The Hodge-Arakelov Theory of Elliptic Curves in Positive Characteristic

Shinichi Mochizuki

October 2000

Contents:

Section 0: Introduction

The purpose of this paper is to study the Hodge-Arakelov theory of elliptic curves (cf. [Mzk1-4]) in *positive characteristic*. The first two §'s (§1,2) are devoted to studying the relationship of the *Frobenius* and *Verschiebung* morphisms of an elliptic curve in positive characteristic to the Hodge-Arakelov theory of elliptic curves. We begin by deriving a *"Verschiebung-Theoretic Analogue of the Hodge-Arakelov Comparison Isomorphism"* (Theorem 1.1) which underlies our analysis in §1,2. From this result, we derive, in particular, an *explicit description of the étale integral structure of an elliptic curve in positive characteristic* (Corollary 1.3). This result may be regarded as a characteristic p version of [Mzk3], Theorem 2.2, which (unlike *loc. cit.*, which holds only for ordinary elliptic curves) is valid *even for supersingular elliptic curves*.

Next, in §2, we apply the theory of §1 to obtain a *new proof using positive characteristic methods* (Theorem 2.3) of the scheme-theoretic portion of the Hodge-Arakelov Comparison Isomorphism of [Mzk1]. In some sense, this new proof is more elegant than the proof of [Mzk1], which involves the verification of various complicated combinatorial identities (cf. the Remarks following Theorem 2.3). This situation is rather reminiscent of the computation of the degree of the hyperbolically ordinary locus in *p-adic Teichmüller theory* ([Mzk5], Chapter V — cf., especially, the second Remark following Corollary 1.3). Indeed, in that case, as well, characteristic p methods (involving Frobenius and Verschiebung) give rise to *various nontrivial combinatorial identities*. It would be interesting if this sort of phenomenon could be understood more clearly at a conceptual level. Another interesting feature of the proof of Theorem 2.3 is the crucial use of a certain subgroup scheme of an elliptic curve in positive characteristic which may be regarded as an analogue of the *"global multiplicative subspace"* of [Mzk4], §3. That is to say, the crucial role of this subgroup scheme is reminiscent of the observation (cf. [Mzk4], §3,4) that such a global multiplicative subspace in the context of elliptic curves over number fields seems to be crucial to the application of Hodge-Arakelov theory to diophantine geometry.

Also, we remark that in the course of proving Theorem 2.3, we correct several *misprints* (cf. the Remark immediately following the proof of Proposition 2.2) in [Mzk3].

Finally, in §3, we work out the theory of [Mzk4], §2, in the case of $p = 2$. In *loc. cit.*, this theory was only worked out in the case of *odd* p (for the sake of simplicity). The case of $p = 2$ involves dealing with various technical complications modulo 2. Unlike the case of odd p, where the theory of [Mzk4], §2, allows one to relate the Lagrangian arithmetic Kodaira-Spencer morphism to the usual geometric Kodaira-Spencer morphism of a family of elliptic curves, in the case of $p = 2$, one obtains the result (Corollary 3.7) that *the Lagrangian arithmetic Kodaira-Spencer morphism is naturally related to the usual geometric Kodaira-Spencer morphism of the ample line bundle under consideration.*

Notation and Conventions:

We will denote by $(\overline{\mathcal{M}}_{\mathrm{ell}}^{\log})_{\mathbb{Z}}$ the *log moduli stack of log elliptic curves over* $\mathbb{Z}$ (cf. [Mzk1], Chapter III, Definition 1.1), where the log structure is that defined by the divisor at infinity. (In [Mzk1-4], $\overline{\mathcal{M}}_{\mathrm{ell}}$ was denoted by "$\overline{\mathcal{M}}_{1,0}$." This change of notation was adopted in response to the criticism voiced by a number of mathematicians with respect to the notation $\overline{\mathcal{M}}_{1,0}$.) The open substack of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$ parametrizing (smooth) elliptic curves will be denoted by $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Z}} \subseteq (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$.

Acknowledgements: The author would like to thank A. Tamagawa for stimulating discussions of the various topics presented in this manuscript.

Section 1: The Verschiebung Morphism in Positive Characteristic

Fix a *prime number* p. Let $S^{\log}$ be a fine noetherian log scheme over $\mathbb{F}_p$, and

$$C^{\log} \to S^{\log}$$

a *log elliptic curve* (cf. [Mzk1], Chapter III, Definition 1.1) over $S^{\log}$. Write $D \subseteq S$ for the pull-back to S of the divisor at infinity of the moduli stack of log elliptic curves, and $E \subseteq C$ for the one-dimensional semi-abelian scheme which forms an open subscheme of the semi-stable compactification C. Also, let us assume that $D \subseteq S$ forms a *Cartier divisor* in S, and that on the open dense subscheme

$$U_S \stackrel{\text{def}}{=} S \backslash D \subseteq S$$

of S, the log structure of $S^{\log}$ is *trivial.*

Since S is an $\mathbb{F}_p$-scheme, it is equipped with a *Frobenius morphism*

$$\Phi_S : S \to S$$

If n is a nonnegative integer, then we shall denote the result of base-change with respect to the n-th power of Φ_S by means of a *superscript* F^n. Note that the n-th power of the *Verschiebung morphism*

$$V_E^n : E^{F^n} \to E$$

for the group scheme $E \to S$ extends uniquely to a morphism

$$V_G^n : G_n \to C$$

satisfying the properties: (i) $V_G^n|_{U_S} = V_E^n|_{U_S}$; (ii) in a neighborhood of the divisor at infinity D, V_G^n is a finite étale covering of degree p^n.

If the *q-parameter* of the log elliptic curve $C^{\log} \to S^{\log}$ admits a *p^n-th root* at all points of D, then let us write

$$H_n \to S$$

for the semi-stable genus 1 curve over S which is equal to $E \to S$ over U_S, and, near D, is the unique minimal semi-stable model of $E|_{U_S}$ for which the closure of the p^n-torsion points of $E|_{U_S}$ lie in the smooth locus of $H_n \to S$. Then the morphism $[p^n]_E : E \to E$ given by multiplication by p^n extends to a morphism

$$[p^n]_H : H_n \to C$$

which factors

$$H_n \xrightarrow{\Phi_H^n} G_n \xrightarrow{V_G^n} C$$

Moreover, this first morphism $\Phi_H^n : H_n \to G_n$ may be identified with the n-th iterate of the relative (over S) Frobenius morphism $H_n \to H_n^{F^n}$ of H_n. Thus, in particular, G_n may be identified with $H_n^{F^n}$. Also, over U_S, this factorization is the usual factorization of $[p^n]_E : E \to E$ as the composite of the n-th iterate of Frobenius with the n-th iterate of the Verschiebung morphism.

