck Conjecture

In this §, we attempt to present what might be referred to as the most fundamental "prototype result" among the family of results (including the Tate and Grothendieck Conjectures) that states that maps between varieties are "essentially equivalent" to maps between arithmetic fundamental groups. The result given below, especially in the form Corollary 1.2, is interesting in that *it allows one to express the fundamental phenomenon involved using elementary language that can, in principle, be understood even by high school students* (cf. the Remark following Corollary 1.2). In particular, it does not require a knowledge of the notion of a Galois group or any another advanced notions, hence provides a convincing example of how advanced mathematics can be applied to prove results which can be stated in simple terms. Also, it may be useful for explaining to mathematicians in other fields (who may not be familiar with Galois groups or other notions used in arithmetic geometry) *the essence of the Tate and Grothendieck Conjectures.* Another interesting feature of Corollary 2.1 is that *it shows how the Tate conjecture may be thought of as being of the "same genre" as the Grothendieck Conjecture in that it expresses how the isomorphic class of a curve (in this case, an elliptic curve) may be recovered from Galois-theoretic information.*

§1.1. The Tate Conjecture for non-CM Elliptic Curves

Let K be a *number field* (i.e., a finite extension of $\mathbf{Q}$). If E is an *elliptic curve* over K, and N is a natural number, then let us write

$$K(E[N])$$

for the minimal finite extension field of K over which all of the *N-torsion points are defined.* Note that the extension $K(E[N])$ will always be *Galois.* Then we have the following elementary consequence of the "Tate Conjecture for abelian varieties over number fields" proven in [Falt]:

Theorem 1.1. *Let K be a number field. Let E_1 and E_2 be elliptic curves over K such that neither E_1 nor E_2 admits complex multiplication over $\overline{\mathbf{Q}}$. Then E_1 and*

E_2 are isomorphic as elliptic curves over K if and only if $K(E_1[N]) = K(E_2[N])$ for all natural numbers N.

Remark. Note that the expression "$K(E_1[N]) = K(E_2[N])$" is to be understood to mean "equal as subfields of some fixed algebraic closure of K." Moreover, the substance of this expression is independent of the choice of algebraic closure precisely because both fields in question are *Galois* extensions of K.

Proof. If $E_1 \cong E_2$ over K, then it is clear that $K(E_1[N]) = K(E_2[N])$ for all natural numbers N. Thus, let us assume that $K(E_1[N]) = K(E_2[N])$ for all natural numbers N, and prove that $E_1 \cong E_2$ over K. In this proof, we use the notation and results of §1.2 below. Since we assume that $K(E_1[N]) = K(E_2[N])$, let us denote this field by $K[N]$. Also, if p is a prime number, then let us write $K[p^\infty]$ for the union of the $K[p^n]$, as n ranges over the positive integers. Finally, for $n \geq 0$, we denote the Galois group $\mathrm{Gal}(K[p^\infty]/K[p^n])$ by $\Gamma[p^n]$; the center of $\Gamma[p^n]$ by $Z\Gamma[p^n]$; and the quotient $\Gamma[p^n]/Z\Gamma[p^n]$ by $P\Gamma[p^n]$.

Let p be a prime number. Then by the semisimplicity of the Tate module, together with the Tate conjecture (both proven in general in [Falt]; cf. also [Ser2], IV), the fact that neither E_1 nor E_2 admits complex multiplication over $\overline{\mathbf{Q}}$ implies that there exists an integer $n \geq 1$ such that the Galois representation on the p-power torsion points of E_1 (respectively, E_2) induces an *isomorphism* $\beta_1 : \Gamma[p^n] \cong GL_2^{[n]}(\mathbf{Z}_p)$ (respectively, $\beta_2 : \Gamma[p^n] \cong GL_2^{[n]}(\mathbf{Z}_p)$), where $GL_2^{[n]}(\mathbf{Z}_p) \subseteq GL_2(\mathbf{Z}_p)$ is the subgroup of matrices that are $\equiv 1$ modulo p^n. Since the kernel of $GL_2^{[n]}(\mathbf{Z}_p) \to PGL_2^{[n]}(\mathbf{Z}_p)$ is easily seen to be equal to the center of $GL_2^{[n]}(\mathbf{Z}_p)$, it thus follows that β_1, β_2 induce isomorphisms

$$\alpha_1 : P\Gamma[p^n] \cong PGL_2^{[n]}(\mathbf{Z}_p); \quad \alpha_2 : P\Gamma[p^n] \cong PGL_2^{[n]}(\mathbf{Z}_p)$$

Thus, in particular, by Lemma 1.3 of §1.2 below, we obtain that (after possibly increasing n) the automorphism $\alpha \stackrel{\mathrm{def}}{=} \alpha_1 \circ \alpha_2^{-1}$ of $PGL_2^{[n]}(\mathbf{Z}_p)$ is defined by conjugation by an element of $PGL_2(\mathbf{Z}_p)$. In particular, we obtain that there exists a $\mathbf{Z}_p$-linear isomorphism

$$\psi : T_p(E_1) \cong T_p(E_2)$$

between the p-adic Tate modules of E_1 and E_2 with the property that for $\sigma \in \Gamma[p^n]$, we have $\psi(\sigma(t)) = \lambda_\sigma \sigma(\psi(t))$ ($\forall t \in T_p(E_1)$), for some $\lambda_\sigma \in {\mathbf{Z}_p}^\times$ which is independent of t. On the other hand, since the determinant of ψ is clearly compatible with the Galois actions on both sides (given by the cyclotomic character), it thus follows (by taking determinants of both sides of the equation $\psi(\sigma(t)) = \lambda_\sigma \sigma(\psi(t))$) that $\lambda_\sigma^2 = 1$. Since the correspondence $\sigma \mapsto \lambda_\sigma$ is clearly a homomorphism (hence a character of order 2), we thus obtain that:

> (*) There exists a finite extension K' of K over which the $\mathrm{Gal}(\overline{K}/K')$-modules $T_p(E_1)$ and $T_p(E_2)$ become isomorphic.

(Here, K' is the extension of $K[p^n]$ (of degree ≤ 2) defined by the kernel of $\sigma \mapsto \lambda_\sigma$.) Thus, by the Tate Conjecture proven in [Falt], we obtain that $\mathrm{Hom}_{K'}(E_1, E_2) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ contains an element that induces an isomorphism on p-adic Tate modules. On the other hand, since $H_{K'} \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{K'}(E_1, E_2)$ (the module of homomorphisms $(E_1)_{K'} \to (E_2)_{K'}$ over K') is a finitely generated free $\mathbf{Z}$-module of rank ≤ 1 (since E_1, E_2 do not have complex multiplication over $\overline{\mathbf{Q}}$), we thus obtain that $H_{K'}$ is a free $\mathbf{Z}$-module of rank 1. Let $\epsilon \in H_{K'}$ be a generator of $H_{K'}$. Then ϵ necessarily corresponds to an isogeny $E_1 \to E_2$ that induces an isomorphism on p-power torsion points.

Now write $H_{\overline{K}} \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\overline{K}}(E_1, E_2)$. Then the above argument shows that $H_{\overline{K}}$ is a free $\mathbf{Z}$-module of rank 1 with a generator ϵ that induces an isomorphism on p-power torsion points for every prime number p. But this implies that $\epsilon : (E_1)_{\overline{K}} \to (E_2)_{\overline{K}}$ is an *isomorphism*, i.e., that E_1 and E_2 become *isomorphic over* $\overline{K}$.

Thus, it remains to check that E_1 and E_2 are, in fact, isomorphic over K. Let $p \geq 5$ be a prime number which is sufficiently large that: (i) K is absolutely unramified at p; (ii) the Galois representations on the p-power torsion points of E_1 and E_2 induce isomorphisms

$$\beta_1 : \Gamma[p^0] \cong GL_2(\mathbf{Z}_p); \quad \beta_2 : \Gamma[p^0] \cong GL_2(\mathbf{Z}_p)$$

(the existence of such p follows from the "modulo l versions" (for large l) of the semisimplicity of the Tate module, together with the Tate conjecture in [Mord], VIII, §5 ; cf. also [Ser2], IV). Now we would like to consider the extent to which the automorphism $\beta \stackrel{\mathrm{def}}{=} \beta_1 \circ \beta_2^{-1}$ of $GL_2(\mathbf{Z}_p)$ is defined by conjugation by an element of $GL_2(\mathbf{Z}_p)$. Note that by what we did above, we know that the morphism induced by β on $PGL_2^{[n]}(\mathbf{Z}_p)$ (for some large n) is given by conjugation by some element $A \in GL_2(\mathbf{Z}_p)$. Let $\gamma : GL_2(\mathbf{Z}_p) \to GL_2(\mathbf{Z}_p)$ be the automorphism of $GL_2(\mathbf{Z}_p)$ obtained by composing β with the automorphism given by conjugation by A^{-1}. Thus, γ induces the identity on $PGL_2^{[n]}(\mathbf{Z}_p)$. But this implies (by Lemma 1.4 below) that γ induces the identity on $PGL_2(\mathbf{Z}_p)$. In particular, it follows that there exists a homomorphism $\lambda : GL_2(\mathbf{Z}_p) \to {\mathbf{Z}_p}^\times$ such that $\gamma(\sigma) = \lambda(\sigma) \cdot \sigma$ $(\forall \sigma \in GL_2(\mathbf{Z}_p))$. Next, let us recall that since $p \geq 5$, the topological group $SL_2(\mathbf{Z}_p)$ has *no abelian quotients* (an easy exercise). Thus, λ factors through the determinant map $GL_2(\mathbf{Z}_p) \to {\mathbf{Z}_p}^\times$. Moreover, (cf. the argument at the beginning of the proof involving arbitrary p) since the composites of β_1, β_2 with the determinant map are given by the cyclotomic character, we obtain that $\lambda^2 = 1$. In particular, we obtain that λ is trivial on the index 2 subgroup of $GL_2(\mathbf{Z}_p)$ of elements whose determinant is a square. Put another way, if we write K_p for the quadratic extension of K determined by composing the cyclotomic character $\mathrm{Gal}(\overline{K}/K) \to {\mathbf{Z}_p}^\times$ (which is surjective since K is absolutely unramified at p) with the unique surjection ${\mathbf{Z}_p}^\times \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$, then over K_p, the Tate modules $T_p(E_1)$, $T_p(E_2)$ become isomorphic as Galois modules, which implies that $\mathrm{Hom}_{K_p}(E_1, E_2) \neq 0$. But this implies that E_1 and E_2 become isomorphic over K_p.

On the other hand, for distinct primes p, p' as above, K_p, $K_{p'}$ form *linearly disjoint quadratic extensions* of K (as can be seen by considering the ramification at p, p'). Thus, the fact that both $\mathrm{Gal}(\overline{K}/K_p)$ and $\mathrm{Gal}(\overline{K}/K_{p'})$ act trivially on $\mathrm{Hom}_{\overline{K}}(E_1, E_2)$ implies that $\mathrm{Gal}(\overline{K}/K)$ acts trivially on $\mathrm{Hom}_{\overline{K}}(E_1, E_2)$, so $E_1 \cong E_2$ over K, as desired. ○

Remark. The above proof benefited from discussions with A. Tamagawa and T. Tsuji.

Corollary 1.2. *There is a finite set $\Sigma \subseteq \mathbf{Z}$ such that if E_1 and E_2 are arbitrary elliptic curves over $\mathbf{Q}$ whose j-invariants $j(E_1)$, $j(E_2)$ do not belong to Σ, then E_1 and E_2 are isomorphic as elliptic curves over $\mathbf{Q}$ if and only if $\mathbf{Q}(E_1[N]) = \mathbf{Q}(E_2[N])$ for all natural numbers N.*

Proof. In light of Theorem 1.1, it suffices to show that there are only finitely many possibilities (all of which are integral — cf., e.g., [Shi], p. 108, Theorem 4.4) for the j-invariant of an elliptic curve over $\mathbf{Q}$ which has complex multiplication over $\overline{\mathbf{Q}}$. But this follows from the finiteness of the number of imaginary quadratic extensions of $\mathbf{Q}$ with class number one (cf., e.g., [Stk]), together with the theory of [Shi] (cf. [Shi], p. 123, Theorem 5.7, (i), (ii)). (Note that we also use here the elementary facts that: (i) the class group of any order surjects onto the class group of the maximal order; (ii) in a given imaginary quadratic extension of $\mathbf{Q}$, there are only finitely many orders with trivial class group.) ○

Remark. According to an (apparently) unpublished manuscript of J.-P. Serre ([Ser3]) whose existence was made known to the author by Y. Ihara, the set Σ of Corollary 1.2, i.e., the list of rational j-invariants of elliptic curves with complex multiplication, is as follows:

$$d = 1, \mathfrak{f} = 1 \Longrightarrow j = j(i) = 2^6 \cdot 3^3$$
$$d = 1, \mathfrak{f} = 2 \Longrightarrow j = j(2i) = (2 \cdot 3 \cdot 11)^3$$
$$d = 2, \mathfrak{f} = 1 \Longrightarrow j = j(\sqrt{-2}) = (2^2 \cdot 5)^3, \quad \text{([Weber], p. 721)}$$
$$d = 3, \mathfrak{f} = 1 \Longrightarrow j = j(\frac{-1+\sqrt{-3}}{2}) = 0$$
$$d = 3, \mathfrak{f} = 2 \Longrightarrow j = j(\sqrt{-3}) = 2^4 \cdot 3^3 \cdot 5^3, \quad \text{([Weber], p. 721)}$$
$$d = 3, \mathfrak{f} = 3 \Longrightarrow j = j(\frac{-1+3\sqrt{-3}}{2}) = -3 \cdot 2^{15} \cdot 5^3, \quad \text{([Weber], p. 462)}$$
$$d = 7, \mathfrak{f} = 1 \Longrightarrow j = j(\frac{-1+\sqrt{-7}}{2}) = -3^3 \cdot 5^3, \quad \text{([Weber], p. 460)}$$
$$d = 7, \mathfrak{f} = 2 \Longrightarrow j = j(\sqrt{-7}) = (3 \cdot 5 \cdot 17)^3, \quad \text{([Weber], p. 475)}$$
$$d = 11, \mathfrak{f} = 1 \Longrightarrow j = j(\frac{-1+\sqrt{-11}}{2}) = -2^{15}, \quad \text{([Weber], p. 462)}$$

$$d = 19, \mathfrak{f} = 1 \Longrightarrow j = -(2^5 \cdot 3)^3, \quad \text{([Weber], p. 462)}$$
$$d = 43, \mathfrak{f} = 1 \Longrightarrow j = -(2^6 \cdot 3 \cdot 5)^3, \quad \text{([Weber], p. 462)}$$
$$d = 67, \mathfrak{f} = 1 \Longrightarrow j = -(2^5 \cdot 3 \cdot 5 \cdot 11)^3, \quad \text{([Weber], p. 462)}$$
$$d = 163, \mathfrak{f} = 1 \Longrightarrow j = -(2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29)^3, \quad \text{([Weber], p. 462)}$$

(where $\mathbf{Q}(\sqrt{-d})$ is the imaginary quadratic extension of $\mathbf{Q}$ containing the order in question, $\mathfrak{f}$ is the conductor of the order, and the reference given in parentheses is for the values of the invariants "f" and "f_1" of [Weber], which are related to the j-invariant as follows: $j = (f^{24} - 16)^3/f^{24} = (f_1^{24} + 16)^3/f_1^{24}$).

Remark. Thus, if one defines elliptic curves over $\mathbf{Q}$ using cubic equations, constructs the group law on elliptic curves by considering the intersection of the cubic with various lines, and interprets the notion of isomorphism of elliptic curves (over $\mathbf{Q}$) to mean "being defined by the same cubic equation, up to coordinate transformations," then Corollary 1.2 may be expressed as follows:

> *Except for the case of finitely many exceptional j-invariants, two elliptic curves E_1, E_2 over $\mathbf{Q}$ are isomorphic if and only if for each natural number N, the coordinates ($\in \mathbf{C}$) necessary to define the N-torsion points of E_1 generate the same subfield of $\mathbf{C}$ as the coordinates necessary to define the N-torsion points of E_2.*

(where, of course, the j-invariant is defined as a polynomial in the coefficients of the cubic). In this form, the essential phenomenon at issue in the Tate or Grothendieck Conjectures may be understood even by high school students or mathematicians unfamiliar with Galois theory.

§1.2. Some Pro-p Group Theory

Let $n \geq 1$ be an integer. In this §, let us denote by PGL_2 the algebraic group (defined over $\mathbf{Z}$) obtained by forming the quotient of GL_2 by $\mathbf{G}_m$ (where $\mathbf{G}_m \hookrightarrow GL_2$ is the standard embedding by scalars), and by

$$PGL_2^{[n]}(\mathbf{Z}_p) \subseteq PGL_2(\mathbf{Z}_p)$$

the subgroup of elements which are $\equiv 1$ modulo p^n. Let us write $pgl_2(\mathbf{Z}_p)$ for the quotient of the Lie algebra $M_2(\mathbf{Z}_p)$ (of 2 by 2 matrices with $\mathbf{Z}_p$ coefficients) by the scalars $\mathbf{Z}_p \subseteq M_2(\mathbf{Z}_p)$. Thus, $pgl_2(\mathbf{Z}_p) \subseteq pgl_2(\mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = pgl_2(\mathbf{Q}_p)$. Write $pgl_2^{[n]}(\mathbf{Z}_p) \subseteq pgl_2(\mathbf{Z}_p)$ for the submodule which is the image of matrices in $M_2(\mathbf{Z}_p)$ which are $\equiv 0$ modulo p^n. Thus, for n sufficiently large, $pgl_2^{[n]}(\mathbf{Z}_p)$ maps bijectively onto $PGL_2^{[n]}(\mathbf{Z}_p)$ via the exponential map (cf. [Ser1], Chapter V, §7).

Lemma 1.3. *Let $\alpha : PGL_2^{[n]}(\mathbf{Z}_p) \to PGL_2^{[n]}(\mathbf{Z}_p)$ be an automorphism of the profinite topological group $PGL_2^{[n]}(\mathbf{Z}_p)$ such that $\alpha(PGL_2^{[m]}(\mathbf{Z}_p)) = PGL_2^{[m]}(\mathbf{Z}_p)$ for all $m \geq n$. Then there exists an element $A \in PGL_2(\mathbf{Z}_p)$ such that for some $m \geq n$, the restriction $\alpha|_{PGL_2^{[m]}(\mathbf{Z}_p)}$ is given by conjugation by A.*

Proof. Let us write

$$\mathcal{A} : pgl_2(\mathbf{Q}_p) \to pgl_2(\mathbf{Q}_p)$$

for the morphism on Lie algebras induced by α. By [Ser1], Chapter V, §7, 9, after possibly replacing n by a larger n, we may assume that α is the homomorphism obtained by exponentiating $\mathcal{A}$. Moreover, by the well-known theory of the Lie algebra $pgl_2(\mathbf{Q}_p)$, it follows that $\mathcal{A}$ may be obtained by conjugating by some $A' \in PGL_2(\mathbf{Q}_p)$. (Indeed, this may be proven by noting that $\mathcal{A}$ induces an automorphism of the "variety of Borel subalgebras of $pgl_2(\mathbf{Q}_p)$." Since this variety is simply $\mathbf{P}^1_{\mathbf{Q}_p}$, we thus get an automorphism of $\mathbf{P}^1_{\mathbf{Q}_p}$, hence an element of $PGL_2(\mathbf{Q}_p)$, as desired.) On the other hand, it follows from immediately from the structure theory of finitely generated $\mathbf{Z}_p$-modules that A' may be written as a product

$$A' = C_1 \cdot A'' \cdot C_2$$

where $C_1, C_2 \in PGL_2(\mathbf{Z}_p)$, and A'' is defined by a matrix of the form $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, where $\lambda_1, \lambda_2 \in \mathbf{Q}_p{}^\times$.