Next, let us recall the *universal extension* of E

$$E^\dagger \to E$$

(cf. [Mzk1], Chapter III, Definition 1.2), which extends naturally to an object $E^\dagger_C \to C$ over C (cf. [Mzk1], Chapter III, Corollary 4.3). In [Mzk3], §1, we constructed (in the case of a base which is flat over $\mathbb{Z}$) an object $E^\dagger_{C,\mathrm{et}} \to C$, i.e., the *"universal extension equipped with the étale integral structure."* By reducing this object (in the case of a $\mathbb{Z}$-flat base) modulo p, we may thus also speak of $E^\dagger_{C,\mathrm{et}} \to S$ in the present context of a base S over $\mathbb{F}_p$. Moreover, in addition to this "full étale integral structure," we also constructed *"intermediate étale integral structures $E^{\dagger;\{N\}}_{C,\mathrm{et}}$* (where $N \geq 0$ is an integer) which "lie between $E^\dagger_{C,\mathrm{et}}$ and $E^\dagger_C$ and coincide with $E^\dagger_{C,\mathrm{et}}$ in relative degrees $\leq N$" — cf. the discussion at the end of [Mzk3], §4, for more details. Just as in the case of $E^\dagger_{C,\mathrm{et}}$, even though the $E^{\dagger;\{N\}}_{C,\mathrm{et}}$ were defined over $\mathbb{Z}$-flat bases, by reducing modulo p, it makes sense to speak of the $E^{\dagger;\{N\}}_{C,\mathrm{et}}$ in the present context of a base S over $\mathbb{F}_p$.

Now let us *fix an integer $n \geq 0$*. Then it follows from the construction of the étale integral structure in [Mzk3], §1, that for some *sufficiently large integer $m \geq n$* (depending on n), we have a *canonical section*

$$\kappa_{H_m} : H_m \to E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}$$

of $E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}} \to C$ over the "covering" $[p^m]_H : H_m \to C$. (Here, we assume, for the moment that the q-parameter of our log elliptic curve admits a p^m-th root at all points of D. In fact, we shall see shortly that if suffices to take m equal to n.)

Thus, if we think of the structure sheaves of the various objects which are affine over C as $\mathcal{O}_C$-algebras, then pulling back functions by κ_{H_m} defines a morphism

$$\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}} = \mathcal{O}^{<p^n}_{E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}} \to \mathcal{O}_{H_m}$$

Here the superscript "$< p^n$" denotes the functions of *"relative (or 'torsorial') degree $< p^n$"* (cf. [Mzk3], §1, for more details). We are now ready to state and prove the *main result of this* §, which is a sort of "Verschiebung-theoretic analogue" of the "Hodge-Arakelov Comparison Isomorphism" of [Mzk1]:

Theorem 1.1. (Verschiebung-Theoretic Analogue of the Hodge-Arakelov Comparison Isomorphism) *Assume that the q-parameter of the log elliptic curve $C^{\log} \to S^{\log}$ admits a p^n-th root at all points of D. Then the morphism just defined in fact factors through $\mathcal{O}_{G_n} \subseteq \mathcal{O}_{G_m} \subseteq \mathcal{O}_{H_m}$ and induces an isomorphism*

$$\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}} = \mathcal{O}^{<p^n}_{E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}} \xrightarrow{\sim} \mathcal{O}_{G_n}$$

of rank p^n vector bundles on C. In particular, the morphism $\kappa_{H_m} : H_m \to E_{C,\mathrm{et}}^{\dagger;\{p^n-1\}}$ factors as the triple composite of the morphism $\Phi_H^m : H_m \to G_m$, the natural projection $G_m \to G_n$, and a morphism

$$\kappa_{G_n} : G_n \to E_{C,\mathrm{et}}^{\dagger;\{p^n-1\}}$$

(which is necessarily unique).

Remark. In particular, in the simplest (nontrivial) case $n = 1$, we obtain an isomorphism

$$\mathcal{O}_{E_C^\dagger}^{<p} = \mathcal{O}_{E_{C,\mathrm{et}}^\dagger}^{<p} \xrightarrow{\sim} \mathcal{O}_{G_1}$$

i.e., in this case, one can define the isomorphism *without ever mentioning "étale integral structures."* Moreover, (as was pointed out to the author by M. Emerton) in this case, (if we assume, for simplicity, that $S = U_S$, then) the morphism

$$\kappa_{G_1} : G_1 = E^F \to E^\dagger$$

is the morphism defined by associating to a point of E^F (which may be thought of as a line bundle $\mathcal{L}$ of degree 0 on E^F) the *line bundle (of degree* 0*) with connection on* E (i.e., point of $E^\dagger$) given by $\Phi_E^*\mathcal{L}$ equipped with the unique connection for which sections of $\mathcal{L}$ are *horizontal.* Of course, one expects that a similar explicit description can be given for $n \geq 1$. We leave the (routine) details of working out such a description to the enthusiastic reader.

Proof. Let us first show that the morphism *factors through* $\mathcal{O}_{G_n}$, as asserted. First, note that by working in the *universal case* (where, say, S is isomorphic to a copy of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$, and the classifying morphism $S \to (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$ is given by a power of the Frobenius morphism), it suffices to show that this factorization holds *in a neighborhood of the divisor at infinity.* But in a neighborhood of infinity (where the Frobenius and Verschiebung lift naturally to mixed characteristic), the section κ_{H_m} *factors through* G_m (cf. [Mzk3], §1). Thus, we see immediately that the morphism in question maps into $\mathcal{O}_{G_m} \subseteq \mathcal{O}_{H_m}$.

Next, let us observe that (cf. the discussion of [Mzk3], §2) if we apply the base-change $G_m \to C$, it follows that the morphism in question amounts to the map given by evaluating linear combinations of the polynomials $\binom{T}{j}$ (where $j = 0, \dots, p^n - 1$) on the points given by mapping T to an element of $\mathbb{Z}/p^m\mathbb{Z}$. Thus, these polynomials define functions on the finite set $\mathbb{Z}/p^m\mathbb{Z}$. But, by Lemma 1.2 below, these functions in fact arise from functions on the quotient $\mathbb{Z}/p^m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$. Since this quotient corresponds to the intermediate covering $G_m \to G_n \to C$ (of $G_m \to C$), it thus follows that the morphism in question maps into $\mathcal{O}_{G_n} \subseteq \mathcal{O}_{G_m}$, as desired.

Note that the analysis of the preceding paragraph (cf. [Mzk3], §2) shows also that the morphism in question

$$\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}} \to \mathcal{O}_{G_n}$$

is *injective*, at least in a neighborhood of infinity. Indeed, this follows from the fact that the left- (respectively, right-) hand side of this morphism injects into the reduction modulo p of the sheaf of functions on the right- (respectively, left-) hand side of the *isomorphism*

$$\kappa^\infty_{\mathrm{et}} : E^{F^\infty} \ \stackrel{\sim}{\to}\ (E^\dagger_{\mathrm{et}})^\wedge$$

of [Mzk3], Theorem 2.2 (in such a way that the morphism in question is compatible with the isomorphism "$\stackrel{\sim}{\to}$" of *loc. cit.*).

Thus, in summary, we have a morphism

$$\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}} \to \mathcal{O}_{G_n}$$

between two vector bundles of rank p^n on C which is *generically an isomorphism* (since it is injective near infinity, and the ranks are the *same*). Now if we work in the *universal case* (i.e., where S is isomorphic to a copy of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$, and the classifying morphism $S \to (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$ is given by a power of the Frobenius morphism), then in order to conclude that this morphism is an isomorphism, it suffices to observe (since C is proper and integral over $\mathbb{F}_p$) that the *determinant bundles* of $\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}}$ and $\mathcal{O}_{G_n}$ *define the same class in* $\mathrm{Pic}_{\mathbb{Q}}(C) \stackrel{\mathrm{def}}{=} \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \mathbb{Q}$. But it is clear from the construction of $E^\dagger_{C,\mathrm{et}}$ (cf. [Mzk3], §1) that

$$[\det(\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}})] = -\sum_{j=0}^{p^n-1} j \cdot [\omega_E]$$

— where $[-]$ denotes the class of a line bundle in $\mathrm{Pic}_{\mathbb{Q}}(C)$ (thought of as an *additive group*), and ω_E denotes the line bundle on S given by the relative cotangent bundle of E over S restricted to the zero section $0_E : S \to E$.

On the other hand, let us observe that the inverse image $G_n \times_C 0_C \subseteq G_n$ of the zero section $0_C : S \to C$ of C forms a *finite flat group scheme* over S, which we shall denote by $G_n[V^n_G]$. Since the covering $G_n \to C$ is clearly a $G_n[V^n_G]$-*torsor*, we have

$$G_n \times_C G_n \cong G_n \times_S G_n[V^n_G]$$

i.e.,

$$[\det(\mathcal{O}_{G_n})]|_{G_n} = [\det(\mathcal{O}_{G_n[V^n_G]})]|_{G_n}$$

hence (by applying the morphism $\mathrm{Pic}_{\mathbb{Q}}(G_n) \to \mathrm{Pic}_{\mathbb{Q}}(C)$ given by taking norms of line bundles) we have that:

$$[\det(\mathcal{O}_{G_n})] = [\det(\mathcal{O}_{G_n[V_G^n]})]|_C$$

On the other hand, if we write $H_n[\Phi_H^n] \stackrel{\mathrm{def}}{=} H_n \times_{G_n} 0_{G_n} \subseteq H_n$ for the *kernel of the n-th iterate of Frobenius* (which is clearly a finite flat group scheme over S), then it is well-known from the elementary theory of abelian varieties (cf., e.g., [Mumf4], §14, 15) that the group schemes $H_n[\Phi_H^n]$ and $G_n[V_G^n]$ are *Cartier dual* to one another, hence that (as vector bundles over C) we have:

$$\mathcal{O}_{H_n[\Phi_H^n]} \cong (\mathcal{O}_{G_n[V_G^n]})^\vee$$

Moreover, since the Frobenius morphism is *totally inseparable* (so its fibers are all geometrically connected) it follows immediately that

$$[\det(\mathcal{O}_{H_n[\Phi_H^n]})] = \sum_{j=0}^{p^n-1} j \cdot [\omega_E]$$

hence that

$$[\det(\mathcal{O}_{G_n[V_G^n]})] = -[\det(\mathcal{O}_{H_n[\Phi_H^n]})] = -\sum_{j=0}^{p^n-1} j \cdot [\omega_E] = [\det(\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}})]$$

as desired. This completes the proof. ○

Lemma 1.2. *Let T be an indeterminate, and N a nonnegative integer $< p^n$. Write* $\mathrm{Poly}(\mathbb{Z}, \mathbb{Z}_p)$ *for the ring of $\mathbb{Z}_p$-valued polynomial functions on $\mathbb{Z}$. Then (inside* $\mathrm{Poly}(\mathbb{Z}, \mathbb{Z}_p)$*) we have:*

$$\binom{T + p^n \cdot \phi}{N} \equiv \binom{T}{N} \pmod{p}$$

for all $\phi \in \mathrm{Poly}(\mathbb{Z}, \mathbb{Z}_p)$.

Proof. Write

$$\Psi(T) \stackrel{\mathrm{def}}{=} \binom{T}{p}$$

and (for $a \geq 0$ an integer) $\Psi^a(T)$ for the result of iterating $T \mapsto \Psi(T)$ a total of a-times (cf. [Mzk3], §8.2). Thus, $\Psi^a(T)$ is a polynomial of degree p^a whose leading coefficient has the same p-adic absolute value as $\frac{1}{(p^a)!}$. Then it is well-known and easy to verify that the polynomials $\binom{T}{N}$ (for $N < p^n$) may be written as polynomials with $\mathbb{Z}_p$ coefficients in the $\Psi^a(T)$, for $a < n$. Thus, it suffices to verify that

$$\Psi^a(T + p^n \cdot \phi) \equiv \Psi^a(T) \pmod{p^{n-a}}$$

for all $\phi \in \mathrm{Poly}(\mathbb{Z}, \mathbb{Z}_p)$, $a < n$.