Now observe that the fact that $\mathcal{A}$ arises from an automorphism of $PGL_2^{[n]}(\mathbf{Z}_p)$ implies that $\mathcal{A}$ induces an automorphism of $pgl_2^{[n]}(\mathbf{Z}_p)$ (cf. the discussion at the beginning of this §). Since conjugation by C_1 and C_2 clearly induces automorphisms of $pgl_2^{[n]}(\mathbf{Z}_p)$, it thus follows that conjugation by A'' induces an automorphism of $pgl_2^{[n]}(\mathbf{Z}_p)$. Now, by considering, for instance, upper triangular matrices with zeroes along the diagonal, one sees that A'' can only induce an automorphism of $pgl_2^{[n]}(\mathbf{Z}_p)$ if $\lambda_1 = \lambda_2 \cdot u$, where $u \in \mathbf{Z}_p{}^\times$. Let $A \stackrel{\text{def}}{=} \lambda_1^{-1} \cdot A'$. Then clearly $A \in PGL_2(\mathbf{Z}_p)$, and conjugation by A induces $\mathcal{A}$. Thus, by using the exponential map, we obtain that for some $m \geq n$, the restriction $\alpha|_{PGL_2^{[m]}(\mathbf{Z}_p)}$ is given by conjugation by A, as desired. ◯

The following lemma was pointed out to the author by A. Tamagawa:

Lemma 1.4. *Let $\alpha : PGL_2(\mathbf{Z}_p) \to PGL_2(\mathbf{Z}_p)$ be an automorphism of the profinite topological group $PGL_2(\mathbf{Z}_p)$ such that for some integer $m \geq 1$, the restriction $\alpha|_{PGL_2^{[m]}(\mathbf{Z}_p)}$ is the identity. Then α itself is the identity.*

Proof. Since $PGL_2(\mathbf{Z}_p)$ is generated by the image of the $PGL_2(\mathbf{Z}_p)$-conjugates of matrices of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ (where $\lambda \in \mathbf{Z}_p$), it follows that it suffices to show that α is the identity on (the image in $PGL_2(\mathbf{Z}_p)$ of) such matrices. For $m \geq 0$ an integer, write

$$G_m \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \right\} \subseteq PGL_2(\mathbf{Z}_p)$$

where $\lambda \in p^m \cdot \mathbf{Z}_p$. Since, by hypothesis, α preserves G_m for some m, it follows that α preserves the *centralizer* $Z(G_m)$ of G_m in $PGL_2(\mathbf{Z}_p)$. On the other hand, one checks easily that $Z(G_m) = G_0$. Thus, α preserves G_0, i.e., induces an automorphism of the topological group $G_0 \cong \mathbf{Z}_p$ which is the identity on $p^m \cdot \mathbf{Z}_p$. Since $\mathbf{Z}_p$ is torsion free, it thus follows that α is the identity on G_0, as desired. ◯

Section 2: Hyperbolic Curves as their own "Anabelian Albanese Varieties"

In this §, we present an application (Corollary 2.1) of the main theorem of [Mzk2] which is interesting in that it is *purely algebro-geometric*, i.e., it makes no mention of Galois actions or other arithmetic phenomena.

§2.1. A Corollary of the Main Theorem of [Mzk2]

In this §, we fix a nonempty set of *prime numbers* Σ, and use the notation of the discussion of Theorem A in the Introduction. Now Theorem A has the following immediate consequence:

Corollary 2.1. *Let K be a field of characteristic* 0*. Let C be a hyperbolic curve over K, and let $\psi : X \to Y$ be a morphism of (geometrically integral) smooth varieties over K which induces an isomorphism $\Delta_X \cong \Delta_Y$. Let us write "$\mathrm{Hom}_K^{\mathrm{dom}}(-, C)$" for the set of dominant K-morphisms from "$-$" to C. Then the natural morphism of sets*

$$\mathrm{Hom}_K^{\mathrm{dom}}(Y, C) \to \mathrm{Hom}_K^{\mathrm{dom}}(X, C)$$

induced by $\psi : X \to Y$ is a bijection.

Proof. By a standard technique involving the use of subfields of K which are finitely generated over $\mathbf{Q}$, we reduce immediately to the case where K is finitely generated over $\mathbf{Q}$. (We recall for the convenience of the reader that the essence of this technique lies in the fact that since we are working with K-schemes of finite type, all schemes and morphisms between schemes are defined by *finitely many* *polynomials* with coefficients in K, hence may be defined over any subfield of K that contains these coefficients (of which there are only finitely many!).)

Next, observe that since the morphism $\psi : X \to Y$ induces an isomorphism between the respective geometric fundamental groups, it follows from the exact sequences reviewed above that it induces an isomorphism $\Pi_X \cong \Pi_Y$. By Theorem A of the Introduction, it thus follows that the morphism of sets under consideration — i.e., $\mathrm{Hom}_K^{\mathrm{dom}}(Y, C) \to \mathrm{Hom}_K^{\mathrm{dom}}(X, C)$ — is naturally isomorphic to the morphism of sets given by

$$\mathrm{Hom}_{\Gamma_K}^{\mathrm{open}}(\Pi_Y, \Pi_C) \to \mathrm{Hom}_{\Gamma_K}^{\mathrm{open}}(\Pi_X, \Pi_C)$$

which is bijective. This completes the proof. ○

Remark. As stated above, Corollary 2.1 is interesting in that it is a *purely algebro-geometric application* of Theorem A, i.e., it makes no mention of Galois actions or other arithmetic phenomena. The observation that Corollary 2.1 holds first arose in discussions between the author and A. Tamagawa. Typical examples of morphisms $\psi : X \to Y$ as in Corollary 2.1 are:

(1) the case where $X \to Y$ is a fiber bundle in, say, the étale topology, with proper, simply connected fibers;

(2) the case where $Y \subseteq \mathbf{P}_k^n$ is a closed subvariety of dimension ≥ 3 in some projective space, and X is obtained by intersecting Y with a hyperplane in $\mathbf{P}_k^n$.

In these cases, the fact that the resulting morphism on geometric fundamental groups is an isomorphism follows from the long exact homotopy sequence of a fiber bundle in the first case (cf. [SGA1], X, Corollary 1.4), and Lefshetz-type theorems (cf. [SGA2], XII, Corollary 3.5) in the second case. Since this consequence of Theorem A (i.e., Corollary 2.1) is purely algebro-geometric, *it is natural to ask if one can give a purely algebro-geometric proof of Corollary 2.1.* In §2.2 below, we give a partial answer to this question.

§2.2. A Partial Generalization to Finite Characteristic

Let k be an *algebraically closed field.* Let C be a *proper hyperbolic curve* over k. Suppose that we are also given a *connected, smooth closed subvariety*

$$Y \subseteq \mathbf{P}_k^n$$

of projective space, of dimension ≥ 3, together with a *hyperplane* $H \subseteq \mathbf{P}_k^n$ such that the scheme-theoretic intersection $X \stackrel{\mathrm{def}}{=} H \bigcap Y$ is still smooth. Note that X is necessarily *connected* (cf. [SGA2], XII, Corollary 3.5) and of dimension ≥ 2.

If k is of *characteristic* $p > 0$, and S is a k-scheme, then let us write $\Phi_S : S \to S$ for the *Frobenius morphism* on S (given by raising regular functions on S to the power p). If k is of characteristic 0, then we make the convention that $\Phi_S : S \to S$ denotes the *identity morphism*. If T is a k-schemes, then we define

$$\mathrm{Hom}^{\Phi}(T, C)$$

to be the inductive limit of the system

$$\mathrm{Hom}_k^{\mathrm{dom}}(T, C) \to \mathrm{Hom}_k^{\mathrm{dom}}(T, C) \to \ldots \to \mathrm{Hom}_k^{\mathrm{dom}}(T, C) \to \ldots$$

where the arrows are those induced by applying the functor $\mathrm{Hom}_k^{\mathrm{dom}}(-, C)$ to the morphism Φ_T. Thus, in particular, if k is of characteristic 0, then $\mathrm{Hom}^{\Phi}(T, C) = \mathrm{Hom}_k^{\mathrm{dom}}(T, C)$.

Now we have the following partial generalization of Corollary 2.1 of §2.1 to the case of varieties over a field of arbitrary characteristic:

Theorem 2.2. *Let k, C, X, and Y be as above. Then the natural morphism*

$$\mathrm{Hom}^{\Phi}(Y, C) \to \mathrm{Hom}^{\Phi}(X, C)$$

induced by the inclusion $X \hookrightarrow Y$ is a bijection.

Proof. Let us denote by A_X, A_Y, and A_C the *Albanese varieties* of X, Y, and C, respectively. We refer to [Lang], Chapter II, §3, for basic facts concerning Albanese varieties. Thus, the inclusion $X \hookrightarrow Y$ induces a morphism $A_X \to A_Y$. I *claim* that this morphism is a *purely inseparable isogeny* . Indeed, by various well-known Leftshetz theorem-type results (cf., [SGA2], XII, Corollary 3.5), the inclusion $X \hookrightarrow Y$ induces an isomorphism $\pi_1(X) \cong \pi_1(Y)$; since (by the universal property of the Albanese variety as the "minimal abelian variety to which the original variety maps") we have surjections $\pi_1(X) \twoheadrightarrow \pi_1(A_X)$, $\pi_1(Y) \twoheadrightarrow \pi_1(A_Y)$, we thus obtain that $\pi_1(A_X) \twoheadrightarrow \pi_1(A_Y)$ is a surjection. Moreover, since $X \to A_X$, $Y \to A_Y$ induce isomorphisms on the respectively étale first cohomology groups with $\mathbf{Z}_l$-coefficients (where l is prime to the characteristic of k), we thus obtain that $\pi_1(A_X) \twoheadrightarrow \pi_1(A_Y)$ is a surjection which is an isomorphism on the respective maximal pro-l quotients. It follows from the elementary theory of abelian varieties that this implies that $A_X \to A_Y$ is a purely inseparable isogeny, as desired. Note that since $A_X \to A_Y$ is an isogeny, it follows in particular that it is *faithfully flat*.

Now let $\gamma_X : X \to C$ be a *dominant k-morphism*. Write $\alpha_X : A_X \to A_C$ for the induced morphism on Albanese varieties. If γ_X arises from some $\gamma_Y : Y \to C$, then this γ_Y is *unique*. Indeed, γ_Y is determined by its associated α_Y, and the composite of α_Y with $A_X \to A_Y$ is given by α_X (which is uniquely determined by γ_X). Thus, the fact that α_Y is uniquely determined follows from the fact that

$A_X \to A_Y$ is fully faithful. This completes the proof of the claim, and hence of the injectivity portion of the bijectivity assertion in Theorem 2.2.

Now suppose that γ_X is *arbitrary* (i.e., does not necessarily arise from some γ_Y). The surjectivity portion of the bijectivity assertion in Theorem 2.2 amounts to showing that, up to replacing γ_X by the composite of γ_X with some power of Φ_X, γ_X necessarily arises from some $\gamma_Y : Y \to C$. Now although $\alpha_X : A_X \to A_C$ itself might not factor through A_Y, since $A_X \to A_Y$ is *purely inseparable*, it follows that the composite of α_X with some power of Φ_{A_X} will factor through A_Y. Thus, if we replace γ_X by the composite of γ_X with some power of Φ_X, then α_X will factor (uniquely) through A_Y. Let us denote this morphism by $\alpha_Y : A_Y \to A_C$. Thus, in order to complete the proof of surjectivity, it suffices to show:

(*) *The restriction $\alpha_Y|_Y$ of α_Y to Y (relative to the natural morphism $Y \to A_Y$) maps into the subvariety $C \subseteq A_C$.*

Before continuing, we observe the following:

(1) The assertion (*) for characteristic zero k follows immediately from the assertion (*) for k of finite characteristic. Indeed, this follows via the usual argument of replacing k first by a finitely generated $\mathbf{Z}$-algebra, and then reducing modulo various primes. Thus, in the following, we assume the k is of characteristic $p > 0$.

(2) The assertion (*) will follow if we can show that the restriction $\alpha_Y|_{\widehat{Y}}$ (where we write $\widehat{Y}$ for the *completion* of Y along X) maps into $C \subseteq A_C$.

Now let us show that (up to possibly composing γ_X again with a power of Frobenius), γ_X *extends to* $\widehat{Y}$. If $\mathcal{I}$ is the sheaf of ideals on Y that defines the closed subscheme $X \subseteq Y$, then let us write $Y_n \stackrel{\text{def}}{=} V(\mathcal{I}^n) \subseteq Y$ for the *n-th infinitesimal neighborhood of X in Y*, and $\mathcal{J} \stackrel{\text{def}}{=} \mathcal{I}|_X \cong \mathcal{O}_X(-1)$. Write $\mathcal{T}$ for the pull-back of the tangent bundle of C to X via γ_X. Since $\mathcal{T}^{-1}$ is generated by global sections, it thus follows that $\mathcal{T}^{-1} \otimes \mathcal{J}^{-1}$ is *ample*, hence, by *Serre duality* (cf., e.g., [Harts], Chapter III, Theorem 7.6), together with the fact that $\dim(X) \geq 2$, that there exists a natural number N such that

$$H^1(X, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes p^N}) = 0$$

Note that this implies that for all $n \geq p^N$, we have:

$$H^1(X, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n}) = 0$$

(Indeed, it suffices to assume that $n > p^N$. Then since $\mathcal{J}^{-1} \cong \mathcal{O}_X(1)$ is *very ample*, it follows that there exists a section $s \in \Gamma(X, \mathcal{O}_X(1))$ whose zero locus $Z \stackrel{\text{def}}{=} V(s) \subseteq X$ is smooth of dimension ≥ 1. Thus, s defines an exact sequence

$$0 \to \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n} \to \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1} \to \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1}|_Z \to 0$$

whose associated long exact cohomology sequence yields:

$$H^0(Z, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1}|_Z) \to H^1(X, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n}) \to H^1(X, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1})$$

But $H^0(Z, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1}|_Z) = 0$ since $\mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1}|_Z$ is the inverse of an ample line bundle on a smooth scheme of dimension ≥ 1, while $H^1(X, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n-1}) = 0$ by the induction hypothesis.)

Next, observe that $\Phi^N_{Y_{p^N}} : Y_{p^N} \to Y_{p^N}$ *factors through* X (since $\Phi^N_{Y_{p^N}}$ is induced by raising functions to the p^N-th power). Thus, if we compose $\gamma_X : X \to C$ with Φ^N_X, we see that this composite extends to a morphism $Y_{p^N} \to C$. Moreover, since the pull-back to X via this composite of the tangent bundle on C is given by $\mathcal{T}^{\otimes p^N}$, it follows that the obstruction to extending this composite to Y_{n+1} for $n \geq p^N$ is given by an element of the cohomology group

$$H^1(X, \mathcal{T}^{\otimes p^N} \otimes \mathcal{J}^{\otimes n})$$

which (by the above discussion concerning cohomology groups) is zero. Thus, in summary, if we replace the given γ_X by its composite with Φ^N_X, the resulting γ_X extends to a morphism $\widehat{Y} \to C$. This completes the proof of (*), and hence of the entire proof of Theorem 2.2. ○

Remark. The above proof benefited from discussions with A. Tamagawa.

Remark. Note that the other case discussed in the Remark at the end of §2.1, i.e., the case of a fiber bundle with proper, simply connected fibers also admits a purely algebro-geometric proof: namely, it follows immediately from the theory of Albanese varieties that there do not exist any nonconstant morphisms from a simply connected smooth proper variety to an abelian variety.

Remark. The role played by the Albanese variety in the proof of Theorem 2.2 given above suggests that the property proven in Corollary 2.1 and Theorem 2.2 might be thought of as asserting that a hyperbolic curve is, so to speak, *its own "anabelian Albanese variety."* This is the reason for the title of §2.

Section 3: Discrete Real Anabelian Geometry

The original motivation for the p-adic result of [Mzk2] came from *the (differential) geometry of the upper half-plane uniformization* of a hyperbolic curve.

This point of view — and, especially, the related idea that Kähler geometry at archimedean primes should be regarded as analogous to Frobenius actions at p-adic primes — is discussed in detail in [Mzk4], Introduction (especially §0.10; cf. also the Introduction of [Mzk3]). In the present §, we attempt to make this motivation more rigorous by presenting the *real analogues of various theorems/conjectures* of anabelian geometry. The substantive mathematics here — i.e., essentially the geometry of the Siegel upper half-plane and Teichmüller space — is not new, but has been well-known to topologists, Teichmüller theorists, and symmetric domain theorists for some time. What is (perhaps) new is the formulation or point of view presented here, namely, that these geometric facts should be regarded as real analogues of Grothendieck's conjectured anabelian geometry.

§**3.1. Real Complex Manifolds**

We begin with the following purely analytic definition: Let X be a *complex manifold* and ι an *anti-holomorphic involution* (i.e., automorphism of order 2) of X.

Definition 3.1. A pair such as (X, ι) will be referred to as a *real complex manifold*. If X has the structure of an abelian variety whose origin is fixed by ι, then (X, ι) will be referred to as a *real abelian variety*. If $\dim_{\mathbf{C}}(X) = 1$, then (X, ι) will be referred to as a *real Riemann surface*. A real Riemann surface (X, ι) will be called *hyperbolic* if the universal covering space of X is isomorphic (as a Riemann surface) to the upper half-plane $\mathfrak{H} \stackrel{\mathrm{def}}{=} \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$.