We use induction on a. The assertion is clear for $a = 0$. If the assertion is true for ϕ, a, then we have

$$\Psi^a(T + p^n \cdot \phi) = \Psi^a(T) + p^{n-a} \cdot \psi$$

for some $\psi \in \mathrm{Poly}(\mathbb{Z}, \mathbb{Z}_p)$. Thus, it suffices to verify that

$$\Psi(\Psi^a(T) + p^{n-a} \cdot \psi) \equiv \Psi^{a+1}(T) \pmod{p^{n-a-1}}$$

On the other hand, we have

$$\begin{aligned}
\Psi(\Psi^a(T) + p^{n-a} \cdot \psi) &= \binom{\Psi^a(T) + p^{n-a} \cdot \psi}{p} \\
&= \sum_{j=0}^{p} \binom{\Psi^a(T)}{p-j} \cdot \binom{p^{n-a} \cdot \psi}{j} \\
&= \binom{\Psi^a(T)}{p} + \sum_{j=1}^{p} \binom{\Psi^a(T)}{p-j} \cdot \binom{p^{n-a} \cdot \psi}{j} \\
&\equiv \Psi^{a+1}(T) \pmod{p^{n-a-1}}
\end{aligned}$$

(where we note that $\binom{p^{m-a} \cdot \psi}{j} \equiv 0 \pmod{p^{m-a-1}}$ for all $j = 1, \ldots, p$). This completes the proof. ○

In particular, if, in Theorem 1.1, we assume $S = U_S$ (for simplicity) and let $n \to \infty$, then we obtain a characteristic p version of [Mzk3], Theorem 2.2, which is valid *even for supersingular elliptic curves*:

Corollary 1.3. **(Explicit Description of the Étale Integral Structure of an Elliptic Curve in Positive Characteristic)** *Assume that $S = U_S$. Then the isomorphisms of Theorem 1.1 for $n \to \infty$ define an isomorphism:*

$$G_\infty \stackrel{\mathrm{def}}{=} \varprojlim_n \ G_n \ \stackrel{\sim}{\to} \ E^\dagger_{\mathrm{et}}$$

which, for ordinary elliptic curves, may be identified with the reduction modulo p of the isomorphism of [Mzk3], Theorem 2.2.

Finally, we also have the following consequence of Theorem 1.1 (obtained by restricting the isomorphism of Theorem 1.1 to the zero section 0_C of $C \to S$):

Corollary 1.4. (Explicit Description of the Structure Sheaf of the Kernel of an Iterate of the Verschiebung Morphism) *Write $G_n[V_G^n] \subseteq G_n$ for the finite flat group scheme $G_n \times_C 0_C \subseteq G_n$. Then the morphism κ_{G_n} of Theorem 1.1 defines an isomorphism*

$$\mathcal{O}^{<p^n}_{E^\dagger_{C,\mathrm{et}}}|_{0_C} = \mathcal{O}^{<p^n}_{E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}}|_{0_C} \xrightarrow{\sim} \mathcal{O}_{G_n[V_G^n]}$$

such that the filtration on the left-hand side given by relative degree over C defines a filtration on the right-hand side which is dual to the filtration on $\mathcal{O}_{H_n[\Phi_H^n]}$ (where $H_n[\Phi_H^n] \stackrel{\mathrm{def}}{=} H_n \times_{G_n} 0_{G_n} \subseteq H_n$) given by considering j-th infinitesimal neighborhoods of 0_{H_n}, for varying j.

Proof. It remains only to observe the asserted coincidence of filtrations. But this follows from the fact that the successive subquotients of both filtrations are of the form $\omega_E^{\otimes -j}$ (for some integer $j \geq 0$). Thus, any nonzero discrepancy between these two filtrations would imply the existence of a nonzero global section of a *negative power of the line bundle* ω_E over C. By working in the *universal case* (i.e., where S is isomorphic to a copy of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$, and the classifying morphism $S \to (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$ is given by a power of the Frobenius morphism), we thus see that this would imply the existence of a nonzero section of a negative power of ω_E over $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$, which is absurd since ω_E is ample on $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$. ○

Section 2: The Comparison Isomorphism in Positive Characteristic

The purpose of the present § is to present a new approach to the *Hodge-Arakelov Comparison Isomorphism* of [Mzk1], based on the characteristic p methods of §1 — cf. especially Theorem 1.1.

In this §, we maintain the notation of §1. In addition, we introduce the following notation:

$$\mathcal{C}^\dagger \stackrel{\mathrm{def}}{=} E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}; \quad \mathcal{G}^\dagger_n \stackrel{\mathrm{def}}{=} \mathcal{C}^\dagger \times_{C,V_G^n} G_n; \quad \mathcal{H}^\dagger_n \stackrel{\mathrm{def}}{=} \mathcal{G}^\dagger_n \times_{G_n,\Phi_H^n} H_n = \mathcal{C}^\dagger \times_{C,[p^n]_H} H_n$$

Thus, we have a natural commutative diagram:

$$\begin{array}{ccccc}
\mathcal{H}_n^\dagger & \longrightarrow & \mathcal{G}_n^\dagger & \longrightarrow & \mathcal{C}^\dagger \\
\downarrow & & \downarrow & & \downarrow \\
H_n & \xrightarrow{\Phi_H^n} & G_n & \xrightarrow{V_H^n} & C
\end{array}$$

(where both squares are cartesian, and we observe that the composite of the two lower horizontal arrows is the morphism $[p^n]_H : H_n \to C$ arising from multiplication by p^n). Moreover, the section $\kappa_{G_n} : G_n \to E_{C,\mathrm{et}}^{\dagger;\{p^n-1\}}$ of Theorem 1.1 defines sections

$$\kappa_{\mathcal{G}_n^\dagger} : G_n \to \mathcal{G}_n^\dagger; \quad \kappa_{\mathcal{H}_n^\dagger} : H_n \to \mathcal{H}_n^\dagger$$

that are compatible with each other and with the above commutative diagram.

Next, let us assume that we are given a *torsion point*

$$\eta_H \in H_n(S)$$

of *order* m, where $(m, p) = 1$. Write $\eta_G \in G_n(S)$ for the image of η_H in $G_n(S)$. These torsion points define *sheaves*

$$\mathcal{L}_H \stackrel{\mathrm{def}}{=} \mathcal{O}_{H_n}(p^n \cdot [\eta_H]); \quad \mathcal{L}_G \stackrel{\mathrm{def}}{=} \mathcal{O}_{G_n}([\eta_G])$$

on H_n and G_n, respectively, which are *(ample) line bundles over* U_S. Near infinity, these sheaves are only coherent, but, in fact, may in most cases be *treated as ample line bundles*, by working (in a neighborhood of infinity) with appropriate $\boldsymbol{\mu}_m$*-coverings*

$$H_n' \to H_n; \quad G_n' \to G_n$$

(i.e., coverings which induce bijections on the various irreducible components of the special fibers at infinity, and which induce the "raising to the m-th power maps" on each of the copies of $\mathbb{G}_m$ in the special fibers at infinity). These coverings have the property that the divisors $[\eta_H]$, $[\eta_G]$ become *Cartier* when pulled back via these coverings. Thus, one may think of sections of the sheaves $\mathcal{L}_H$, $\mathcal{L}_G$ over H_n, G_n, as $\boldsymbol{\mu}_m$*-invariant sections* of the resulting *(ample) line bundles* over H_n', G_n'. Note, moreover, that since $\boldsymbol{\mu}_m$ is a group scheme of *multiplicative type*, the operation of taking $\boldsymbol{\mu}_m$-invariants is *exact*.