Remark. Note that if $X_{\mathbf{R}}$ is a *smooth algebraic variety over* $\mathbf{R}$, then $X_{\mathbf{R}}(\mathbf{C})$ equipped with the anti-holomorphic involution defined by complex conjugation defines a *real complex manifold* (X, ι). Moreover, one checks easily that $X_{\mathbf{R}}$ is uniquely determined by (X, ι). Conversely, any real complex manifold (X, ι) such that X is *projective* arises from a unique algebraic variety $X_{\mathbf{R}}$ over $\mathbf{R}$. Indeed, this follows easily from "Chow's Theorem" (that any projective complex manifold is necessarily algebraic) and the (related) fact that any holomorphic isomorphism between projective algebraic varieties (in this case, the given X and its complex conjugate) is necessarily algebraic. Thus, in summary, one motivating reason for the introduction of Definition 3.1 is that *it allows one to describe the notion of a (proper, smooth) algebraic variety over* $\mathbf{R}$ *entirely in terms of complex manifolds and analytic maps.*

Remark. In the case of one complex dimension, one does not even need to assume projectivity: That is, any real Riemann surface (X, ι) such that X is algebraic arises from a unique algebraic curve $X_{\mathbf{R}}$ over $\mathbf{R}$. Indeed, this follows easily by observing that any holomorphic isomorphism between Riemann surfaces associated to complex algebraic curves is necessarily algebraic. (Note that this may be proven by noting that any such isomorphism extends naturally to the "one-point compactifications" of the Riemann surfaces (which have natural algebraic structures), hence is necessarily algebraizable.) It is not clear to the author whether or not this can be generalized to higher dimensions.

In the following, we shall consider various groups G with natural augmentations $G \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$. In this sort of situation, we shall denote the inverse image of the identity element (respectively, the complex conjugation element) in $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ by G^+ (respectively, G^-).

If X is a *complex manifold*, then we shall denote by

$$\mathrm{Aut}(X) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$$

the group of automorphisms of X which are *either holomorphic or anti-holomorphic*, equipped with its natural augmentation (which sends holomorphic (respectively, anti-holomorphic) automorphisms to the identity (respectively, complex conjugation element) in $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$). Thus,

$$\mathrm{Aut}^+(X), \mathrm{Aut}^-(X) \subseteq \mathrm{Aut}(X)$$

denote the subsets of holomorphic and anti-holomorphic automorphisms, respectively. In many cases, X will come equipped with a *natural Riemannian metric which is preserved by* $\mathrm{Aut}(X)$. The principal examples of this situation are the following:

Example 3.2. (The Siegel Upper Half-Plane) Let $g \geq 1$ be an integer. Let us write

$$\mathfrak{H}_g \stackrel{\mathrm{def}}{=} \{Z \in M_g(\mathbf{C}) \mid Z = {}^tZ; \mathrm{Im}(Z) > 0\}$$

(where "^{t}" denotes the "transpose matrix," and "> 0" is to be understood to mean "positive definite") for the *Siegel upper half-plane.* (Thus, $\mathfrak{H}_1$ is the usual upper half-plane $\mathfrak{H}$.) We shall regard $\mathfrak{H}_g$ as a *complex manifold* (equipped with the obvious complex structure). Set $J_g \stackrel{\mathrm{def}}{=} \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \in M_{2g}(\mathbf{R})$ (where $I_g \in M_g(\mathbf{R})$ is the identity matrix). Write

$$GSp_{2g} \stackrel{\mathrm{def}}{=} \{M \in M_{2g}(\mathbf{R}) \mid M \cdot J \cdot {}^tM = \eta \cdot J,\ \eta \in \mathbf{R}^\times\}$$

for the group of *symplectic similitudes.* Thus, we have a natural character

$$\chi : GSp_{2g} \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$$

that maps an $M \in GSp_{2g}$ to the sign of η (where η is as in the above definition of GSp_{2g}). In particular, χ defines GSp_{2g}^+, GSp_{2g}^-. Then we have a natural homomorphism

$$\phi : GSp_{2g} \to \mathrm{Aut}(\mathfrak{H}_g)$$

given by letting $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GSp_{2g}$ act on $Z \in \mathfrak{H}_g$ by

$$Z \mapsto (AZ^{\chi(M)} + B)(CZ^{\chi(M)} + D)^{-1}$$

Thus, ϕ is compatible with the augmentations to $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. Now it is clear that the kernel of ϕ is given by the scalars $\mathbf{R}^\times \subseteq GSp_{2g}$. In fact, ϕ is *surjective*. Indeed, this is well-known when $+$'s are added to both sides (i.e., for holomorphic automorphisms — cf., e.g., [Maass], §4, Theorem 2). On the other hand, since ϕ is compatible with the augmentations to $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$, the surjectivity of ϕ thus follows from the "5-Lemma." Thus, in summary, we have a natural isomorphism

$$GSp_{2g}/\mathbf{R}^\times \cong \mathrm{Aut}(\mathfrak{H}_g)$$

Moreover, the space $\mathfrak{H}_g$ admits a natural *Riemannian metric*. Relative to this metric, any two points Z_1, Z_2 of $\mathfrak{H}_g$ can be joined by a *unique geodesic* (cf. [Maass], §3, Theorem). Moreover, this Riemannian metric is *preserved by the action of GSp_{2g} on $\mathfrak{H}_g$*. (Indeed, this follows from [Maass], §4, Theorem 1, in the holomorphic case. As for the anti-holomorphic case, it suffices to check that the metric is preserved by a single anti-holomorphic map. But this is clear from [Maass], §4, Theorem 1, for the map $Z \mapsto -\overline{Z}$.)

Example 3.3. **(Teichmüller Space)** Let $g, r \geq 0$ be integers such that $2g-2+r > 0$. Let us denote by $T_{g,r}$ the *Teichmüller space of genus g Riemann surfaces with r marked points*. Thus, $T_{g,r}$ has a natural structure of complex manifold. Moreover, $T_{g,r}$ is equipped with a natural Kähler metric, called the *Weil-Petersson metric*, whose associated Riemannian metric has the property that *any two points $t_1, t_2 \in T_{g,r}$ may be joined by a unique geodesic* (cf. [Wolp], §5.1).

Write

$$\mathrm{Mod}_{g,r}$$

for the *full modular group*, i.e., the group of homotopy classes of homeomorphisms of a topological surface of type (g, r) onto itself. Note that $\mathrm{Mod}_{g,r}$ is equipped with an augmentation $\mathrm{Mod}_{g,r} \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ given by considering whether or not the homeomorphism preserves the orientation of the surface. The quotient $T_{g,r}/\mathrm{Mod}^+_{g,r}$ (in the sense of stacks) may be identified with the moduli stack $\mathcal{M}_{g,r}$ of hyperbolic curves of type (g, r) over $\mathbf{C}$, and the Weil-Petersson metric *descends to $\mathcal{M}_{g,r}$*. Moreover, the Riemannian metric arising from the Weil-Petersson metric on $\mathcal{M}_{g,r}$ is *preserved by complex conjugation*. Indeed, this follows easily, for instance, from the definition of the Weil-Petersson metric in terms of integration of the square of the absolute value of a quadratic differential (on the Riemann surface in question) divided by the $(1,1)$-form given by the Poincaré metric (on the Riemann surface in question) — cf., e.g, [Wolp], §1.4.

If (g,r) is not *exceptional* (i.e., not equal to the cases $(0,3)$, $(0,4)$, $(1,1)$, $(1,2)$, or $(2,0)$), then it is known (by a theorem of Royden — cf., e.g., [Gard], §9.2, Theorem 2) that one has a natural isomorphism

$$\mathrm{Mod}_{g,r} \cong \mathrm{Aut}(T_{g,r})$$

which is compatible with the natural augmentations to $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. Now I claim that (at least if (g,r) is nonexceptional, then) $\mathrm{Aut}(T_{g,r})$ *preserves (the Riemannian metric arising from) the Weil-Petersson metric*. Indeed, since $T_{g,r}/\mathrm{Mod}^+_{g,r} = \mathcal{M}_{g,r}$, and the Weil-Petersson metric descends to $\mathcal{M}_{g,r}$, it thus follows that $\mathrm{Mod}^+_{g,r}$ preserves the Weil-Petersson metric. Thus, the claim follows from the fact (observed above) that (the Riemannian metric arising from) the Weil-Petersson metric on $\mathcal{M}_{g,r}$ is preserved by complex conjugation.

Now let us return to our discussion of an arbitrary *real complex manifold* (X,ι). By analogy with the case when (X,ι) arises from a real algebraic variety (cf. the Remark following Definition 3.1), we will refer to the fixed point locus of ι as the *real locus of* (X,ι), and use the notation

$$X(\mathbf{R})$$

for this locus. Observe that $X(\mathbf{R})$ is necessarily a *real analytic submanifold* of X of real dimension equal to the complex dimension of X. (Indeed, this follows immediately by considering the local structure of ι at a point $x \in X(\mathbf{R})$.) Moreover, at any $x \in X(\mathbf{R})$, the involution ι induces a *semi-linear* (i.e., with respect to complex conjugation) *automorphism* ι_x of order 2 of the complex vector space $T_x(X)$ (i.e., the tangent space to the complex manifold X at x). That is to say, ι_x defines a *real structure* $T_x(X)_{\mathbf{R}} \subseteq T_x(X)_{\mathbf{R}} \otimes_{\mathbf{R}} \mathbf{C} = T_x(X)$ on $T_x(X)$. Put another way, this real structure $T_x(X)_{\mathbf{R}}$ is simply the tangent space to the real analytic submanifold $X(\mathbf{R}) \subseteq X$.

Since ι acts *without fixed points* on $X \backslash X(\mathbf{R})$, it follows that the quotient of $X \backslash X(\mathbf{R})$ by the action of ι defines a real analytic manifold over which $X \backslash X(\mathbf{R})$ forms an unramified double cover. In the following, in order to analyze the action of ι on all of X, we would like to consider the quotient of X by the action of ι *in the sense of real analytic stacks*. Let us denote this quotient by X^ι. Thus, we have an unramified double cover

$$X \to X^\iota$$

which extends the cover discussed above over $X \backslash X(\mathbf{R})$.

The Galois group of this double cover (which is isomorphic to $\mathbf{Z}/2\mathbf{Z}$) may be identified with the Galois group $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. Thus, this double cover induces a short exact sequence of fundamental groups

$$1 \to \pi_1(X) \to \pi_1(X^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to 1$$

where we omit base-points, since they are inessential to the following discussion. (Here, by "π_1" we mean the usual (discrete) topological fundamental group in the sense of algebraic topology.)

Now write $\widetilde{X} \to X$ for the *universal covering space* of X. Thus, $\widetilde{X}$ also has a natural structure of complex manifold, and ι induces an anti-holomorphic automorphism $\widetilde{\iota}$ (not necessarily of order 2!) of $\widetilde{X}$, which is uniquely determined up to composition with the covering transformations of $\widetilde{X} \to X$. Since $\widetilde{X}$ is also the universal cover of the real analytic stack X^ι, it thus follows that by considering the covering transformations of the covering $\widetilde{X} \to X^\iota$, we get a natural homomorphism

$$\pi_1(X^\iota) \to \mathrm{Aut}(\widetilde{X})$$

which is compatible with the natural projections of both sides to $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$.

Thus, if, for instance, (X, ι) is a *hyperbolic real Riemann surface*, then by Example 3.2, there is a natural isomorphism $\mathrm{Aut}(\widetilde{X}) \cong PGL_2(\mathbf{R})$ (well-defined up to conjugation by an element of $PGL_2^+(\mathbf{R})$). Thus, we obtain a natural representation

$$\rho_X : \pi_1(X^\iota) \to PGL_2(\mathbf{R})$$

which is compatible with the natural projections of both sides to $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$.

Definition 3.4. Let (X, ι) be a hyperbolic real Riemann surface. Then the representation

$$\rho_X : \pi_1(X^\iota) \to PGL_2(\mathbf{R})$$

(which is defined up to composition with conjugation by an element of $PGL_2^+(\mathbf{R})$) just constructed will be referred to as the *canonical representation of* (X, ι).

Remark. The point of view of Definition 3.4 is discussed in [Mzk3], §1, "Real Curves," although the formulation presented there is somewhat less elegant.

§3.2. Fixed Points of Anti-Holomorphic Involutions

Let T be a (nonempty) *complex manifold* which is also equipped with a *smooth Riemannian metric*. Let us also assume that the Riemannian metric on T satisfies the following property:

(*) For any two distinct points $t_1, t_2 \in T$, there exists a unique geodesic joining t_1 and t_2.

Then we have the following result, which is fundamental to the theory of the present §3:

Lemma 3.5. *Let T be a (nonempty)* **complex manifold** *equipped with a* **smooth Riemannian metric** *satisfying the condition (*). Let $\iota_T : T \to T$ be an anti-holomorphic involution of T which preserves this Riemannian metric. Then the fixed point set $F_{\iota_T} \stackrel{\mathrm{def}}{=} \{t \in T \mid \iota_T(t) = t\}$ of ι_T is a nonempty, connected real analytic submanifold of T of real dimension equal to the complex dimension of T.*

Proof. From the discussion of §3.1, it follows that it suffices to prove that ι_T is nonempty and connected. First, we prove nonemptiness. Let $t_1 \in T$ be any point of T, and set $t_2 \stackrel{\mathrm{def}}{=} \iota_T(t_1)$. If $t_1 = t_2$, then $t_1 \in F_{\iota_T}$, so we are done. If $t_1 \neq t_2$, then let γ be the unique geodesic joining t_1, t_2. Then since the subset $\{t_1, t_2\}$ is preserved by ι_T, it follows that γ *is also preserved by* ι_T. Thus, it follows in particular that the *midpoint* t of γ is preserved by ι_T, i.e., that $t \in F_{\iota_T}$, so F_{ι_T} is nonempty as desired. Connectedness follows similarly: If $t_1, t_2 \in F_{\iota_T}$, then the unique geodesic γ joining t_1, t_2 is also clearly fixed by ι_T, i.e., $\gamma \subseteq F_{\iota_T}$, so F_{ι_T} is pathwise connected. ○

Remark. The idea for this proof (using the Weil-Petersson metric in the case of Teichmüller space) is essentially due to Wolpert ([Wolp]), and was related to the author by C. McMullen. We remark that this idea has been used to give a solution of the *Nielsen Realization Problem* (cf. the Introduction of [Wolp]). It is easiest to see what is going on by thinking about what happens in the case when $T = \mathfrak{H}$ (the upper half-plane) equipped with the *Poincaré metric* $\frac{dx^2+dy^2}{y^2}$. Also, we remark that in the case when $T = \mathbf{P}^1_{\mathbf{C}}$, both the hypothesis and the conclusion of Lemma 3.5 are *false*! (That is, the hypothesis is false because there will always exist "conjugate points," and the conclusion is false because it is easy to construct examples of anti-holomorphic involutions without fixed points.)

Now assume that (X, ι) is any *real complex manifold* equipped with a smooth Riemannian metric (i.e., X is equipped with a smooth Riemannian metric preserved by ι) such that the induced Riemannian metric on the universal cover $T \stackrel{\mathrm{def}}{=} \widetilde{X}$ satisfies (*). Let $Y \subseteq X(\mathbf{R})$ be a *connected component of the real analytic manifold* $X(\mathbf{R})$. Then since ι acts trivially on Y, the quotient of Y by the action of ι forms a real analytic stack Y^ι whose associated coarse space is Y itself, and which fits into a commutative diagram:

$$\begin{array}{ccc} Y & \longrightarrow & Y^\iota \\ \downarrow & & \downarrow \\ X & \longrightarrow & X^\iota \end{array}$$

Moreover, the mapping $Y^\iota \to Y$ (where we think of Y as the coarse space associated to the stack Y^ι) defines a splitting of the exact sequence:

$$1 \to \pi_1(Y) \to \pi_1(Y^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to 1$$

hence a homomorphism $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to \pi_1(Y^\iota)$. If we compose this homomorphism with the natural homomorphism $\pi_1(Y^\iota) \to \pi_1(X^\iota)$, then we get a morphism

$$\alpha_Y : \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to \pi_1(X^\iota)$$

naturally associated to Y, which is well-defined up to composition with an inner autormorphism of $\pi_1(X)$. In particular, the image of complex conjugation under α_Y defines a conjugacy class of *involutions* ι_Y of $\pi_1(X^\iota)$. Thus, to summarize, *we have associated to each connected component $Y \subseteq X(\mathbf{R})$ of the real locus of (X, ι) a conjugacy class of involutions ι_Y in $\pi_1(X^\iota)$.*

Now we have the following immediate consequence of Lemma 3.5:

Theorem 3.6. **("General Discrete Real Section Conjecture")** *Let (X, ι) be a* **real complex manifold** *equipped with a smooth Riemannian metric (i.e., X is equipped with a smooth Riemannian metric preserved by ι) such that the induced Riemannian metric on the universal cover $\widetilde{X}$ satisfies (*). Then the correspondence $Y \mapsto \iota_Y$ defines a bijection*

$$\pi_0(X(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1(X^\iota))$$

from the set of connected components of the real locus $X(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1(X^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, involutions in $\pi_1(X^\iota)$). Moreover, the centralizer of an involution $\iota_Y \in \pi_1(X^\iota)$ is the image of $\pi_1(Y^\iota)$ in $\pi_1(X^\iota)$.

Proof. Indeed, let $\iota_T \in \pi_1(X^\iota)$ be an involution. Then ι_T may be thought of as an anti-holomorphic involution of $T \stackrel{\mathrm{def}}{=} \widetilde{X}$. By Lemma 3.5, the fixed point locus F_{ι_T} of ι_T is nonempty and connected. Thus, F_{ι_T} maps into some connected component $Y \subseteq X(\mathbf{R})$. (In fact, the morphism $F_{\iota_T} \to Y$ is a covering map.) By *functoriality* (consider the map of triples $(T, \iota_T, F_{\iota_T}) \to (X, \iota, Y)$!), it follows that $\iota_Y = \iota_T$. Thus, every involution in $\pi_1(X^\iota)$ arises as some ι_Y. Next, let us show uniqueness. If ι_T arises from two distinct $Y_1, Y_2 \subseteq X(\mathbf{R})$, then it would follow that the fixed point locus F_{ι_T} contains at two distinct connected components (corresponding to Y_1, Y_2), thus contradicting Lemma 3.5. Finally, if $\alpha \in \pi_1(X^\iota)$ commutes with ι_Y, then α preserves F_{ι_Y}, hence induces an automorphism of F_{ι_Y} over Y^ι. But since $F_{\iota_Y} \to Y^\iota$ is a covering map, this implies that α is in the image of $\pi_1(Y^\iota)$ in $\pi_1(X^\iota)$. This completes the proof. ○

Remark. Thus, Theorem 3.6 is a sort of analogue of the so-called "Section Conjecture" of anabelian geometry for the *discrete fundamental groups of real complex manifolds* — see [Groth], p. 289, (2); [NTM], §1.2, (GC3), for more on the Section Conjecture.

§3.3. Hyperbolic Curves and their Moduli

By the discussion of Examples 3.2 (in the case of $\mathfrak{H}$), 3.3, in §3.1, together with Theorem 3.6 of §3.2, we obtain the following:

Corollary 3.7. **("Discrete Real Section Conjecture for Hyperbolic Real Riemann Surfaces")** *Let (X, ι) be a* **hyperbolic real Riemann surface***. Then the correspondence $Y \mapsto \iota_Y$ of §3.2 defines a bijection*

$$\pi_0(X(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1(X^\iota))$$

from the set of connected components of the real locus $X(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1(X^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, involutions in $\pi_1(X^\iota)$).