In particular, it follows that (if, by abuse of notation, we denote all structure morphisms to S by f) the push-forward sheaves

$$f_*(\mathcal{L}_H|_{\mathcal{H}_n^\dagger}); \quad f_*(\mathcal{L}_G|_{\mathcal{G}_n^\dagger})$$

admit natural filtrations $F^r(-)$ (of ranks $r \cdot p^n$, r, respectively, for $r = 1, \dots, p^n$) whose successive subquotients $F^{r+1}/F^r(-)$ may be identified with

$$\tau_E^{\otimes r} \otimes_{\mathcal{O}_S} f_*(\mathcal{L}_H); \quad \tau_E^{\otimes r} \otimes_{\mathcal{O}_S} f_*(\mathcal{L}_G)$$

(where $\tau_E \stackrel{\mathrm{def}}{=} \omega_E^\vee$), respectively. Moreover, since Φ_H^n is *purely inseparable of degree* p^n, it follows that the divisor $(\Phi_H^n)^{-1}([\eta_G])$ is *linearly equivalent* to the divisor $p^n[\eta_H]$. This gives rise to a *natural* $H_n[\Phi_H^n]$*-action on* $\mathcal{L}_H$ (compatible with the evident $H_n[\Phi_H^n]$-action on H_n itself). Relative to this action, we have

$$f_*(\mathcal{L}_G|_{\mathcal{G}_n^\dagger}) = f_*(\mathcal{L}_H|_{\mathcal{H}_n^\dagger})^{H_n[\Phi_H^n]}$$

(where the superscript $H_n[\Phi_H^n]$ denotes "$H_n[\Phi_H^n]$-invariants").

We are now ready to define the *evaluation maps* that will appear in the comparison isomorphisms. First, we observe that by using the sections $\kappa_{\mathcal{H}_n^\dagger}$, $\kappa_{\mathcal{G}_n^\dagger}$, we may regard the group schemes

$$H_n[p^n] \subseteq H_n; \quad G_n[V_G^n] \subseteq G_n$$

(i.e., the kernels of the morphisms $[p^n]_H : H_n \to C$; $V_G^n : G_n \to C$, respectively) as being contained in $\mathcal{H}_n^\dagger$, $\mathcal{G}_n^\dagger$, respectively. Thus, restriction to these subschemes yields morphisms

$$\Xi_H : f_*(\mathcal{L}_H|_{\mathcal{H}_n^\dagger}) \to \mathcal{L}_H|_{H_n[p^n]}$$

$$\Xi_G : f_*(\mathcal{L}_G|_{\mathcal{G}_n^\dagger}) \to \mathcal{L}_G|_{G_n[V_G^n]}$$

with the property that the latter morphism is the result of applying the operation of taking $H_n[\Phi_H^n]$*-invariants* to the former.

Before proving the *comparison isomorphisms* involving these evaluation maps, we would like to discuss some technical points, as follows: First, let us note that the tautological inclusion $\mathcal{O}_{G_n} \hookrightarrow \mathcal{O}_{G_n}([\eta_G]) = \mathcal{L}_G$ defines a morphism

$$\mathcal{O}_S \to f_*(\mathcal{L}_G)$$

whose composite with the restriction morphism $f_*(\mathcal{L}_G) \to \mathcal{L}_G|_{0_G} = \mathcal{O}_S$ (where we use the fact that since the order m of η_G is *prime to* p, we have $0_G \bigcap \eta_G = \emptyset$) is the identity. In fact, it is easy to see that here, 0_G may be replayed by any p^n-torsion point, and hence that (by elementary algebraic geometry) we have the following:

Lemma 2.1. *These two morphisms are isomorphisms, i.e., we have:*

$$\mathcal{O}_S \xrightarrow{\sim} f_*(\mathcal{L}_G) \xrightarrow{\sim} \mathcal{L}_G|_\sigma = \mathcal{O}_S$$

(where $\sigma \in G_n(S)$ is any p^n-torsion point). In particular, $f_*(\mathcal{L}_G)$ is a line bundle on S of degree zero.

Next, we would like to *relate the evaluation maps constructed above to those that appear in the theory of [Mzk1].* To do this, we would like first to make the following observation concerning concerning integral structures over $\mathbb{Z}$ (or $\mathbb{Z}[\frac{1}{2}]$):

Proposition 2.2. *Let $R \stackrel{\mathrm{def}}{=} \mathbb{Z}$ if $p = 2$, $R \stackrel{\mathrm{def}}{=} \mathbb{Z}[\frac{1}{2}]$ if $p > 2$. Assume (just for the remainder of this Proposition and its proof) that S is a an R-flat scheme, and that $E \to S$ is a* **family of elliptic curves** *over S. Notation:*

(1) *Write $E^\dagger_{[p^n]} \stackrel{\mathrm{def}}{=} E^\dagger \times_{E,[p^n]_E} E$ (where $[p^n]_E : E \to E$ is multiplication by p^n) — cf. [Mzk3], §9. This object also has an "étale integral structure version" $E^\dagger_{[p^n],\mathrm{et}} \stackrel{\mathrm{def}}{=} E^\dagger_{\mathrm{et}} \times_{E,[p^n]_E} E$.*

(2) *Write $* \stackrel{\mathrm{def}}{=} \mathcal{O}_E([0_E])$; $E^*_{[p^n]} \to E$ for the* **Hodge torsor** *associated to the line bundle $\mathcal{O}_E(p^n \cdot [0_E])$ (cf. [Mzk3], §3) — i.e., the ω_E-torsor of connections on this line bundle. Note that this is compatible with the notation of [Mzk3], §9. Moreover, there is an "étale integral structure version" $E^*_{[p^n],\mathrm{et}}$ of $E^*_{[p^n]}$ (cf. [Mzk3], §9, for details).*

Then, if we think of these objects $E^\dagger_{[p^n]}$, $E^\dagger_{[p^n],\mathrm{et}}$, $E^*_{[p^n]}$, $E^*_{[p^n],\mathrm{et}}$ as being various "R-integral structures" on the object $E^\dagger \otimes_{\mathbb{Z}} \mathbb{Q}$, then the following **coincidences of R-integral structures** *hold: $E^\dagger_{[p^n]} = E^*_{[p^n]}$; $E^\dagger_{[p^n],\mathrm{et}} = E^*_{[p^n],\mathrm{et}}$.*

Proof. Indeed, by working in the universal case (i.e., over $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Z}}$), one sees that coincidences of integral structures may be verified in a formal neighborhood of infinity, i.e., in the case where

$$S \stackrel{\mathrm{def}}{=} \mathrm{Spec}(R[[q^{\frac{1}{2p^n}}]][q^{-1}])$$

and $E \to S$ is the Tate curve with q-parameter equal to q. Write $E' \to S$ for the Tate curve with q-parameter equal to $q^{\frac{1}{p^n}}$. Then, if we think of E (respectively, E') as the quotient "$\mathbb{G}_m/q^{\mathbb{Z}}$" (respectively, "$\mathbb{G}_m/q^{\frac{1}{p^n}\cdot\mathbb{Z}}$"), then the natural inclusion $\mathbb{Z} \hookrightarrow \frac{1}{p^n} \cdot \mathbb{Z}$ induces an *étale isogeny*

$$\psi : E \to E'$$

of degree p^n (i.e., the morphism $\mathbb{G}_m/q^{\mathbb{Z}} \to \mathbb{G}_m/q^{\frac{1}{p^n}\cdot\mathbb{Z}}$ covered by the identity morphism $\mathbb{G}_m \to \mathbb{G}_m$ on $\mathbb{G}_m$).

Next, let us denote by $\epsilon \in E'(S)$ the origin 0_E (respectively, the 2-torsion point defined by $q^{\frac{1}{2p^n}}$) if $p > 2$ (respectively, if $p = 2$). Then it follows easily from an elementary computation — namely, the fact that the sum of the fractions $\frac{i}{d}$ (for $i = 0, \ldots, d-1$) is equal to $\frac{1}{2d} \cdot d(d-1) = \frac{1}{2}(d-1)$ (which is $\in \mathbb{Z}$ if d is odd, and $\in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$ if d is even) — that

$$\psi^{-1}([\epsilon]) = p^n \cdot [0_E]$$

(where "$[-]$" denotes the divisor class defined by the divisor inside the brackets). Let us denote the Hodge torsor associated to ϵ by $(E')^\epsilon \to E'$. Then we have:

$$(E')^\epsilon \times_{E'} E = E^*_{[p^n]}$$

(by "functoriality of formation of Hodge torsors") and

$$(E')^\dagger \times_{E'} E = E^\dagger_{[p^n]}$$

(cf. the discussion of [Mzk3], §9). Also, similar statements hold for "étale integral structure versions."

Now we are ready to *compare integral structures*. First, let us write $\epsilon_\infty \in \mathbb{Q}$ for the invariant (associated to ϵ and) denoted by "$i_\chi/2m$" in [Mzk3], §9. Sorting through the definitions, one verifies easily that if $p = 2$ (respectively, $p > 2$):

$$\epsilon_\infty = 0 \quad \text{(respectively, } \epsilon_\infty = \frac{1}{2}\text{)}$$

— i.e., in either case, we obtain the *key fact* that $\epsilon_\infty \in R$. If we split $(E')^\dagger \to E'$ via its canonical q-adic formal splitting, and write T for the usual coordinate on the affine portion of $(E')^\dagger$ determined by the trivialization dU/U of $\omega_{E'}$ (cf. the notation of [Mzk3], §9), then the integral structure of $(E')^\epsilon$ (respectively, $(E')^\dagger$) is given by polynomials in:

$$T - \epsilon_\infty \quad \text{(respectively, } T\text{)}$$

But since $\epsilon_\infty \in R$, it follows that these two integral structures *coincide*. The étale integral structure versions are handled similarly by considering $\binom{T-\epsilon_\infty}{r}$, $\binom{T}{r}$ instead of $(T-\epsilon_\infty)^r$, T^r (for $r \geq 0$). ○

Remark. We would like to take this opportunity to correct *two misprints* in [Mzk3], §9, p. 78:

> (i) The equation on the upper half of the page following the phrase "This makes it natural to define" should read $E^\dagger_{[d],\mathrm{et}} \stackrel{\mathrm{def}}{=} E^\dagger_{\mathrm{et}} \times_{E,[d]} E$.

(ii) In the first line of Definition 9.1, the phrase "is to be" should read "to be."

Remark. Proposition 2.2 applies to the *characteristic p discussion* of the present § as follows: First of all, since the order m of η_H is *prime to p*, it follows that (at least over U_S) the Hodge torsor associated to $\mathcal{L}_H$ is naturally isomorphic (cf. [Mzk3], Proposition 3.4) to (the reduction modulo p of) the object $E^*_{[p^n]}$ appearing in Proposition 2.2. Thus, (since the object $\mathcal{H}^\dagger_n|_{U_S}$ of the present discussion is clearly the same as the reduction modulo p of the object $E^\dagger_{[p^n]}$ appearing in Proposition 2.2) Proposition 2.2 implies that:

> *The Hodge torsor associated to $\mathcal{L}_H$ is naturally isomorphic to $\mathcal{H}^\dagger_n|_{U_S}$.*

A similar statement holds for étale integral structure versions. Thus, in particular, it follows that:

> *The evaluation morphism Ξ_H constructed above may be identified with the reduction modulo p of the evaluation morphism of [Mzk1], Introduction, Theorem A.*

(cf. [Mzk3], §9, especially Theorem 9.2).