Corollary 3.8. **("Discrete Real Section Conjecture for Moduli of Hyperbolic Curves")** *Let $g, r \geq 0$ be integers such that $2g - 2 + r > 0$. Write $(\mathcal{M}_{g,r}, \iota_{\mathcal{M}})$ for the moduli stack of complex hyperbolic curves of type (g, r), equipped with its natural anti-holomorphic involution (arising from the structure of $\mathcal{M}_{g,r}$ as an algebraic stack defined over $\mathbf{R}$). If (X, ι) arises from a real hyperbolic curve of type (g, r), then the exact sequence*

$$1 \to \pi_1(X) \to \pi_1(X^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to 1$$

defines a homomorphism $\alpha_{(X,\iota)} : \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to \pi_1(\mathcal{M}_{g,r}^{\iota_{\mathcal{M}}}) = \mathrm{Mod}_{g,r} \subseteq \mathrm{Out}(\pi_1(X))$ (where "$\mathrm{Out}(-)$" denotes the group of outer automorphisms of the group in parentheses). This correspondence $(X, \iota) \mapsto \alpha_{(X,\iota)}$ defines a bijection

$$\pi_0(\mathcal{M}_{g,r}(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1(\mathcal{M}_{g,r}^{\iota_{\mathcal{M}}}))$$

from the set of connected components of $\mathcal{M}_{g,r}(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1(\mathcal{M}_{g,r}^{\iota_{\mathcal{M}}}) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, involutions in $\pi_1(\mathcal{M}_{g,r}^{\iota_{\mathcal{M}}})$). Moreover, the centralizer of an involution $\iota_Y \in \pi_1(\mathcal{M}_{g,r}^{\iota_{\mathcal{M}}})$ is the image of $\pi_1(Y^\iota)$ in $\pi_1(\mathcal{M}_{g,r}^{\iota_{\mathcal{M}}})$.

Remark. Note that the *injectivity portion* of the bijection of Corollary 3.8, together with the determination of the centralizer of an involution (the final sentence in the statement of Corollary 3.8), may be regarded as the discrete real analogue of the so-called "Strong Isomorphism Version of the Grothendieck Conjecture." (For the convenience of the reader, we recall that the "Strong Isomorphism Version of the Grothendieck Conjecture" is the statement of Theorem A in the Introduction, except with K-morphism (respectively, homomorphism) replaced by K-isomorphism (respectively, isomorphism).)

Remark. The author was informed by M. Seppala that results similar to Corollary 3.8 have been obtained in [AG].

§3.4. Abelian Varieties and their Moduli

We begin with a lemma:

Lemma 3.9. *Let (X, ι) be a real complex manifold such that X is an abelian variety over $\mathbf{C}$. Then there exists a translation-invariant Riemannian metric on X which is preserved by ι.*

Proof. By the Remark following Definition 3.1, (X, ι) arises from a projective algebraic variety $X_{\mathbf{R}}$ over $\mathbf{R}$. Write X^c for the complex conjugate of the complex manifold X (i.e., X^c and X have the same underlying real analytic manifold, but holomorphic functions on X^c are anti-holomorphic functions on X). Since X is an abelian variety over $\mathbf{C}$, it follows that X^c is also an abelian variety over $\mathbf{C}$. Thus, the holomorphic isomorphism $\iota : X \cong X^c$ is the composite of an isomorphism of abelian varieties (i.e., one which preserves the group structures) with a translation. In particular, it follows that ι *preserves the invariant differentials* $V \stackrel{\text{def}}{=} \Gamma(X, \Omega_X)$ *on* X. Thus, ι induces a semi-linear (with respect to complex conjugation) automorphism of V, i.e., ι induces a *real structure* $V_{\mathbf{R}} \subseteq V_{\mathbf{R}} \times_{\mathbf{R}} \mathbf{C} = V$ on V. Then any inner product on the real vector space $V_{\mathbf{R}}$ induces an ι-invariant inner product on the underlying real vector space of V which, in turn, induces a translation-invariant Riemannian metric on X which is preserved by ι, as desired. $\bigcirc$

Remark. Note that any Riemannian metric on $\widetilde{X}$ arising from a Riemannian metric as in the conclusion of Lemma 3.9 induces a geometry on $\widetilde{X}$ which is isomorphic to *Euclidean space*, hence enjoys the property that any two points are joined by a unique geodesic.

Now if we apply Theorem 3.6 using Lemma 3.9, Example 3.2, we obtain the following:

Corollary 3.10. ("Discrete Real Section Conjecture for Real Abelian Varieties") *Let (X, ι) be a* **real abelian variety**. *Then the correspondence $Y \mapsto \iota_Y$ of §3.2 defines a bijection*

$$\pi_0(X(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1(X^\iota))$$

from the set of connected components of the real locus $X(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1(X^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, involutions in $\pi_1(X^\iota)$).

Corollary 3.11. ("Discrete Real Section Conjecture for Moduli of Abelian Varieties") *Let $g \geq 1$ be a positive integer. Write $(\mathcal{A}_g, \iota_{\mathcal{A}})$ for the moduli stack of principally polarized abelian varieties of dimension g, equipped with its natural anti-holomorphic involution (arising from the structure of $\mathcal{A}_g$ as an* *algebraic stack defined over* $\mathbf{R}$*). If* (X, ι) *is a real abelian variety of dimension* g*, then the exact sequence*

$$1 \to \pi_1(X) \to \pi_1(X^\iota) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to 1$$

defines a homomorphism $\alpha_{(X,\iota)} : \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to \pi_1(\mathcal{A}_g^{\iota_\mathcal{A}}) \cong GSp(\pi_1(X))$ *(where "*GSp*" denotes the automorphisms that preserve, up to a constant multiple, the symplectic form defined by the polarization). This correspondence* $(X, \iota) \mapsto \alpha_{(X,\iota)}$ *defines a bijection*

$$\pi_0(\mathcal{A}_g(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1(\mathcal{A}_g^{\iota_\mathcal{A}}))$$

from the set of connected components of $\mathcal{A}_g(\mathbf{R})$ *to the set of conjugacy classes of sections of* $\pi_1(\mathcal{A}_g^{\iota_\mathcal{A}}) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ *(or, equivalently, involutions in* $\pi_1(\mathcal{A}_g^{\iota_\mathcal{A}})$*). Moreover, the centralizer of an involution* $\iota_Y \in \pi_1(\mathcal{A}_g^{\iota_\mathcal{A}})$ *is the image of* $\pi_1(Y^\iota)$ *in* $\pi_1(\mathcal{A}_g^{\iota_\mathcal{A}})$*.*

Proof. Note that the bijectivity of the natural morphism

$$\pi_1(\mathcal{A}_g^{\iota_\mathcal{A}}) \to GSp(\pi_1(X))$$

follows from the fact that it is compatible with the projections on both sides to $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (where the projection $GSp(\pi_1(X)) \to \mathbf{Z}^\times = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ is given by looking at the constant multiple to which the symplectic form arising from the polarization is mapped), together with the well-known bijectivity of this morphism on the "+" portions to both sides. ◯

§3.5. Profinite Real Anabelian Geometry

So far we have considered the real analogue of Grothendieck's anabelian geometry given by using the *discrete* fundamental groups of varieties. Another "real analogue" of anabelian geometry is that given by using the *profinite* fundamental groups. Just as in the discrete, the fundamental result was an existence theorem for real points in the presence of involutions (i.e., Lemma 3.5), *in the profinite case, the fundamental existence is given by the following theorem of Cox* (cf. [Frdl], Corollary 11.3):

Lemma 3.12. *Let* X *be a connected real algebraic variety. Then* $X(\mathbf{R}) \neq \emptyset$ *if and only if* $H^i_{\mathrm{et}}(X, \mathbf{Z}/2\mathbf{Z}) \neq 0$ *(where "*H^i_{et}*" denotes étale cohomology) for infinitely many* i*.*

Remark. In particular, if the complex manifold $X(\mathbf{C})$ is a "$K(\pi, 1)$" space (i.e., its universal cover is contractible), and, moreover, its fundamental group $\pi_1(X(\mathbf{C}))$ is *good* (i.e., the cohomology of $\pi_1(X(\mathbf{C}))$ with coefficients in any finite $\pi_1(X(\mathbf{C}))$-module is isomorphic (via the natural morphism) to the cohomology of the profinite completion of $\pi_1(X(\mathbf{C}))$ with coefficients in that module), then we obtain that:

> (*) $X(\mathbf{R}) \neq \emptyset$ if and only if $H^i_{\mathrm{et}}(\pi_1^{\mathrm{alg}}(X), \mathbf{Z}/2\mathbf{Z}) \neq 0$ for infinitely many integers i.

(where $\pi_1^{\mathrm{alg}}(X)$ denotes the algebraic fundamental group of the scheme X). Also, let us observe that if the projection $\pi_1^{\mathrm{alg}}(X) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ possesses a splitting, then the fact that $H^i_{\mathrm{et}}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \mathbf{Z}/2\mathbf{Z}) \neq 0$ for infinitely many i implies that $H^i_{\mathrm{et}}(\pi_1^{\mathrm{alg}}(X), \mathbf{Z}/2\mathbf{Z}) \neq 0$ for infinitely many i.

Since hyperbolic curves and abelian varieties satisfy the conditions of the above Remark, we thus obtain the following:

Corollary 3.13. **("Profinite Real Section Conjecture for Real Hyperbolic Curves")** *Let X be a* **hyperbolic curve** *over $\mathbf{R}$. Then the profinite version of the correspondence $Y \mapsto \iota_Y$ of §3.2 defines a bijection*

$$\pi_0(X(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1^{\mathrm{alg}}(X))$$

from the set of connected components of the real locus $X(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1^{\mathrm{alg}}(X) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, involutions in $\pi_1^{\mathrm{alg}}(X)$).

Proof. *Surjectivity* follows from the above Remark, using the technique of [Tama1]: Namely, given a section $\alpha : \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to \pi_1^{\mathrm{alg}}(X)$ of $\pi_1^{\mathrm{alg}}(X) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$, the family of open subgroups of $\pi_1^{\mathrm{alg}}(X)$ containing $\mathrm{Im}(\alpha)$ defines a system of coverings $\{X_i \to X\}$ (as i varies over the elements of some index set I) such that (by the above Remark) each $X_i(\mathbf{R}) \neq 0$. Since each $X_i(\mathbf{R})$ has only finitely many connected components, it thus follows that there exists a compatible system (indexed by I) of connected components of $X_i(\mathbf{R})$. But this amounts to the assertion that α arises from some connected component of $X(\mathbf{R})$, as desired (cf. [Tama1], Corollary 2.10).

Injectivity follows from the fact that involutions arising from distinct connected components define distinct elements of $H^1(\pi_1^{\mathrm{alg}}(X), \mathbf{Z}/2\mathbf{Z})$ — cf. [Schd], §20, Propositions 20.1.8, 20.1.12. ○

Remark. To the author's knowledge, the first announcement in the literature of a result such as Corollary 3.13 (in the proper case) appears in a manuscript of Huisman ([Huis]). (In fact, [Huis] also treats the one-dimensional case of Corollary 3.14 below.) Unfortunately, however, the author was not able to follow the portion of Huisman's proof ([Huis], Lemma 5.7) that corresponds to the application of Cox's theorem (as in the Remark following Lemma 3.12).

Corollary 3.14. ("Profinite Real Section Conjecture for Real Abelian Varieties") *Let X be an* **abelian variety** *over* $\mathbf{R}$. *Then the profinite version of the correspondence $Y \mapsto \iota_Y$ of §3.2 defines a bijection*

$$\pi_0(X(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1^{\mathrm{alg}}(X))$$

from the set of connected components of the real locus $X(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1^{\mathrm{alg}}(X) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, involutions in $\pi_1^{\mathrm{alg}}(X)$).

Proof. *Surjectivity* follows as in the proof of Corollary 3.13. *Injectivity* follows, for instance, from the discrete result (Corollary 3.10), together with the injectivity of the natural morphism

$$H^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1(X(\mathbf{C}))) \to H^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1^{\mathrm{alg}}(X \otimes_{\mathbf{R}} \mathbf{C}))$$

— itself a consequence of the fact that $\pi_1^{\mathrm{alg}}(X \otimes_{\mathbf{R}} \mathbf{C})) = \pi_1(X(\mathbf{C})) \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$, where $\widehat{\mathbf{Z}}$ is the profinite completion of $\mathbf{Z}$ (hence a faithfully flat $\mathbf{Z}$-module). ○

As for the case of moduli, the above argument breaks down in most cases since it is either false that or unknown whether or not the fundamental group of the corresponding moduli stacks is *good*. More precisely, $\pi_1(\mathcal{A}_g) = Sp(2g, \mathbf{Z})$ is known *not to be good* if $g \geq 2$ (cf. Lemma 3.16 below). (If $g = 1$, then the "profinite real section conjecture" for $\mathcal{A}_g$ is essentially contained in Corollary 3.13 above.) On the other hand, to the author's knowledge, *it is not known whether or not $\pi_1(\mathcal{M}_{g,r})$ is good* if $g > 2$. If $g \leq 2$, then, up to passing to finite étale coverings, $\mathcal{M}_{g,r}$ may be written as a successive extension of smooth families of hyperbolic curves, hence has a good fundamental group. Thus, we obtain the following:

Corollary 3.15. ("Profinite Real Section Conjecture for Moduli of Hyperbolic Curves of Genus ≤ 2") *Let $g, r \geq 0$ be integers such that $2g-2+r > 0$, $g \leq 2$. Write $(\mathcal{M}_{g,r})_{\mathbf{R}}$ for the moduli stack of complex hyperbolic curves of type (g, r) over $\mathbf{R}$. If X is a real hyperbolic curve of type (g, r), then X defines a section $\alpha_{(X,\iota)} : \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \to \pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}})$. This correspondence $(X, \iota) \mapsto \alpha_{(X,\iota)}$ defines a bijection*

$$\pi_0((\mathcal{M}_{g,r})_{\mathbf{R}}(\mathbf{R})) \cong \mathrm{Hom}_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}}))$$

from the set of connected components of $(\mathcal{M}_{g,r})_{\mathbf{R}}(\mathbf{R})$ to the set of conjugacy classes of sections of $\pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}}) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ (or, equivalently, conjugacy classes of involutions in $\pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}})$). Moreover, the centralizer of an involution $\iota_Y \in \pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}})$ is the image of the profinite completion of $\pi_1(Y^\iota)$ in $\pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}})$.

Proof. Since (as just remarked) the fundamental groups involved are *good*, *surjectivity* follows as in Corollaries 3.13, 3.14.

As for *injectivity*, we reason as follows. Given two real hyperbolic curves X, Y of the same type (g,r) which induce the same section α (up to conjugacy) of $\pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}}) \to \mathrm{Gal}(\mathbf{C}/\mathbf{R})$, we must show that they belong to the same connected component of $(\mathcal{M}_{g,r})_{\mathbf{R}}(\mathbf{R})$. First, let us observe that since $[\mathbf{C} : \mathbf{R}] = 2$, it follows that the marked points of X and Y over $\mathbf{C}$ consist of: (i.) points defined over $\mathbf{R}$; (ii) complex conjugate pairs. Moreover, the combinatorial data of which points are defined over $\mathbf{R}$ and which points are conjugate pairs is clearly determined by the section α. Thus, there exists an "ordering of connected components of the divisor of marked points over $\mathbf{R}$" of X, Y, which is compatible with α. Write

$$\mathcal{N} \to (\mathcal{M}_{g,r})_{\mathbf{R}}$$

for the finite étale covering defined by the moduli stack (over $\mathbf{R}$) of hyperbolic curves equipped with such an ordering. Then $\mathcal{N}$ may be written as a *"successive extension"*

$$\mathcal{N} = \mathcal{N}_r \to \mathcal{N}_{r-1} \to \ldots \to \mathcal{N}_1 \to \mathcal{N}_0$$

of smooth families (i.e., the $\mathcal{N}_{j+1} \to \mathcal{N}_j$) of either *hyperbolic curves* (where we include curves which are stacks — cf. the remark in parentheses following the list below) or *surfaces* (of a special type, to be described below) *over the stack* $\mathcal{N}_0$, where $\mathcal{N}_0$ may be described as follows:

(1) If $g = 0$, then $\mathcal{N}_0$ is the moduli stack of 4-pointed curves of genus 0, equipped with an "ordering type" $\mathcal{T}$, where $\mathcal{T}$ is one of the following: a total ordering of the four points; a total ordering of two points, plus a pair of conjugate points; a total ordering of two pairs of conjugate points. In each of these three cases, one sees that $\mathcal{N}_0$ is a *hyperbolic curve* over $\mathbf{R}$, so we conclude injectivity from Corollary 3.13.

(2) If $g = 1$, then $\mathcal{N}_0$ is either the moduli stack of 1-pointed curves of genus 1 (which is a hyperbolic curve, so we may conclude injectivity from Corollary 3.13), or $\mathcal{N}_0$ is the moduli stack of 2-pointed curves of genus 1, where the two points are unordered. In this case, by considering the "group of automorphisms of the underlying genus 1 curve which preserve the invariant differentials," we get a morphism $\mathcal{N}_0 \to (\mathcal{M}_{1,1})_{\mathbf{R}}$, which is a smooth family whose fiber over the elliptic curve E is the stack given by forming the quotient of $E \backslash \{0_E\}$ (where 0_E is the origin of E) by the action of ± 1. (Indeed, this fiber parametrizes the "difference" of the two unordered points.) In particular, $(\mathcal{M}_{1,1})_{\mathbf{R}}$, as well as these fibers over $(\mathcal{M}_{1,1})_{\mathbf{R}}$ are hyperbolic curves, so injectivity follows from Corollary 3.13.

(3) If $g = 2$, then $\mathcal{N}_0$ is the moduli stack of 0-pointed curves of genus 2. Moreover, by using the well-known morphism $(\mathcal{M}_{2,0})_{\mathbf{R}} \to (\mathcal{M}_{0,6})_{\mathbf{R}}$ (given by considering the ramification points of the canonical double covering of the projective line associated to a curve of genus 2), this case may be reduced to the case $g = 0$, which has already been dealt with.