We are now ready to discuss the "characteristic p approach to the Hodge-Arakelov Comparison Isomorphism of [Mzk1]":

Theorem 2.3. (Positive Characteristic Approach to the Hodge-Arakelov Comparison Isomorphism) *Let p be a prime number; $n \geq 1$ an integer; and*

$$C^{\log} \to S^{\log}$$

a **log elliptic curve** *over a fine noetherian log scheme $S^{\log}$ in characteristic p. Write*

$$H_n \xrightarrow{\Phi^n_H} G_n \xrightarrow{V^n_G} C$$

for the factorization of the compactification $[p^n]_H : H_n \to C$ of the morphism "multiplication by p^n on E" into the n-th iterate of Frobenius, composed with the n-th iterate of the Verschiebung morphism. Also, we introduce the notation:

$$\mathcal{C}^\dagger \stackrel{\mathrm{def}}{=} E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}; \quad \mathcal{G}^\dagger_n \stackrel{\mathrm{def}}{=} \mathcal{C}^\dagger \times_{C,V^n_G} G_n; \quad \mathcal{H}^\dagger_n \stackrel{\mathrm{def}}{=} \mathcal{G}^\dagger_n \times_{G_n,\Phi^n_H} H_n = \mathcal{C}^\dagger \times_{C,[p^n]_H} H_n$$

Moreover, let us assume that we are given a **torsion point**

$$\eta_H \in H_n(S)$$

of **order** m, *where* $(m,p)=1$. *Write* $\eta_G \in G_n(S)$ *for the image of* η_H *in* $G_n(S)$, *and*

$$\mathcal{L}_H \stackrel{\mathrm{def}}{=} \mathcal{O}_{H_n}(p^n \cdot [\eta_H]); \quad \mathcal{L}_G \stackrel{\mathrm{def}}{=} \mathcal{O}_{G_n}([\eta_G])$$

for the resulting sheaves on H_n, G_n. *Then the section* $\kappa_{G_n} : G_n \to E^{\dagger;\{p^n-1\}}_{C,\mathrm{et}}$ *of Theorem 1.1 determines evaluation morphisms*

$$\Xi_H : f_*(\mathcal{L}_H|_{\mathcal{H}_n^\dagger}) \to \mathcal{L}_H|_{H_n[p^n]}$$

$$\Xi_G : f_*(\mathcal{L}_G|_{\mathcal{G}_n^\dagger}) \to \mathcal{L}_G|_{G_n[V_G^n]}$$

with the following properties:

(1) Ξ_G *is an isomorphism over* S.

(2) Ξ_H *is an isomorphism over* $U_S \stackrel{\mathrm{def}}{=} S \backslash D$.

Here, $D \subseteq S$ *is the pull-back to* S *of the divisor at infinity of the moduli stack* $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$.

Proof. First, I claim that over U_S, Ξ_G *is an isomorphism if and only if* Ξ_H *is.* Indeed, to simplify notation, let us assume (just for the remainder of this paragraph) that $U_S = S$. Then it follows that the *theta group* (cf. [Mumf1,2,3]; [Mumf4], §23; or, alternatively, [Mzk1], Chapter IV, §1, for an exposition of the theory of theta groups) $\mathcal{G}_{\mathcal{L}_H}$ of $\mathcal{L}_H$ acts on the line bundle $\mathcal{L}_H$. Since $\mathcal{L}_H$ has relative degree p^n over S, this theta group fits into an exact sequence

$$1 \to \mathbb{G}_m \to \mathcal{G}_{\mathcal{L}_H} \to E[p^n] \to 1$$

and the fact that $(\Phi^n_G)^*\mathcal{L}_G = \mathcal{L}_H$ implies that $\mathcal{L}_G$ determines a section $s_G : E[\Phi^n_E] \to \mathcal{G}_{\mathcal{L}_H}$ of this exact sequence over $E[\Phi^n_E] \subseteq E[p^n] \subseteq E$. In the terminology of theta groups, the image of s_G is a *Lagrangian subgroup* of the theta group (cf. [MB], Chapitre V, Définition 2.5.1). It thus follows from the theory of $\mathcal{G}_{\mathcal{L}_H}$-modules that the $\mathcal{G}_{\mathcal{L}_H}$-linear morphism Ξ_H is an isomorphism if and only if the morphism Ξ_G — which is obtained from Ξ_H by taking $E[\Phi^n_E]$-invariants — is an isomorphism. This completes the proof of the claim.

The fact that Ξ_G is an *isomorphism* may be proven by arguing as follows: First, we observe that it suffices to work in the *universal case*, where, say, S is *proper, connected, and smooth of dimension* 1 over $\mathbb{F}_p$, and the classifying morphism $S \to (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$ is finite. Then Ξ_G is a morphism between two vector bundles of rank p^n on S, hence it will be an isomorphism as soon as we verify the following two facts:

(1) Ξ_G is an isomorphism over the generic point of S.

(2) The degrees of the domain and range of Ξ_G coincide.

Fact (1) follows from the second Remark following Proposition 2.2, together with the *analysis in a neighborhood of infinity* given, for instance, in [Mzk1], Chapter V, Theorem 6.2 (cf. also [Mzk3], §6). Fact (2) follows from the fact that (in light of Lemma 2.1) the domain (respectively, range) of Ξ_G has the *same degree as the domain (respectively, range) of the isomorphism of Corollary 1.4.* This completes the proof that Ξ_G is an isomorphism. ○

Remark. Thus, in particular, the above argument gives a *new proof of the (scheme-theoretic) characteristic zero portion of [Mzk1], Theorem A* — at least in the case when d is a power of a prime number, and m is prime to d. More precisely, although we used the computation at infinity of [Mzk1], the characteristic p argument given above may be used to *replace the complicated degree computations* (especially when d is even!) of [Mzk1], Chapter VI, proof of Theorem 3.1. (Note that although here we are working in characteristic p, we obtain characteristic zero consequences, since any morphism between vector bundles on a flat, proper $\mathbb{Z}$-scheme which is an isomorphism modulo p is necessarily an isomorphism over $\mathbb{Q}$.) Also, we observe that, in fact:

> *The above argument furnishes a new proof of the scheme-theoretic, characteristic zero portion of the Hodge-Arakelov Comparison Isomorphism (i.e., [Mzk1], Theorem A) for arbitrary d, m (as in the statement of this Theorem).*

Indeed, this follows from the fact that the essential point of this characteristic zero portion of the theorem is a certain *coincidence of degrees* (cf. the degree computations of [Mzk1], Chapter VI, proof of Theorem 3.1). On the other hand, it is relatively easy to see (without computing the degrees precisely!) that the two degrees in question are both *polynomials in d*. Thus, their difference is a polynomial in d which vanishes (by the above characteristic p argument) for all d equal to a power of (sufficiently large) p. But this implies that this difference is *identically zero* (for all d).

Remark. One way to interpret the preceding Remark is the following:

> *The characteristic p methods (involving the Frobenius and Verschiebung morphisms) of the present paper yield a new proof of the various combinatorial identities inherent in the computation of degrees in [Mzk1], Chapter VI, proof of Theorem 3.1.*

This situation is rather reminiscent of the situation of [Mzk5], Chapter V — cf., especially, the second Remark following Corollary 1.3. Namely, in that case, as well, characteristic p methods (involving Frobenius and Verschiebung) give rise to *various nontrivial combinatorial identities*. It would be interesting if this sort of phenomenon could be understood more clearly at a conceptual level.