(We remark here that even though some of the hyperbolic curves appearing above are in fact stacks, by passing to appropriate finite étale coverings which are still defined over $\mathbf{R}$ and for which the real points in question lift to real points of the covering, injectivity for such "stack-curves" follows from injectivity for usual curves as proven in Corollary 3.13.) Finally, the surfaces that may appear as fibers in the families $\mathcal{N}_{j+1} \to \mathcal{N}_j$ appearing above are of the following type: If C is a hyperbolic curve over $\mathbf{R}$, write $\Delta_C \subseteq C \times_{\mathbf{R}} C$ for the diagonal. Then the surfaces in question are of the form $\{(C \times_{\mathbf{R}} C)\backslash\Delta_C\}/\mathfrak{S}_2$ (where $\mathfrak{S}_2$ is the symmetric group on two letters permuting the two factors of C, and we note that this quotient is the same whether taken in the sense of schemes or of stacks). Now by passing (as in the one-dimensional case) to appropriate finite étale coverings of these surfaces which are still defined over $\mathbf{R}$ and for which the real points in question lift to real points of the covering, injectivity for such surfaces follows from injectivity for surfaces that may be written as a smooth family of hyperbolic curves parametrized by a hyperbolic curve, hence is a consequence of Corollary 3.13. This completes the proof of *injectivity*.

Before proceeding, we *observe* that the above argument shows that the bijectivity assertion of Corollary 3.15 also holds for any finite étale covering of $\mathcal{M}_{g,r}$ which is defined over $\mathbf{R}$.

The final statement on centralizers may be proven as follows: Given an involution ι_Y, write $\mathcal{M}_Y \to (\mathcal{M}_{g,r})_{\mathbf{R}}$ for the pro-covering defined by the subgroup generated by ι_Y in $\pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}})$. Then the statement on centralizers follows from the fact that the conjugates of ι_Y in $\pi_1^{\mathrm{alg}}((\mathcal{M}_{g,r})_{\mathbf{R}})$ are in bijective correspondence with the connected components of the inverse images of Y in $\mathcal{M}_Y$ (where we note that this bijective correspondence follows from the observation of the preceding paragraph). $\bigcirc$

Remark. Note that in many respects the profinite theory is more difficult and less elegant than the discrete theory, where everything follows easily from the very general Lemma 3.5. It is thus the feeling of the author that *the discrete theory provides a more natural real analogue of anabelian geometry than the profinite theory.*

Lemma 3.16. *Let $g \geq 2$, and let $H \subseteq Sp(2g, \mathbf{Z})$ be a subgroup of finite index. Then there exists a subgroup $H' \subseteq H$ which is normal and of finite index in $Sp(2g, \mathbf{Z})$ such that the cohomological dimension of the profinite completion of H' is $> \dim_{\mathbf{R}}(\mathcal{A}_g) = g(g+1)$. (This estimate holds even if one restricts to H'-modules of order equal to a power of p, for any fixed prime number p.) In particular, if $g \geq 2$, then $Sp(2g, \mathbf{Z})$ is* **not good**.

Proof. First, note that if $Sp(2g, \mathbf{Z})$ is good, then so is any subgroup H of finite index. But there exist H such that if we write $\mathcal{A}_{H'} \to \mathcal{A}_g$ for the finite étale covering defined by a finite index subgroup $H' \subseteq H$, then $\mathcal{A}_{H'}$ is a *complex manifold* (i.e., not just a stack). The cohomology of H' is then given by the cohomology of $\mathcal{A}_{H'}$. Moreover, the cohomological dimension of $\mathcal{A}_{H'}$ is $= \dim_{\mathbf{R}}(\mathcal{A}_{H'}) = \dim_{\mathbf{R}}(\mathcal{A}_g)$. Thus, if the cohomological dimension of the profinite completion of H' is $> \dim_{\mathbf{R}}(\mathcal{A}_g)$, it follows that the cohomology of H' and of its profinite completion (with coefficients in a finite module) are not isomorphic in general, i.e., that H' is not good. But this implies that $Sp(2g, \mathbf{Z})$ is not good, as desired.

Next, let us assume that we are given H as in the statement of Lemma 3.16, and prove the existence of an H' as stated. First, let us observe that since the *congruence subgroup problem* has been resolved affirmatively for $Sp(2g, \mathbf{Z})$ (cf. [BMS]), it follows that:

$$Sp(2g, \mathbf{Z})^{\wedge} = Sp(2g, \widehat{\mathbf{Z}}) = \prod_p Sp(2g, \mathbf{Z}_p)$$

(where the "$\wedge$" denotes the profinite completion, and the product is taken over all prime numbers p). Thus, it follows that the cohomological dimension of $Sp(2g, \mathbf{Z})^{\wedge}$ is $\geq$ the cohomological dimension of $Sp(2g, \mathbf{Z}_p)$ for any prime p. In particular, in order to complete the proof of Lemma 3.16, *it suffices to show that $Sp(2g, \mathbf{Z}_p)$ admits a collection of arbitrarily small normal open subgroups whose p-cohomological dimension is $> g(g+1)$.*

But this follows from the theory of [Laz]: Indeed, by [Laz], V, §2.2.8, it follows that that the p-cohomological dimension of any "p-valuable group" is equal to the "rank" r of the group. Here, a *p-valuable group* (cf. [Laz], III, §2.1.2) is a topogical group with a filtration satisfying certain properties. In the present context, the topological group $Sp^{[n]}(2g, \mathbf{Z}_p)$ (i.e., symplectic matrices which are $\equiv$ to the identity matrix modulo p^n), equipped with the filtration defined by the $Sp^{[m]}(2g, \mathbf{Z}_p)$ for $m \geq n$, will satisfy these properties. Moreover, the *rank* r of a p-valuable group (cf. [Laz], III, §2.1.1, §2.1.3) is the $\mathbf{Q}_p$-dimension of the Lie algebra $sp(2g, \mathbf{Q}_p)$ of $Sp(2g, \mathbf{Z}_p)$. Thus, in this case,

$$r = \dim_{\mathbf{Q}_p}(sp(2g, \mathbf{Q}_p)) = \dim_{\mathbf{R}}(sp(2g, \mathbf{R})) = \dim_{\mathbf{R}}(Sp(2g, \mathbf{R})) > \dim_{\mathbf{R}}(\mathfrak{H}_g) = \dim_{\mathbf{R}}(\mathcal{A}_g)$$

(where $\mathfrak{H}_g$ is the *Siegel upper half-plane* — cf. Example 3.2). Indeed, the inequality here follows from the fact that $Sp(2g, \mathbf{R})$ acts *transitively* on $\mathfrak{H}_g$, with *positive dimensional* isotropy subgroups. This completes the proof. ○

Section 4: Complements to the p-adic Theory

In this §, we present certain complements to the p-adic theory of [Mzk2] which allow us to prove a certain *isomorphism version* of Theorem A of [Mzk2] (cf. §0 of the present manuscript) over a somewhat larger class of fields K than was treated in [Mzk2]. This larger class of fields — which we refer to as *generalized sub-p-adic* — consists of those fields which may be embedded as subfields of a finitely generated extension of the quotient field of $W(\overline{\mathbf{F}}_p)$ (the ring of Witt vectors with coefficients in the algebraic closure of $\mathbf{F}_p$, for some prime number p).

§4.1. Good Chern Classes

In this §, we work over a base field K, which we assume (for simplicity, although it is not absolutely necessary for much of what we shall do) to be *of characteristic* 0. Let X_K be a *smooth, geometrically connected variety* over K.

If p is a prime number, and $n \geq 1$ an integer, then we may consider the *Kummer sequence on* X_K, i.e., the exact sequence of sheaves on $(X_K)_{\mathrm{et}}$ (i.e., the étale site of X_K) given by

$$0 \to (\mathbf{Z}/p^n\mathbf{Z})(1) \to \mathbf{G}_m \to \mathbf{G}_m \to 0$$

(where, the "(1)" is a "Tate twist," and the morphism from $\mathbf{G}_m$ to $\mathbf{G}_m$ is given by raising to the p^n-th power.) The connecting morphism induced on étale cohomology by the Kummer sequence then gives us a morphism

$$\delta_{p,n} : H^1_{\mathrm{et}}(X_K, \mathbf{G}_m) \to H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$$

Now suppose that $\mathcal{L}$ is a *line bundle on* X_K. Then applying $\delta_{p,n}$ to $\mathcal{L} \in H^1_{\mathrm{et}}(X_K, \mathbf{G}_m)$ gives us a compatible system of classes $\delta_{p,n}(\mathcal{L}) \in H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$, hence (by letting p, n vary) a class $c_1(\mathcal{L}) \in H^2_{\mathrm{et}}(X_K, \widehat{\mathbf{Z}}(1))$.

Definition 4.1. We shall refer to $c_1(\mathcal{L}) \in H^2_{\mathrm{et}}(X_K, \widehat{\mathbf{Z}}(1))$ as the *(profinite, étale-theoretic) first Chern class of* $\mathcal{L}$. If $N \geq 1$ is an integer, then we shall refer to $c_1(\mathcal{L})$ mod $N \in H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/N\mathbf{Z})(1))$ as the *(étale-theoretic) first Chern class of* $\mathcal{L}$ *modulo* N.

Next, let us write

$$\pi_1(X_K)$$

for the *(algebraic) fundamental group* of X_K (where we omit the base-point since it will not be explicitly necessary in our discussion). Also, let us assume that we are given a *quotient*

$$\pi_1(X_K) \twoheadrightarrow Q$$

(where Q is profinite, and the surjection is continuous) such that the natural surjection $\pi_1(X_K) \twoheadrightarrow \Gamma_K$ *factors through* Q. Then we make the following *crucial definition*:

Definition 4.2. Let $N \geq 1$ be an integer. For $i, j \in \mathbf{Z}$, a cohomology class $\eta \in H^i_{\mathrm{et}}(X_K, (\mathbf{Z}/N\mathbf{Z})(j))$ will be called *good* if there exists a (nonempty) finite étale covering $Y \to X_K$ such that $\eta|_Y \in H^i_{\mathrm{et}}(Y, (\mathbf{Z}/N\mathbf{Z})(j))$ is zero. We shall say that η is *Q-good* if this covering $Y \to X_K$ may be chosen to arise from a quotient of $\pi_1(X_K)$ that factors through $\pi_1(X_K) \twoheadrightarrow Q$. If $\mathcal{L}$ is a line bundle on X_K, then we will say that *its Chern class is good (respectively, Q-good) modulo N* if the Chern class of $\mathcal{L}$ modulo N in $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/N\mathbf{Z})(1))$ is good (respectively, Q-good).

Recall that a discrete group Γ is said to be *good* if the cohomology of Γ with coefficients in any finite Γ-module is isomorphic (via the natural morphism) to the cohomology of the profinite completion of Γ with coefficients in that module. Then the justification for the terminology of Definition 4.2 is the following:

Lemma 4.3. *Suppose that K is a subfield of $\mathbf{C}$ (the complex number field); that the topological space $\mathcal{X} \stackrel{\mathrm{def}}{=} X_{\mathbf{C}}(\mathbf{C})$ is a "$K(\pi, 1)$" space (i.e., its universal cover is contractible); and that the topological fundamental group $\pi_1^{\mathrm{top}}(\mathcal{X})$ is good. Then it follows that all cohomology classes $\eta \in H^i_{\mathrm{et}}(X_K, (\mathbf{Z}/N\mathbf{Z})(j))$ are good.*

Proof. Write $X_{\mathbf{C}} \stackrel{\mathrm{def}}{=} X_K \otimes_K \mathbf{C}$, $X_{\overline{K}} \stackrel{\mathrm{def}}{=} X_K \otimes_K \overline{K}$. Since finite étale coverings of $X_{\mathbf{C}}$ are always defined over a finite extension of K, and (by well-known elementary properties of étale cohomology) the natural morphism $H^i_{\mathrm{et}}(X_{\overline{K}}, (\mathbf{Z}/N\mathbf{Z})(j)) \to H^i_{\mathrm{et}}(X_{\mathbf{C}}, (\mathbf{Z}/N\mathbf{Z})(j))$ is an isomorphism, one sees immediately that it suffices to prove Lemma 4.3 when $K = \mathbf{C}$, $j = 0$. But then

$$H^i_{\mathrm{et}}(X_{\mathbf{C}}, \mathbf{Z}/N\mathbf{Z}) \cong H^i_{\mathrm{sing}}(X_{\mathbf{C}}, \mathbf{Z}/N\mathbf{Z}) \cong H^i(\pi_1^{\mathrm{top}}(\mathcal{X}), \mathbf{Z}/N\mathbf{Z})$$

(where the second isomorphism (between singular and group cohomology) follows from the fact that $\mathcal{X}$ is a "$K(\pi, 1)$" space). Thus, the fact that η vanishes upon restriction to a (nonempty) finite étale covering follows from the fact that $\pi_1^{\mathrm{top}}(\mathcal{X})$ is assumed to be good. ○

Remark. Thus, under the hypotheses of Lemma 4.3, *every* cohomology class is good. In general, however, we would like to work with varieties X_K that do *not* satisfy the hypotheses of Lemma 4.3, but which nonetheless have the property that *the cohomology classes that we are interested in are good.*

Now let $\mathcal{L}$ be a *line bundle* on X_K. Let us write $\mathbf{L} \to X_K$ for the *geometric line bundle* associated to $\mathcal{L}$ (i.e., the spectrum over X_K of the symmetric algebra over $\mathcal{O}_{X_K}$ of $\mathcal{L}^{-1}$). Also, let us write

$$\mathbf{L}^{\times} \subseteq \mathbf{L} \to X_K$$

for the *complement of the zero section* in $\mathbf{L}$. Thus, $\mathbf{L}^{\times} \to X_K$ is a $\mathbf{G}_m$*-torsor*, and we have an *exact sequence* of (algebraic) fundamental groups

$$\widehat{\mathbf{Z}}(1) = \pi_1((\mathbf{G}_m)_{\overline{K}}) \to \pi_1(\mathbf{L}^\times) \to \pi_1(X_K) \to 1$$

(where we omit base-points since they will not be explicitly necessary in our discussion). In general, however, it is *not necessarily the case* that the first arrow is injective. (Consider, for instance, the line bundle $\mathcal{O}(-1)$ on $\mathbf{P}^1$ (over, say, an algebraically closed K), in which case $\mathbf{L}^\times = \mathbf{A}^2\backslash\{0\}$ has trivial fundamental group.)

Lemma 4.4. *Suppose that the Chern class of $\mathcal{L}$ is* **good** *modulo all powers of p. Then the restriction to $\mathbf{Z}_p(1) \subseteq \widehat{\mathbf{Z}}(1)$ of the morphism $\widehat{\mathbf{Z}}(1) \to \pi_1(\mathbf{L}^\times)$ is* **injective***, so the above exact sequence defines an extension class $\in H^2(\pi_1(X_K), \mathbf{Z}_p(1))$. If, moreover, the Chern class of $\mathcal{L}$ is Q-***good** *modulo all powers of p, then (for all integers $n \geq 1$) the reduction modulo p^n of this extension class arises from an element $\in H^2(Q, (\mathbf{Z}/p^n\mathbf{Z})(1))$.*

Proof. Indeed, let

$$Y \to X_K$$

be a finite étale covering such that the Chern class of $\mathcal{L}$ modulo p^n vanishes upon restriction to Y. Going back to the definition of the Chern class using the Kummer exact sequence, one thus sees that there exists a line bundle $\mathcal{P}$ on Y such that $\mathcal{P}^{\otimes p^n} \cong \mathcal{L}|_Y$. Let us write $\mathbf{P}^\times \to Y$ for the complement of the zero section in the geometric line bundle corresponding to $\mathcal{P}$. Thus, $\mathbf{P}^\times \to Y$ is a $\mathbf{G}_m$-torsor with the property that, if we execute the change of structure group $\mathbf{G}_m \to \mathbf{G}_m$ given by raising to the p^n-th power, we obtain the $\mathbf{G}_m$-torsor $\mathbf{L}^\times|_Y \stackrel{\mathrm{def}}{=} \mathbf{L}^\times \times_{X_K} Y \to Y$. In particular, we obtain a finite étale covering

$$\mathbf{P}^\times \to \mathbf{L}^\times|_Y$$

whose restriction to the geometric fibers of $\mathbf{L}^\times|_Y \to Y$ is (isomorphic to) the covering of $\mathbf{G}_m$ given by raising to the p^n-th power. Sorting through the definitions of the various fundamental groups involved, one thus sees that the existence of such coverings implies that $\mathbf{Z}_p(1) \to \pi_1(\mathbf{L}^\times)$ is injective, and, moreover, that if the covering $Y \to X_K$ arises from a quotient of Q, then the extension class $\in H^2(\pi_1(X_K), (\mathbf{Z}/p^n\mathbf{Z})(1))$ defined by $\pi_1(\mathbf{L}^\times)$ arises from a class $\in H^2(Q, (\mathbf{Z}/p^n\mathbf{Z})(1))$, as desired. Note that here we use that the natural surjection $\pi_1(X_K) \twoheadrightarrow \Gamma_K$ *factors through* Q in order to conclude that the "$\pi_1(X_K)$-module $\widehat{\mathbf{Z}}(1)$" arises from a "Q-module $\widehat{\mathbf{Z}}(1)$." $\bigcirc$

Remark. In the Q-good portion of Lemma 4.4, it was necessary to use finite coefficients $\mathbf{Z}/p^n\mathbf{Z}$ (i.e., rather than $\mathbf{Z}_p$) since it is not clear that the various group extensions of Q by $(\mathbf{Z}/p^n\mathbf{Z})(1)$ form a *compatible* system as n varies. (When

$Q = \pi_1(X_K)$, one need not worry about this since one already has a natural group extension, namely, that arising from $\pi_1(\mathbf{L}^\times)$.)

Lemma 4.5. *Suppose that the Chern class of $\mathcal{L}$ is* **good** *modulo all powers of p. Write*

$$c_1^{\mathrm{gp}}(\mathcal{L}) \in H^2(\pi_1(X_K), \mathbf{Z}_p(1))$$

for the extension class of Lemma 4.4. Then the image of $c_1^{\mathrm{gp}}(\mathcal{L})$ under the natural map

$$H^2(\pi_1(X_K), \mathbf{Z}_p(1)) \to H^2_{\mathrm{et}}(X_K, \mathbf{Z}_p(1))$$

is equal to the (p-adic portion of the) first Chern class $c_1(\mathcal{L})$ of Definition 4.1. If, moreover, the Chern class of $\mathcal{L}$ is **Q-good** *modulo all powers of p, then (for all integers $n \geq 1$) there exists a class $\in H^2(Q, (\mathbf{Z}/p^n\mathbf{Z})(1))$ whose image in $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ is equal to $c_1(\mathcal{L}) \bmod p^n$.*

Proof. If Γ is a *profinite group*, then let us denote by $B(\Gamma)$ the *"classifying site of Γ,"* i.e., the site defined by considering the category of finite sets with continuous Γ-action (and coverings given by surjections of such sets). Thus, if M is a finite abelian group with continuous Γ-action, then M defines a sheaf of abelian groups on this site whose cohomology may be identified with the usual group cohomology of Γ with coefficients in M.

Next, let us note that relative to this notation, there is a *tautological morphism*

$$(X_K)_{\mathrm{et}} \to B(\pi_1(X_K))$$

determined by the well-known equivalence between finite étale coverings of X_K and finite sets with continuous $\pi_1(X_K)$-action. Put another way, this morphism is the étale analogue of the well-known tautological morphism (determined up to homotopy equivalence) in topology from a topological space to the classifying space of its fundamental group. By functoriality, we thus obtain a commutative diagram:

$$\begin{array}{ccc} (\mathbf{L}^\times)_{\mathrm{et}} & \longrightarrow & B(\pi_1(\mathbf{L}^\times)) \\ \downarrow & & \downarrow \\ (X_K)_{\mathrm{et}} & \longrightarrow & B(\pi_1(X_K)) \end{array}$$

(where the horizontal morphisms are the tautological morphisms just discussed, and the vertical morphisms are those induced by functoriality from $\mathbf{L}^\times \to X_K$).

Next, let us observe that both vertical morphisms of the above commutative diagram give rise to *Leray-Serre spectral sequences* on cohomology with coefficients in $\mathbf{Z}_p(1)$. (Here, we note that the fact that the vertical morphism on the right gives rise to such a spectral sequence follows from the injectivity assertion of Lemma 4.4.) In particular, if we consider the differential on the "E_2-term" of these spectral sequences we obtain a commutative diagram:

$$\begin{array}{ccc}
\mathbf{Z}_p = H^0(\pi_1(X_K), H^1(\mathbf{Z}_p(1), \mathbf{Z}_p(1))) & \longrightarrow & \mathbf{Z}_p = H^0_{\text{et}}(X_K, H^1_{\text{et}}((\mathbf{G}_m)_{\overline{K}}, \mathbf{Z}_p(1))) \\
\downarrow & & \downarrow \\
H^2(\pi_1(X_K), \mathbf{Z}_p(1)) & \longrightarrow & H^2_{\text{et}}(X_K, \mathbf{Z}_p(1))
\end{array}$$

(where the vertical morphisms are the differentials of the spectral sequence, and the horizontal morphisms are induced by the morphisms of sites just discussed). On the other hand, sorting through the definitions, one sees that it is a tautology that the image of $1 \in \mathbf{Z}_p$ under the vertical morphism on the right (respectively, left) is the Chern class $c_1(\mathcal{L})$ (respectively, $c_1^{\text{gp}}(\mathcal{L})$). Thus, the assertion that the image of $c_1^{\text{gp}}(\mathcal{L})$ in $H^2_{\text{et}}(X_K, \mathbf{Z}_p(1))$ is equal to $c_1(\mathcal{L})$ follows from the commutativity of the above diagram. The corresponding assertion in the Q-good case follows by replacing $\pi_1(X_K)$, $\mathbf{Z}_p$ in the above argument by Q, $\mathbf{Z}/p^n\mathbf{Z}$, respectively, and applying the Q-good portion of Lemma 4.4. ◯

Lemma 4.6. *Suppose that X_K is equipped with a smooth, proper morphism*

$$X_K \to Z_K$$

(where Z_K is a smooth, geometrically connected variety over K) which admits a section $\sigma : Z_K \to X_K$. Also, let us assume that K may be embedded as a subfield of $\mathbf{C}$, and that if $\overline{z}$ is any geometric point of Z_K such that $k(\overline{z})$ may be embedded as a subfield of $\mathbf{C}$, then the geometric fiber $X_{\overline{z}} \stackrel{\text{def}}{=} X_K \times_{Z_K} \overline{z}$ satisfies the hypotheses of Lemma 4.3 (i.e., its complex valued points form a "$K(\pi, 1)$" space with good topological fundamental group). Then the Chern class of any line bundle $\mathcal{L}$ on X_K for which the pull-back $\sigma^*(\mathcal{L})$ is trivial (as a line bundle on Z_K) is **good** *modulo all integers $N \geq 1$.*

Proof. First, let us observe that we may always replace X_K and Z_K by finite étale coverings of X_K and Z_K, respectively, without affecting the validity of either the hypotheses or the conclusion of the lemma. Next, fix a geometric point $\overline{z}$ of Z as in the statement of Lemma 4.6, and write $X_{\overline{z}}$ for the resulting geometric fiber. Then the *existence of the section* σ implies that we obtain an exact sequence of fundamental groups:

$$1 \to \pi_1(X_{\overline{z}}) \to \pi_1(X_K) \to \pi_1(Z_K) \to 1$$

Indeed, in general (i.e., in the absence of hypothesis that σ exist) the morphism $\pi_1(X_{\overline{z}}) \to \pi_1(X_K)$ need not be injective. That is to say, its kernel is naturally isomorphic to the cokernel of the morphism (induced by $X_K \to Z_K$ via functoriality) between certain étale-theoretic *second homotopy groups* of X_K and Z_K (cf. [Frdl], p. 107, Theorem 11.5). On the other hand, since $X_K \to Z_K$ *admits a section*, it thus follows (by functoriality) that this morphism between second homotopy groups also admits a section, hence that it is surjective (i.e., its cokernel is trivial). This implies the injectivity of the morphism $\pi_1(X_{\overline{z}}) \to \pi_1(X_K)$. Note that, stated in words, the injectivity of this morphism implies that (after possible base-change to a finite étale covering of Z_K) *any finite étale covering of* $X_{\overline{z}}$ *may be realized as the restriction to the fiber* $X_{\overline{z}}$ *of a finite étale covering of* X_K.

Next, let us consider the *Leray-Serre spectral sequence* associated to the morphism $X_K \to Z_K$ for étale cohomology with coefficients in $(\mathbf{Z}/p^n\mathbf{Z})(1)$ (for some p, n as in Definition 4.1). If we consider the "E_2-term"of this spectral sequence, we see that the cohomology group $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ gets a natural filtration whose "highest subquotient" (i.e., the subquotient which is, in fact, a quotient) is a submodule of $H^0_{\mathrm{et}}(Z_K, H^2_{\mathrm{et}}(X_{\overline{z}}, (\mathbf{Z}/p^n\mathbf{Z})(1)))$. On the other hand, by the assumptions placed on $X_{\overline{z}}$, it follows that all the classes of $H^2_{\mathrm{et}}(X_{\overline{z}}, (\mathbf{Z}/p^n\mathbf{Z})(1))$ *vanish* upon restriction to some finite étale covering of $X_{\overline{z}}$. Moreover, by the discussion of the preceding paragraph, it follows that this covering may be realized as the restriction to $X_{\overline{z}}$ of a finite étale covering of X_K. Thus, in conclusion, by replacing X_K and Z_K by appropriate finite étale coverings, we may assume that the image of the class $c_1(\mathcal{L})$ mod p^n in the highest subquotient of $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ *vanishes.*

The next highest subquotient of the natural filtration on $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ induced by the Leray-Serre spectral sequence may be regarded naturally as a submodule of $H^1_{\mathrm{et}}(Z_K, H^1_{\mathrm{et}}(X_{\overline{z}}, (\mathbf{Z}/p^n\mathbf{Z})(1)))$. Thus, by an argument similar to that of the preceding paragraph, we conclude that we may assume that the image of the class $c_1(\mathcal{L})$ mod p^n in the next highest subquotient of $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ also *vanishes.*

The next subquotient (i.e., the subquotient which is, in fact, a submodule) of the natural filtration on $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ induced by the Leray-Serre spectral sequence is given by the submodule of $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ which is the image of $H^2_{\mathrm{et}}(Z_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ in $H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ (via pull-back relative to $X_K \to Z_K$). Note that the existence of the section σ implies that this pull-back morphism $H^2_{\mathrm{et}}(Z_K, (\mathbf{Z}/p^n\mathbf{Z})(1)) \to H^2_{\mathrm{et}}(X_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ is *injective.* Thus, we conclude that the class $c_1(\mathcal{L})$ mod p^n arises as the pull-back to X_K of a class in $H^2_{\mathrm{et}}(Z_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$. On the other hand, by pulling back via σ (and applying the functoriality of the formation of the Chern class of a line bundle), we thus see that this class in $H^2_{\mathrm{et}}(Z_K, (\mathbf{Z}/p^n\mathbf{Z})(1))$ is simply $c_1(\sigma^*(\mathcal{L}))$ mod p^n, which is $= 0$ (since $\sigma^*(\mathcal{L})$ is assumed to be *trivial*). This completes the proof of Lemma 4.6. ○

§4.2. The Group-Theoreticity of a Certain Chern Class

In this §, we let K be a field of *characteristic* 0. Also, we fix a *prime number* p and an integer $g \geq 2$.

Let us denote by $\mathcal{A}$ the *moduli stack of principally polarized abelian varieties of dimension* g. Write

$$\mathcal{G} \to \mathcal{A}$$

for the *tautological abelian scheme* over $\mathcal{A}$, and $\epsilon : \mathcal{A} \to \mathcal{G}$ for its identity section. Also, let us denote by $\mathcal{L}$ the *tautological line bundle* on $\mathcal{G}$ that defines the principal polarization. Thus, $\mathcal{L}$ is *relatively ample over* $\mathcal{A}$, and we assume that it is *rigidified* by some isomorphism $\epsilon^*(\mathcal{L}) \cong \mathcal{O}_{\mathcal{A}}$. Also, we fix a *geometric point* $\overline{a} \in \mathcal{A}(\overline{K})$, and denote the fundamental group $\pi_1(\mathcal{G}_{\overline{a}})$ of the geometric fiber $\mathcal{G}_{\overline{a}}$ by $\pi_1(\mathcal{G}/\mathcal{A})$. Thus, we obtain an exact sequence of fundamental groups

$$1 \to \pi_1(\mathcal{G}/\mathcal{A}) \to \pi_1(\mathcal{G}) \to \pi_1(\mathcal{A}) \to 1$$

equipped with a section $\pi_1(\epsilon) : \pi_1(\mathcal{A}) \to \pi_1(\mathcal{G})$ which allows us to identify $\pi_1(\mathcal{G})$ with the semi-direct product $\pi_1(\mathcal{G}/\mathcal{A}) \rtimes \pi_1(\mathcal{A})$. Next, observe that since $\pi_1(\mathcal{G}/\mathcal{A})$ is a free $\widehat{\mathbf{Z}}$-module of rank $2g$, we may write

$$\pi_1(\mathcal{G}/\mathcal{A}) = \Pi^{(p)}_{\mathcal{G}/\mathcal{A}} \times \Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}$$

for the natural decomposition of $\pi_1(\mathcal{G}/\mathcal{A})$ as a product of a $\mathbf{Z}_p$-free module — i.e., $\Pi^{(p)}_{\mathcal{G}/\mathcal{A}}$ — and a module $\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}$ which is free over the product of all $\mathbf{Z}_{p'}$, where p' ranges over the prime numbers not equal to p. Moreover, the above exact sequence shows that $\pi_1(\mathcal{A})$ *acts naturally on* $\pi_1(\mathcal{G}/\mathcal{A})$ in a way that respects this decomposition. In particular, we may push forward the above exact sequence via the quotient $\pi_1(\mathcal{G}/\mathcal{A}) \twoheadrightarrow \Pi^{(p)}_{\mathcal{G}/\mathcal{A}}$ to obtain exact sequences (where $\Pi^{(p/\mathcal{A})}_{\mathcal{G}}$ is *defined* by the first exact sequence)

$$1 \to \Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}} \to \pi_1(\mathcal{G}) \to \Pi^{(p/\mathcal{A})}_{\mathcal{G}} \to 1$$

$$1 \to \Pi^{(p)}_{\mathcal{G}/\mathcal{A}} \to \Pi^{(p/\mathcal{A})}_{\mathcal{G}} \to \pi_1(\mathcal{A}) \to 1$$

— of which the second exact sequence admits a section that allows us to identify $\Pi^{(p/\mathcal{A})}_{\mathcal{G}}$ with the semi-direct product $\Pi^{(p)}_{\mathcal{G}/\mathcal{A}} \rtimes \pi_1(\mathcal{A})$.

Now let us consider $\pi_1(\mathcal{A})$ in greater detail. First, we observe that $\pi_1(\mathcal{A})$ fits into an exact sequence

$$1 \to Sp(\pi_1(\mathcal{G}/\mathcal{A})) \to \pi_1(\mathcal{A}) \to \Gamma_K \to 1$$

(where $Sp(\pi_1(\mathcal{G}/\mathcal{A}))$ denotes the group of $\widehat{\mathbf{Z}}$-linear automorphisms of $\pi_1(\mathcal{G}/\mathcal{A})$ that preserve the symplectic form defined by the tautological principal polarization). (Note that here, we use the well-known facts that: (i.) when $K = \mathbf{C}$, the topological fundamental group of $\mathcal{A}$ is equal to $Sp(2g, \mathbf{Z})$; (ii.) for $g \geq 2$, the congruence subgroup problem for $Sp(2g, \mathbf{Z})$ has been resolved affirmatively (cf. the proof of Lemma 3.16; [BMS]).) In particular, since

$$Sp(\pi_1(\mathcal{G}/\mathcal{A})) = Sp(\Pi^{(p)}_{\mathcal{G}/\mathcal{A}}) \times Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}})$$

we thus obtain an injection $Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}) \hookrightarrow \pi_1(\mathcal{A})$. Since it is clear that the image of this injection forms a normal subgroup of $\pi_1(\mathcal{A})$, we may form the quotient — which we denote by $\Pi^{(p)}_{\mathcal{A}}$ — of $\pi_1(\mathcal{A})$ by this subgroup. Thus, we obtain exact sequences:

$$1 \to Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}) \to \pi_1(\mathcal{A}) \to \Pi^{(p)}_{\mathcal{A}} \to 1$$

$$1 \to Sp(\Pi^{(p)}_{\mathcal{G}/\mathcal{A}}) \to \Pi^{(p)}_{\mathcal{A}} \to \Gamma_K \to 1$$

Next, let us observe that since the subgroup $Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}) \subseteq \pi_1(\mathcal{A})$ preserves and acts trivially on the quotient $\pi_1(\mathcal{G}/\mathcal{A}) \twoheadrightarrow \Pi^{(p)}_{\mathcal{G}/\mathcal{A}}$, we thus conclude (by thinking of $\Pi^{(p/\mathcal{A})}_{\mathcal{G}}$ as $\Pi^{(p)}_{\mathcal{G}/\mathcal{A}} \rtimes \pi_1(\mathcal{A})$) that $Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}})$ defines a *normal subgroup* of $\Pi^{(p/\mathcal{A})}_{\mathcal{G}}$. Let us denote the quotient of $\Pi^{(p/\mathcal{A})}_{\mathcal{G}}$ by this normal subgroup by $\Pi^{(p)}_{\mathcal{G}}$. Thus, we obtain exact sequences:

$$1 \to Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}) \to \Pi^{(p/\mathcal{A})}_{\mathcal{G}} \to \Pi^{(p)}_{\mathcal{G}} \to 1$$

$$1 \to \Pi^{(p)}_{\mathcal{G}/\mathcal{A}} \to \Pi^{(p)}_{\mathcal{G}} \to \Pi^{(p)}_{\mathcal{A}} \to 1$$

In particular, we obtain surjections $\pi_1(\mathcal{G}) \twoheadrightarrow \Pi^{(p/\mathcal{A})}_{\mathcal{G}} \twoheadrightarrow \Pi^{(p)}_{\mathcal{G}}$, where the kernel of this first (respectively, second) surjection is equal to $\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}}$ (respectively, $Sp(\Pi^{(\neq p)}_{\mathcal{G}/\mathcal{A}})$).

Since, in the present discussion, we would like to concentrate our attention on the *prime* p, let us denote (by abuse of notation relative to Definition 4.1) the p-adic component of the first Chern class of $\mathcal{L}$ by:

$$c_1(\mathcal{L}) \in H^2_{\text{et}}(\mathcal{G}, \mathbf{Z}_p(1))$$

Then we have the following:

Lemma 4.7. *Relative to the tautological morphisms*

$$\mathcal{G}_{\text{et}} \to B(\pi_1(\mathcal{G})) \to B(\Pi^{(p)}_{\mathcal{G}})$$

(cf. the proof of Lemma 4.5), the class $c_1(\mathcal{L}) \bmod p^n \in H^2_{\text{et}}(\mathcal{G}, (\mathbf{Z}/p^n\mathbf{Z})(1))$ *arises from a class* $\in H^2(\Pi^{(p)}_{\mathcal{G}}, (\mathbf{Z}/p^n\mathbf{Z})(1))$.

Proof. Indeed, Lemma 4.7 follows from Lemmas 4.4, 4.5, together with the proof of Lemma 4.6 (where, in Lemma 4.6, we take "$\mathcal{G} \to \mathcal{A}$" as our smooth, proper morphism "$X_K \to Z_K$"). In fact, if we apply Lemmas 4.4, 4.5, 4.6, literally as stated, we already obtain that $c_1(\mathcal{L})$ arises from a class $\in H^2(\pi_1(\mathcal{G}), \mathbf{Z}_p(1))$. Since the kernel of the surjection $\pi_1(\mathcal{G}) \twoheadrightarrow \Pi_{\mathcal{G}}^{(p/\mathcal{A})}$ is equal to $\Pi_{\mathcal{G}/\mathcal{A}}^{(\neq p)}$, which is a profinite group of order prime to p, it thus follows immediately that this class arises from a class $\in H^2(\Pi_{\mathcal{G}}^{(p/\mathcal{A})}, \mathbf{Z}_p(1))$. To see that, in fact, $c_1(\mathcal{L})$ mod p^n arises from a class $\in H^2(\Pi_{\mathcal{G}}^{(p)}, (\mathbf{Z}/p^n\mathbf{Z})(1))$, it suffices to observe that, in the proof of Lemma 4.6, the only coverings of $\mathcal{G}$ that were necessary to annihilate $c_1(\mathcal{L})$ modulo p^n were coverings of $\mathcal{G}$ that restricted to arbitrary p-power coverings of the abelian variety $\mathcal{G}_{\overline{a}}$. But it is clear from the definition of $\Pi_{\mathcal{G}}^{(p)}$ (cf. the discussion above) that such coverings may be constructed from quotients of $\Pi_{\mathcal{G}}^{(p/\mathcal{A})}$ that factor through the quotient $\Pi_{\mathcal{G}}^{(p/\mathcal{A})} \twoheadrightarrow \Pi_{\mathcal{G}}^{(p)}$. Thus, we conclude by taking "Q" to be the quotient $\pi_1(\mathcal{G}) \twoheadrightarrow \Pi_{\mathcal{G}}^{(p)}$ in Lemmas 4.4, 4.5. This completes the proof of Lemma 4.7. ◯

Next, let us write $\mathcal{M}$ for the *moduli stack of smooth, proper curves of genus g* over K, and

$$\mathcal{C} \to \mathcal{M}$$

for the *tautological curve* over $\mathcal{M}$. Then we would like to relate $\mathcal{C} \to \mathcal{M}$ to $\mathcal{G} \to \mathcal{A}$ as follows: Let us write $\mathcal{J} \to \mathcal{M}$ for the *Jacobian* of $\mathcal{C} \to \mathcal{M}$, and (for $d \in \mathbf{Z}$) let us write $\mathcal{J}_d \to \mathcal{M}$ for the $\mathcal{J}$-torsor over $\mathcal{M}$ that parametrizes line bundles on $\mathcal{C}$ of relative degree d over $\mathcal{M}$. Thus, the canonical bundle $\omega_{\mathcal{C}/\mathcal{M}}$ on $\mathcal{C}$ defines a natural isomorphism $\mathcal{J}_{2g-2} \cong \mathcal{J}$. On the other hand, by assigning to a point of the curve $\mathcal{C}$ the line bundle on $\mathcal{C}$ defined by that point (regarded as an effective divisor), we obtain a morphism

$$\mathcal{C} \to \mathcal{J}_1$$

(which is, in fact, a closed immersion). Raising line bundles of degree 1 to the $(2g-2)$-th power defines a finite morphism $\mathcal{J}_1 \to \mathcal{J}_{2g-2} \cong \mathcal{J}$. Thus, composing this morphism with $\mathcal{C} \to \mathcal{J}_1$, we obtain a natural finite morphism $\mathcal{C} \to \mathcal{J}$. Now, if we write $\mathcal{M} \to \mathcal{A}$ for the *Torelli morphism* (i.e., the classifying morphism of the abelian scheme $\mathcal{J} \to \mathcal{M}$), we thus obtain a commutative diagram:

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{G} \\ \downarrow & & \downarrow \\ \mathcal{M} & \longrightarrow & \mathcal{A} \end{array}$$

with the property that the pull-back to $\mathcal{C}$ of the tautological line bundle $\mathcal{L}$ on $\mathcal{G}$ forms a line bundle $\mathcal{P}$ on $\mathcal{C}$ which is *relatively ample* over $\mathcal{M}$.

Next, we consider *fundamental groups*. Fix a geometric point $\overline{m} \in \mathcal{M}(\overline{K})$, and a *set Σ of prime numbers such that $p \in \Sigma$*. Write $\pi_1(\mathcal{C}/\mathcal{M})$ for $\pi_1(\mathcal{C}_{\overline{m}})$, and

$\pi_1(\mathcal{C}/\mathcal{M}) \twoheadrightarrow \Pi_{\mathcal{C}/\mathcal{M}}$ for the *maximal pro-Σ quotient* of $\pi_1(\mathcal{C}/\mathcal{M})$. Since this quotient is *characteristic*, we thus obtain a morphism

$$\rho_{\mathcal{M}} : \pi_1(\mathcal{M}) \to \mathrm{Out}(\Pi_{\mathcal{C}/\mathcal{M}})$$

(where $\mathrm{Out}(-)$ denotes the group of continuous outer automorphisms of the profinite group in parentheses). Let us write $\Pi_{\mathcal{M}}$ for the quotient of $\pi_1(\mathcal{M})$ by the kernel of the restriction of $\rho_{\mathcal{M}}$ to $\pi_1(\mathcal{M}_{\overline{K}}) \subseteq \pi_1(\mathcal{M})$. Thus, if we write $\Pi_{\mathcal{M}_{\overline{K}}}$ for the image of the restriction of $\rho_{\mathcal{M}}$ to $\pi_1(\mathcal{M}_{\overline{K}})$, then we obtain an exact sequence

$$1 \to \Pi_{\mathcal{M}_{\overline{K}}} \to \Pi_{\mathcal{M}} \to \Gamma_K \to 1$$

Moreover, $\rho_{\mathcal{M}}$ factors through the quotient $\pi_1(\mathcal{M}) \twoheadrightarrow \Pi_{\mathcal{M}}$, hence defines a morphism

$$\rho^{\Pi}_{\mathcal{M}} : \Pi_{\mathcal{M}} \to \mathrm{Out}(\Pi_{\mathcal{C}/\mathcal{M}})$$

Now, if we pull-back the natural exact sequence

$$1 \to \Pi_{\mathcal{C}/\mathcal{M}} = \mathrm{Inn}(\Pi_{\mathcal{C}/\mathcal{M}}) \to \mathrm{Aut}(\Pi_{\mathcal{C}/\mathcal{M}}) \to \mathrm{Out}(\Pi_{\mathcal{C}/\mathcal{M}}) \to 1$$

(where $\mathrm{Inn}(-)$ (respectively, $\mathrm{Aut}(-)$) denotes the group of continuous inner (respectively, all) automorphisms of the profinite group in parentheses) via the morphism $\rho^{\Pi}_{\mathcal{M}}$ defined by $\rho_{\mathcal{M}}$, we obtain an exact sequence

$$1 \to \Pi_{\mathcal{C}/\mathcal{M}} \to \Pi_{\mathcal{C}} \to \Pi_{\mathcal{M}} \to 1$$

Moreover, it follows immediately from the definitions of the various "Π's" and "$\Pi^{(p)}$'s" that we obtain a commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \Pi_{\mathcal{C}/\mathcal{M}} & \longrightarrow & \Pi_{\mathcal{C}} & \longrightarrow & \Pi_{\mathcal{M}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Pi^{(p)}_{\mathcal{G}/\mathcal{A}} & \longrightarrow & \Pi^{(p)}_{\mathcal{G}} & \longrightarrow & \Pi^{(p)}_{\mathcal{A}} & \longrightarrow & 1
\end{array}$$

Thus, we conclude the following:

Corollary 4.8. *For all integers $n \geq 1$, the first Chern class of the relatively ample line bundle $\mathcal{P}$ on $\mathcal{C}$ modulo p^n ($\in H^2_{\mathrm{et}}(\mathcal{C}, (\mathbf{Z}/p^n\mathbf{Z})(1))$) arises from a class $\in H^2(\Pi_{\mathcal{C}}, (\mathbf{Z}/p^n\mathbf{Z})(1))$.*

Proof. This follows immediately from the above discussion by "pulling back" the classes of Lemma 4.7 via $\mathcal{C} \to \mathcal{G}$, $\Pi_{\mathcal{C}} \to \Pi^{(p)}_{\mathcal{G}}$. ○

§4.3. A Generalization of the Main Result of [Mzk2]

In this §, we maintain the notation of §4.2.

Let us assume that we are given two *hyperbolic curves* X_1, X_2 *of type* (g, r) *over* K. For $i = 1, 2$, let us write $\pi_1((X_i)_{\overline{K}}) \twoheadrightarrow \Pi_{(X_i)_{\overline{K}}}$ for the *maximal pro-*Σ *quotient* of $\pi_1((X_i)_{\overline{K}})$, and $\pi_1(X_i) \twoheadrightarrow \Pi_{X_i}$ for the quotient of $\pi_1(X_i)$ by the kernel of $\pi_1((X_i)_{\overline{K}}) \twoheadrightarrow \Pi_{(X_i)_{\overline{K}}}$. Thus, for $i = 1, 2$, we obtain exact sequences:

$$1 \to \Pi_{(X_i)_{\overline{K}}} \to \Pi_{X_i} \to \Gamma_K \to 1$$

Next, let us write $\mathcal{M}$ for the *moduli stack of hyperbolic curves of type* (g, r) *over* K. Since X_i defines a point $[X_i] \in \mathcal{M}(K) \subseteq \mathcal{M}(\overline{K})$, if we join the points $[X_1], [X_2] \in \mathcal{M}(\overline{K})$ via a path in the *étale fundamental groupoid of* $\mathcal{M}_{\overline{K}}$, then we obtain a *class* — which we denote by β — *of outer isomorphisms*

$$\beta = \{\Pi_{(X_1)_{\overline{K}}} \cong \Pi_{(X_2)_{\overline{K}}}\}$$

with the property that any two outer isomorphisms of this class differ by an element of $\rho^{\Pi}_{\mathcal{M}}(\Pi_{\mathcal{M}_{\overline{K}}})$.

Next, let us assume that we are given an *isomorphism*

$$\alpha : \Pi_{X_1} \cong \Pi_{X_2}$$

which preserves and induces the identity on the quotients $\Pi_{X_i} \twoheadrightarrow \Gamma_K$. Thus, α induces isomorphisms:

$$\Pi_{\alpha_{\overline{K}}} : \Pi_{(X_1)_{\overline{K}}} \cong \Pi_{(X_2)_{\overline{K}}}$$

$$\alpha_{H^2_{\text{et}}} : H^2_{\text{et}}(X_1, \mathbf{Z}_p(1)) \cong H^2(\Pi_{X_1}, \mathbf{Z}_p(1)) \cong H^2(\Pi_{X_2}, \mathbf{Z}_p(1)) \cong H^2_{\text{et}}(X_2, \mathbf{Z}_p(1))$$

Now we make the following important

Definition 4.9. We shall say that α is *of monodromy type* if the isomorphism $\Pi_{\alpha_{\overline{K}}}$ defined by α belongs to the class of isomorphisms defined by β.

Corollary 4.10. *Suppose that α is* **of monodromy type** *and $r = 0$. Then for $i = 1, 2$, there exist ample line bundles $\mathcal{P}_i$ on X_i with the property that $c_1(\mathcal{P}_1) \in H^2_{\text{et}}(X_1, \mathbf{Z}_p(1))$ maps to $c_1(\mathcal{P}_2) \in H^2_{\text{et}}(X_2, \mathbf{Z}_p(1))$ under $\alpha_{H^2_{\text{et}}}$.*

Proof. Since X_1, X_2 define classifying morphisms $\kappa_1, \kappa_2 : \text{Spec}(K) \to \mathcal{M}$, we let $\mathcal{P}_1$, $\mathcal{P}_2$, be the respective pull-backs (where we note that $X_i = \mathcal{C} \times_{\mathcal{M}, \kappa_i} \text{Spec}(K)$) of the line bundle $\mathcal{P}$ of Corollary 4.8. Then the coincidence of cohomology classes over $\mathbf{Z}_p$ asserted in Corollary 4.10 may be checked after reduction modulo p^n (where we let n range over all positive integers). Moreover, by pulling back the class $\in H^2(\Pi_{\mathcal{C}}, (\mathbf{Z}/p^n\mathbf{Z})(1))$ (cf. the Remark immediately following the present proof) whose existence was established in Corollary 4.8, this coincidence of cohomology classes modulo p^n will follow as soon as we show that the morphisms

$$\xi_i : \Gamma_K \to \Pi_{\mathcal{M}}$$

defined by X_1, X_2 *coincide* up to composition with an inner automorphism defined by an element of $\Pi_{\mathcal{M}_{\overline{K}}}$ (where we note that such inner automorphisms induce the identity on all group cohomology modules). But, tracing through the definitions — cf., especially, the definition of $\Pi_{\mathcal{M}}$ (which implies that we have a *natural inclusion* $\Pi_{\mathcal{M}} \hookrightarrow \Gamma_K \times \mathrm{Out}(\Pi_{\mathcal{C}/\mathcal{M}})$) and Definition 4.9 — we see that this coincidence of the ξ_i (up to composition with an inner automorphism defined by an element of $\Pi_{\mathcal{M}_{\overline{K}}}$) is a formal consequence of the existence of the *isomorphism of monodromy type* α. This completes the proof of Corollary 4.10. ○

Remark. Note that in the proof of Corollary 4.10, we also made implicit use of the fact that the isomorphism of monodromy type α may be recovered from some appropriate inner automorphism of $\Pi_{\mathcal{M}}$ defined by an element of $\Pi_{\mathcal{M}_{\overline{K}}}$ that relates the ξ_i to one another. Indeed, this follows by pulling back the exact sequence

$$1 \to \Pi_{\mathcal{C}/\mathcal{M}} \to \Pi_{\mathcal{C}} \to \Pi_{\mathcal{M}} \to 1$$

via the ξ_i. In particular, we made implicit use of the fact that hyperbolic curves have *center-free* geometric fundamental groups, a property *not* possessed by abelian varieties. This is why it was necessary prove Corollary 4.8 before proving Corollary 4.10 (i.e., why we could not derive Corollary 4.10 directly from Lemma 4.7).

We are now ready to state and prove the *main result of the present §4*:

Definition 4.11. We shall say that K is *generalized sub-p-adic* if K may be embedded as a subfield of a finitely generated extension of the quotient field of $W(\overline{\mathbf{F}}_p)$ (the ring of Witt vectors with coefficients in the algebraic closure of $\mathbf{F}_p$).

Remark. Note that *sub-p-adic fields are always generalized sub-p-adic.* On the other hand, fields such as the maximal algebraic extension of $\mathbf{Q}$ which is unramified over p are *generalized sub-p-adic, but not sub-p-adic.*

Remark. Suppose that K is *generalized sub-p-adic.* Then note that even if we do not know *a priori* that the hyperbolic curves X_1, X_2 are of the same type (g, r), *the mere existence of an isomorphism*

$$\alpha : \Pi_{X_1} \cong \Pi_{X_2}$$

(which preserves and induces the identity on the quotients $\Pi_{X_i} \twoheadrightarrow \Gamma_K$, but is not necessarily of monodromy type) *already implies that X_1 and X_2 are of the same type*. Indeed, to see this, we reduce immediately to the case where K is finite over the quotient field of $W(\overline{\mathbf{F}}_p)$ and then consider the dimension of the weight 0 portion of the Hodge-Tate decomposition of the maximal pro-p abelian quotient of $\Pi_{(X_i)_{\overline{K}}}$. This dimension gives back the genus g; then r may be recovered from the fact that $\Pi_{(X_i)_{\overline{K}}}$ is free on $2g + r - 1$ generators (respectively, not free) if $r > 0$ (respectively, $r = 0$). Thus, in conclusion, *when K is generalized sub-p-adic, it makes sense to state that such an isomorphism α is "of monodromy type" even if we do not assume a priori (as in the above discussion) that the X_i are of the same type.*

Theorem 4.12. (Monodromy Type Isomorphism Version of the Grothendieck Conjecture over Generalized Sub-p-adic Fields) *Suppose that K is a* **generalized sub-p-adic field**. *Let X_1, X_2 be hyperbolic curves over K. Let us write* $\mathrm{Isom}(X_1, X_2)$ *for the set of K-isomorphisms between X_1 and X_2, and* $\mathrm{Isom}^{\mathrm{mono}}_{\Gamma_K}(\Pi_{X_1}, \Pi_{X_2})$ *for the set of continuous group isomorphisms $\Pi_{X_1} \cong \Pi_{X_2}$ over Γ_K, considered up to composition with an inner automorphism arising from $\Pi_{(X_1)_{\overline{K}}}$ or $\Pi_{(X_2)_{\overline{K}}}$, which are of* **monodromy type** *(cf. Definition 4.9). Then the natural map*

$$\mathrm{Isom}(X_1, X_2) \to \mathrm{Isom}^{\mathrm{mono}}_{\Gamma_K}(\Pi_{X_1}, \Pi_{X_2})$$

is bijective.

Remark. If the morphisms $\xi_i : \Gamma_K \to \Pi_{\mathcal{M}}$ defined by the X_i coincide up to composition with an inner automorphism of $\Pi_{\mathcal{M}}$ defined by an element of $\Pi_{\mathcal{M}_{\overline{K}}}$, then *every choice of such an inner automorphism defines an isomorphism $\alpha : \Pi_{X_1} \cong \Pi_{X_2}$ over Γ_K of monodromy type* (cf. the proof of Corollary 4.10 and the Remark following this proof). Thus, one consequence of Theorem 4.12 that does not make explicit use of the notion of "isomorphisms of monodromy type" is the following:

> If K is generalized sub-p-adic, and $\mathcal{M}$ denotes the moduli stack of hyperbolic curves of type (g, r) over K, then the natural morphism
>
> $$\mathcal{M}(K) \to \mathrm{Sect}_{\Gamma_K}(\Gamma_K, \Pi_{\mathcal{M}})$$
>
> is *injective*.

(Here, $\Pi_{\mathcal{M}}$ is as defined in §4.2 (where we note that the same formal definition can be made even in the case $r > 0$), and "$\mathrm{Sect}_{\Gamma_K}(\Gamma_K, \Pi_{\mathcal{M}})$" is the set of sections of the projection $\Pi_{\mathcal{M}} \twoheadrightarrow \Gamma_K$ considered up to composition with an inner automorphism of $\Pi_{\mathcal{M}}$ arising from $\Pi_{\mathcal{M}_{\overline{K}}}$.)

Proof. In a word, once one has Corollary 4.10, the proof of Theorem 4.12 is entirely similar to the proof of Theorem A in [Mzk2], so we will only sketch details.

First, we reduce immediately to the case where K is a *finite extension of the quotient field of* $W(\overline{\mathbf{F}}_p)$ (cf. Lemmas 4.13, 4.14, below; [Mzk2], §15), and X_1, X_2 are *proper of genus* g (cf. [Mzk2], proof of Theorem 14.1).

Now, *the main idea of the proof is to replace the portion of the proof of [Mzk2] given in [Mzk2], §1 – 6, by Corollary 4.10*, by using the following argument. First, (for $i = 1, 2$) let us write

$$\mathcal{H}_i \stackrel{\text{def}}{=} H^2_{\text{et}}(X_i, \mathbf{Q}_p(1))$$

and $\mathcal{G}_i \subseteq \mathcal{H}_i$ for the *geometric part* of $\mathcal{H}_i$, i.e., the $\mathbf{Q}_p$-subspace generated by first Chern classes of line bundles on X_i. Also, let us write J_i for the *Jacobian* of X_i, and $T(J_i)$ for its associated *p-adic Tate module.* Note that α induces an isomorphism $\alpha_{\mathcal{H}} : \mathcal{H}_1 \cong \mathcal{H}_2$. Also, let us observe that since K has cohomological dimension 1 (cf. Lemma 4.13 below), applying the Leray-Serre spectral sequence (for Galois cohomology with coefficients in $\mathbf{Q}_p(1)$) to the surjection $\Pi^{(p)}_{X_i} \twoheadrightarrow \Gamma_K$ gives rise to an exact sequence:

$$0 \to H^1(K, T(J_i) \otimes \mathbf{Q}_p) \to \mathcal{H}_i \to \mathbf{Q}_p \to 0$$

(where the "$T(J_i)$" on the left should, strictly speaking, be the dual of $T(J_i)$, but we identify $T(J_i)$ with its dual via the standard principal polarization on the Jacobian J_i; the "$\mathbf{Q}_p$" on the right arises from the isomorphism $H^0(K, H^2(\Pi^{(p)}_{(X_i)_{\overline{K}}}, \mathbf{Q}_p(1)) \cong \mathbf{Q}_p$ defined by the "degree map").

Now I *claim* that $\alpha_{\mathcal{H}}(\mathcal{G}_1) = \mathcal{G}_2$. Indeed, by Corollary 4.10, there exists a line bundle $\mathcal{P}_i$ of *nonzero degree* on X_i such that $\alpha_{\mathcal{H}}(c_1(\mathcal{P}_1)) = c_1(\mathcal{P}_2)$. Thus, to show that $\alpha_{\mathcal{H}}(\mathcal{G}_1) = \mathcal{G}_2$, it suffices to show that $\alpha_{\mathcal{H}}$ preserves first Chern classes of line bundles of degree 0. Since we are working over $\mathbf{Q}_p$, we may always replace K by a finite extension of K without affecting the validity of the claim. In particular, we may assume that the X_i have semi-stable reduction over K. Write $\mathcal{J}_i$ for the unique semi-abelian scheme over $\mathcal{O}_K$ whose generic fiber is J_i. Now if $\mathcal{L}_i$ is a line bundle of degree 0 on X_i, it defines a point $[\mathcal{L}_i] \in J_i(K)$, hence, by Kummer theory (i.e., considering the obstruction to the p-power divisibility of $[\mathcal{L}_i]$ — cf. [Mzk2], §6, the discussion following Definition 6.1), determines an element $\kappa(\mathcal{L}_i) \in H^1(K, T(J_i) \otimes \mathbf{Q}_p)$. If we regard this Galois cohomology group as a subspace of $\mathcal{H}_i$ via the exact sequence of the preceding paragraph, then this class $\kappa(\mathcal{L}_i)$ *coincides with the first Chern class* $c_1(\mathcal{L}_i)$ *of* $\mathcal{L}_i$ (cf. [Mzk2], the Remark preceding Definition 6.2). On the other hand, *if* $[\mathcal{L}_1] \in J_1(K)$ *arises from a point* $\in \mathcal{J}_1(\mathcal{O}_K)$ *which is equal to the zero section modulo* $\mathfrak{m}_K$, *then* $\kappa(\mathcal{L}_1)$ *corresponds, via* α, *to* $\kappa(\mathcal{L}_2)$ *for some degree* 0 *line bundle* $\mathcal{L}_2$ *on* X_2 *defined by a point* $\in \mathcal{J}_2(\mathcal{O}_K)$ (which will also be equal to the zero section modulo $\mathfrak{m}_K$). Indeed, this follows by applying "Tate's theorem" (cf. [Tate], Theorem 4) as in the argument of the proof of [Mzk2], Theorem 7.4, to the p-divisible groups defined by the formal groups associated to

$\mathcal{J}_1$, $\mathcal{J}_2$. On the other hand, for *any* point $\in J_1(K)$ it follows from the fact that $\overline{\mathbf{F}}_p = \mathcal{O}_K/\mathfrak{m}_K$ *is a union of finite fields* that *some nonzero multiple of this point arises from a point* $\in \mathcal{J}_1(\mathcal{O}_K)$ *which is equal to the zero section modulo* $\mathfrak{m}_K$. Thus, since we are working with $\mathbf{Q}_p$*-coefficients*, we thus conclude that $\alpha_{\mathcal{H}}$ maps the $\mathbf{Q}_p$-subspace of $\mathcal{H}_1$ generated by first Chern classes of line bundles of degree 0 onto the corresponding subspace of $\mathcal{H}_2$. This completes the proof of the claim.

Before proceeding, we note here that *the argument of the preceding paragraph is the only place in this proof where we use that the original base field is a subfield of a finitely generated extension of the quotient field of* $W(\overline{\mathbf{F}}_p)$ — i.e., as opposed to $W(k)$, where we permit k to be an *arbitrary perfect field of characteristic* p. The arguments to be used in the remainder of the proof are valid for $\overline{\mathbf{F}}_p$ replaced by an arbitrary such k. Also, we remark here that (not surprisingly) the portion of the argument of [Mzk2] that corresponds to what was done in the preceding paragraph is given in [Mzk2], §1 – 6, where it was necessary, especially for the arguments of [Mzk2], Lemma 4.1, §6, to assume that the residue field be *finite* (i.e., not an arbitrary perfect field of characteristic p).

Now that we know that α preserves (up to $\mathbf{Q}_p$-coefficients) first Chern classes of line bundles over finite extensions of K, the rest of the argument of [Mzk2] goes through without much change. Namely, [Mzk2], Proposition 7.4, follows by the same argument as that given in *loc. cit.* (except that instead of working over a K which is finite over $\mathbf{Q}_p$ as in *loc. cit.*, we work over the present "K," which is finite over the quotient field of $W(\overline{\mathbf{F}}_p)$). We remark that in the present context, it is not necessary to distinguish between "F-geometricity" and "FI-geometricity" as was done in [Mzk2], since we are working with *proper* curves to begin with (cf. the Remark at the end of [Mzk2], §7). Then [Mzk2], §8, goes through without change (except that the finite field "k" is to be replaced by $\overline{\mathbf{F}}_p$). The convergence arguments of [Mzk2], §9, 10, are entirely valid when k is any perfect field of characteristic p, so no changes are necessary in these two §'s. [Mzk2], §11, is unnecessary in the present context since we are working with *proper* curves to begin with. Finally, the arguments of [Mzk2], §12 – 14, go through without essential change (except that they are much easier in the present context since we are working with *proper* curves to begin with). This completes the proof of the bijectivity assertion of Theorem 4.12 (cf. [Mzk2], Corollary 14.2). ○

Remark. Thus, Theorem 4.12 states (roughly) that the isomorphism class of a hyperbolic curve over a finite extension of the quotient field of $W(\overline{\mathbf{F}}_p)$ may be recovered from the outer action of the Galois group on its geometric fundamental group. In particular, one need not make use of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ (as was done in [Mzk2]). In this sense, *Theorem 4.12 is reminiscent of the main results of [Tama2]*, which state that in certain cases, the isomorphism class of a hyperbolic curve over $\overline{\mathbf{F}}_p$ is completely determined by the isomorphism class of its geometric fundamental group (cf. the results of [Tama1], which make essential use of the action of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$). It would be interesting to see if the relationship between Theorem 4.12 and [Tama2] could be understood more explicitly.

Remark. Another interesting aspect of Theorem 4.12 is the following: Note that, if K is a finite extension of the quotient field of $W(\overline{\mathbf{F}}_p)$, then *its absolute Galois group* Γ_K *has cohomological dimension* 1 (cf. Lemma 4.13 below). On the other hand, if X is a hyperbolic curve over K, then $\Pi_{X_{\overline{K}}}$ has cohomological dimension 2. Thus, *the cohomological dimension of* Π_X *is equal to* 3. Since, roughly speaking, Theorem 4.12, states that the structure of X is determined by Π_X, *Theorem 4.12 is reminiscent of the rigidity theorem of Mostow-Prasad for hyperbolic manifolds of real dimension* 3 (cf. the discussion of [Mzk4], Introduction, §0.10, 2.2.3, 2.2.6).

The following Lemma is, in essence, well-known:

Lemma 4.13. *Let K be a finite extension of the quotient field of $W(\overline{\mathbf{F}}_p)$. Then Γ_K is center-free and has cohomological dimension equal to* 1.

Proof. First, write L for the quotient field of $W(\overline{\mathbf{F}}_p)$, and L' for the union (inside L) of the quotient fields of the $W(k)$, as k ranges over all finite extensions of $\mathbf{F}_p$. Then the ring of integers $\mathcal{O}_{L'}$ of L' is the union of the $W(k)$, hence *stictly henselian*. Moreover, since $\mathcal{O}_L = W(\overline{\mathbf{F}}_p)$ is the p-adic completion of $\mathcal{O}_{L'}$, it follows immediately from the general theory of henselian rings that $\Gamma_L = \Gamma_{L'}$. In particular, since K is a finite extension of L, it follows that there exists a finite extension K' of L' such that $K = L \otimes_{L'} K'$. Moreover, since $\mathcal{O}_{K'}$ is strictly henselian, with completion equal to $\mathcal{O}_K$, we have $\Gamma_K = \Gamma_{K'}$. Thus, it suffices to prove that $\Gamma_{K'}$ is center-free and of cohomological dimension equal to 1. In the remainder of the proof, to simplify notation, we shall simply write K for K'.

Next, observe that by considering the maximal tamely ramified extension K^{tm} of K, we obtain an exact sequence

$$1 \to \Gamma_{K^{\mathrm{tm}}} \to \Gamma_K \to \prod_{l \neq p} \mathbf{Z}_l(1) \to 1$$

(where the product ranges over all prime numbers not equal to p). Since $\Gamma_{K^{\mathrm{tm}}}$ is a pro-p-group which is well-known to be center-free and of cohomological dimension 1 (cf., e.g., [Mzk2], the proof of Lemma 15.6), we thus obtain immediately that Γ_K is of cohomological dimension 1. To show that Γ_K is center-free, it suffices to show $\mathrm{Gal}(K^{\mathrm{tm}}/K)$ acts *faithfully* on $\Gamma^{\mathrm{ab}}_{K^{\mathrm{tm}}} \otimes \mathbf{Q}_p$ (where "ab" denotes the maximal abelian quotient). But this may be done as follows: Let $K_0 \subseteq K$ be a *finite* extension of $\mathbf{Q}_p$ such that K/K_0 is *unramified*. Thus, it follows that K^{tm} is also the maximal unramified extension of K_0, so $\mathrm{Gal}(K^{\mathrm{tm}}/K) \hookrightarrow \mathrm{Gal}(K^{\mathrm{tm}}/K_0)$. Now let L_0/K_0 be a finite, Galois, totally tamely ramified extension of K_0. Then $L_0 \subseteq K^{\mathrm{tm}}$, so we obtain a *surjection*:

$$\Gamma^{\mathrm{ab}}_{K^{\mathrm{tm}}} \otimes \mathbf{Q}_p \twoheadrightarrow (\Gamma^{\mathrm{ab}}_{L_0})^{\mathrm{wild}} \otimes \mathbf{Q}_p$$

(where the superscript "wild" denotes the wild inertia subgroup). But by the class field theory of finite extensions of $\mathbf{Q}_p$, one knows that $(\Gamma^{\mathrm{ab}}_{L_0})^{\mathrm{wild}} \otimes \mathbf{Q}_p$ is naturally isomorphic (via the p-adic logarithm — cf., e.g., [Mzk5], §2) to L_0, so the action of $\mathrm{Gal}(L_0/K_0)$ on $(\Gamma_{L_0}^{\mathrm{ab}})^{\mathrm{wild}} \otimes \mathbf{Q}_p$ is *faithful*. Since arbitrary finite quotients of $\mathrm{Gal}(K^{\mathrm{tm}}/K)$ may be realized as "$\mathrm{Gal}(L_0/K_0)$'s" for appropriate choices of K_0, L_0, it thus follows that $\mathrm{Gal}(K^{\mathrm{tm}}/K)$ acts *faithfully* on $\Gamma_{K^{\mathrm{tm}}}^{\mathrm{ab}} \otimes \mathbf{Q}_p$, as desired. This completes the proof of Lemma 4.13. ◯

Lemma 4.14. *Let K be generalized sub-p-adic. Then Γ_K is center-free.*

Proof. First, let us consider the case where K is *algebraic* (though not necessarily of finite degree) over $\mathbf{Q}$. Since K is assumed to be generalized sub-p-adic, it thus follows that K is contained in a finite extension of the quotient field of $W(\overline{\mathbf{F}}_p)$. In particular, it follows that there is a prime $\mathfrak{p}$ of K dividing p whose ramification index over p is *finite*. Thus, if we choose a prime $\overline{\mathfrak{p}}$ of $\overline{\mathbf{Q}}$ lying over $\mathfrak{p}$, and write $I_{\mathfrak{p}} \subseteq \Gamma_K$ for the inertia group of $\mathfrak{p}$ defined by this prime $\overline{\mathfrak{p}}$ of $\overline{\mathbf{Q}}$, then we have

$$\{1\} \neq I_{\mathfrak{p}} \subseteq \Gamma_K \subseteq \Gamma_{\mathbf{Q}}$$

If Γ_K is *not* center-free, then it follows that there exists some $\sigma\ (\neq 1) \ \in \Gamma_K$ that *commutes with* $I_{\mathfrak{p}}$. But one knows from algebraic number theory (cf. [NSW], Chapter XII, Corollary 12.1.3) that $I_{\mathfrak{p}} \bigcap (\sigma \cdot I_{\mathfrak{p}} \cdot \sigma^{-1}) = \{1\}$, hence that $I_{\mathfrak{p}} = \{1\}$, which is absurd. This completes the proof of Lemma 4.14 for *algebraic* K.

Now let K be *arbitrary generalized sub-p-adic*. Write $K_0 \stackrel{\mathrm{def}}{=} K \bigcap \overline{\mathbf{Q}}$. Thus, we have a *surjection*

$$\pi : \Gamma_K \twoheadrightarrow \Gamma_{K_0}$$

Since (by the above paragraph) we know that Γ_{K_0} is center-free, it follows that the center $Z(\Gamma_K)$ of Γ_K lies in the kernel of π. In particular, if X_L is any hyperbolic curve of type (g,r) over a finite extension L of K, and $\sigma \in Z(\Gamma_K) \subseteq \mathrm{Ker}(\pi)$, then it is essentially a tautology that the isomorphism

$$\Pi_{(X_L)_{\overline{K}}} \cong \Pi_{(X_L)^{\sigma}_{\overline{K}}}$$

induced by conjugating by σ is *of monodromy type*. (Note that here, the fact that $Z(\Gamma_K) \subseteq \mathrm{Ker}(\pi)$ implies that this isomorphism lies in the class β of isomorphisms determined by the image of $\rho^{\Pi}_{\mathcal{M}}(\Pi_{\mathcal{M}_{\overline{\mathbf{Q}}}}) \subseteq \mathrm{Out}(\Pi_{\mathcal{C}/\mathcal{M}})$, as opposed to the larger class of isomorphisms determined by the image of $\rho^{\Pi}_{\mathcal{M}}(\Pi_{\mathcal{M}_{\mathbf{Q}}}) \subseteq \mathrm{Out}(\Pi_{\mathcal{C}/\mathcal{M}})$.)

With this observation in hand, it follows that Lemma 4.14 may be derived from Lemma 4.13 by means of Theorem 4.12 using exactly the same argument as that used to derive [Mzk2], Lemma 15.8, from [Mzk2], Lemma 15.6, by means of [Mzk2], Corollary 15.3. ◯

Bibliography

[AG] N. Alling and N. Greenleaf, *Foundations of the theory of Klein surfaces*, *Lecture Notes in Mathematics* **219**, Springer Verlag (1971).

[BMS] H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for SL_n, $(n \geq 3)$ and Sp_{2n}, $(n \geq 2)$*, *IHES Publ. Math.* **33** (1967), pp. 59-137.

[Falt] G. Faltings, *Endlichkeitssätze für Abelschen Varietäten über Zahlkörpern*, *Inv. Math.* **73** (1983), pp. 349-366.

[Frdl] E. Friedlander, *Étale Homotopy of Simplicial Schemes*, Annals of Math. Studies **104**, Princeton University Press (1982).

[Gard] F. Gardiner, *Teichmüller Theory and Quadratic Differentials*, John Wiley and Sons (1987).

[Groth] A. Grothendieck, *letter to G. Faltings* (June 1983) in Lochak, L. Schneps, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, *London Math. Soc. Lect. Note Ser.* **242**, Cambridge Univ. Press (1997).

[Harts] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer Verlag (1977).

[Huis] J. Huisman, *On the fundamental group of a real algebraic curve*, manuscript.

[Kerck] S. Kerckhoff, *The Nielsen realization problem*, *Bull. Amer. Math. Soc. (N.S.)* **2** (1980), pp. 452-454.

[Krav] S. Kravetz, *On the geometry of Teichmüller spaces and the structure of their modular groups*, *Ann. Acad. Sci. Fenn. Ser. A I* **278** (1959), 35 pp.

[Lang] S. Lang, *Abelian Varieties*, Springer Verlag (1983).

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

[Maass] H. Maass, *Siegel's Modular Forms and Dirichlet Series*, Lecture Notes in Mathematics **216**, Springer Verlag (1971).

[Mord] L. Szpiro, *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*, *Astérisque* **127**, Soc. Math. France (1985).

[Mzk1] S. Mochizuki, *The Profinite Grothendieck Conjecture for Closed Hyperbolic Curves over Number Fields*, *J. Math. Sci., Univ. Tokyo* **3** (1996), pp. 571-627.

[Mzk2] S. Mochizuki, *The Local Pro-p Anabelian Geometry of Curves*, *Inv. Math.* **138** (1999), pp. 319-423.

[Mzk3] S. Mochizuki, *A Theory of Ordinary p-adic Curves*, *Publ. of RIMS* **32** (1996), pp. 957-1151.

[Mzk4] S. Mochizuki, *Foundations of p-adic Teichmüller Theory*, AMS/IP Studies in Advanced Mathematics **11**, American Mathematical Society/International Press (1999).

[Mzk5] S. Mochizuki, *A Version of the Grothendieck Conjecture for p-adic Local Fields*, The International Journal of Math. **8**, No. 4 (1997), pp. 499-506.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323**, Springer Verlag (2000).

[NTM] H. Nakamura, A. Tamagawa, S. Mochizuki, *The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves*, Sugaku **50** (1998), pp. 113–129; English translation in Sugaku Expositions (to appear).

[Schd] C. Scheiderer, *Real and étale cohomology*, Lecture Notes in Mathematics **1588**, Springer Verlag (1994).

[Ser1] J.-P. Serre, *Lie Algebras and Lie Groups*, Lecture Notes in Mathematics **1500**, Springer Verlag (1992).

[Ser2] J.-P. Serre (with the collaboration of Willem Kuyk and John Labute), *Abelian l-adic Representations and Elliptic Curves*, Addison-Wesley Publishing Company (1989).

[Ser3] J.-P. Serre, *Liste des courbes elliptiques à multiplication complexe dont l'invariant modulaire j est rational*, manuscript.

[SGA1] A. Grothendieck et al., *Revêtements étales et groupe fondamental*, Lecture Notes in Mathematics **224**, Springer Verlag (1971).

[SGA2] A. Grothendieck et al., *Cohomologie Locale des Faisceaux Cohérents et Théorèmes de Lefshetz Locaux et Globaux*, North-Holland, Amsterdam (1968).

[Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Publ. Math. Soc. of Japan **11**, Iwanami Shoten and Princeton University Press (1971).

[Stk] H. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), pp. 1-27.

[Tama1] A. Tamagawa, *The Grothendieck Conjecture for Affine Curves*, Compositio Math. **109**, No. 2 (1997), pp. 135-194.

[Tama2] A. Tamagawa, *On the tame fundamental groups of curves over algebraically closed fields of characteristic* > 0, to appear in the present Volume.

[Tate] J. Tate, *p-Divisible Groups*, Proceedings of a Conference on Local Fields, Driebergen, Springer Verlag (1967), pp. 158-183.

[Weber] H. Weber, *Lehrbuch der Algebra*, Vol. III, Chelsea Publ. Company.

[Wolp] S. Wolpert, *Geodesic length functions and the Nielsen problem*, J. Differential Geom. **25** (1987), pp. 275-296.