Remark. One interesting feature of the above proof is the crucial use of the isogeny $\Phi_H^n : H_n \to G_n$, i.e., (over U_S) the (n-th iterate of the) *Frobenius morphism* $\Phi_E^n : E \to E^{F^n}$. Put another way, this amounts to the use of the subgroup scheme $E[\Phi_E^n] \subseteq E$ (i.e., the kernel of Φ_E^n), which, of course, does not exist in characteristic zero. Note that this subgroup scheme is essentially the same as the *"multiplicative subspace"* that played an essential role in [Mzk4], §2. That is to say, it is interesting to note that just as in the context of [Mzk4] (cf., especially, §3, 4) the *crucial arithmetic object* that one wants over a number field is a *"global multiplicative subspace,"* in the above proof, the crucial arithmetic object that makes the proof work (in *positive!* characteristic) is the "global multiplicative subspace" $E[\Phi_E^n] \subseteq E$ (which is defined over all of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$).

Remark. Another interesting and key point in the above proof is the fact that, unlike the case in characteristic zero (where the structure sheaf of a finite flat group scheme on a proper curve always has degree zero):

> *In positive characteristic, the structure sheaf of a finite flat group scheme on a proper curve can have nonzero degree.*

In fact, it is precisely because of this phenomenon that in order to make the comparison isomorphism hold in characteristic zero over the proper object $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Q}}$, it is necessary to introduce *Gaussian poles* (cf., e.g., [Mzk1], Introduction, §1).

Section 3: Lagrangian Galois Actions in the 2-adic Case

In [Mzk4], §2, we assumed (for the sake of simplicity) that the prime of interest p was *odd*. In the present, §2, we would like to work out the theory of [Mzk4], §2, in the case $p = 2$. This involves dealing with various subtle technical issues modulo 2.

§3.1. Definition and Construction

Let $p = 2$. Let $d > 1$ be a *power of* 2. Let A be a *complete discrete valuation ring of mixed characteristic* $(0, p)$*, with perfect residue field*, which *contains all the* $2d$*-th roots of unity*. Write K (respectively, k) for the *quotient field* (respectively, *residue field*) of A.

Set

$$S \stackrel{\mathrm{def}}{=} \mathrm{Spec}(A[[q^{\frac{1}{N}}]])$$

for some *odd* positive integer N. Endow S with the *log structure* defined by the divisor $V(q^{\frac{1}{N}}) \subseteq S$, and denote the open subscheme of S where the log structure is trivial by $U_S \subseteq S$. Write

$$\Pi_S \stackrel{\text{def}}{=} \pi_1(U_S \otimes \mathbb{Q})$$

(for some choice of basepoint), and

$$C^{\log} \to S^{\log}$$

for the *log elliptic curve* determined by the "Tate curve," i.e., the degenerating elliptic curve $E \to S$ (more precisely: one-dimensional semi-abelian scheme) with "q-parameter" equal to $q \in \mathcal{O}_S$.

Set

$$Z \stackrel{\text{def}}{=} \text{Spec}(A[[q^{\frac{1}{2N \cdot d}}]])$$

Endow Z with the *log structure* defined by the divisor $V(q^{\frac{1}{2N \cdot d}}) \subseteq Z$. Thus, we obtain a morphism $Z^{\log} \to S^{\log}$ of log schemes.

Next, let us write

$$E_{d,Z} \to Z$$

for the object which is equal to the one-dimensional semi-abelian scheme $E_Z \stackrel{\text{def}}{=} E \times_S Z$ over $U_Z \stackrel{\text{def}}{=} U_S \times_S Z$, and, "near infinity," is the pull-back to Z of the object "E_d" (cf. [Mzk1], Chapter IV, §4, where we take "N" of *loc. cit.* to be d). In words, this object "E_d" is the result of removing the nodes from the unique regular semi-stable model of the Tate curve (with q-parameter "q") over the base $\mathbb{Z}[[q^{\frac{1}{d}}]]$. Then the object "$E^*_{[d],\text{et}} \to E$" of [Mzk3], §9, defines an object

$$E^*_{[d],\text{et},Z} \to E_{d,Z}$$

(which, over $(U_Z)_{\mathbb{Q}}$, may be identified with the *universal extension* $E^\dagger \to E$ of E) over $E_{d,Z}$. Indeed, the discussion of [Mzk3], §9, applies literally over U_Z; "near infinity," the fact that we get an object over $E_{d,Z}$ follows from the fact that the *integral structure in question*, i.e., "$\binom{d \cdot (T-(i_\chi/2m))}{r}$" (in the notation of [Mzk3], §9) is invariant with respect to the transformations $T \mapsto T + \frac{j}{d}$, $\forall j \in \mathbb{Z}$.

Next, let us observe E_Z has a *unique finite flat subgroup scheme G^μ_Z annihilated by d*. This subgroup scheme is naturally isomorphic to $\boldsymbol{\mu}_d$. Thus, we have:

$$\boldsymbol{\mu}_d \cong G^\mu_Z \subseteq E_Z[d] \subseteq E_{d,Z}$$

(where $E_Z[d] \subseteq E_{d,Z}$ denotes the closed subscheme which is the kernel of multiplication by d on $E_{d,Z}$). Note, moreover, that, in fact, G^μ_Z descends to a subscheme $G^\mu_S \subseteq E[d] \subseteq E$ over S.

Since the quotient $(E_Z[d])/G^{\mu}_Z$ is naturally isomorphic to the constant group scheme $(\mathbb{Z}/d\mathbb{Z})_Z$, it is easy to see that, over Z, *there exists a finite étale group scheme* $H_Z \subseteq E_Z[d]$ such that the natural morphism

$$G^{\mu}_Z \times_Z H_Z \to E_Z[d]$$

is an *isomorphism of group schemes.* Thus, if we write $E_{H_Z} \stackrel{\text{def}}{=} E_{d,Z}/H_Z$, then we see that $E_{H_Z} \to Z$ is a *one-dimensional semi-abelian group scheme* (i.e., its fibers are all *geometrically connected*), and that the natural quotient morphism

$$(E_Z \subseteq)\ E_{d,Z} \twoheadrightarrow E_{H_Z}$$

(over Z) has kernel equal to H_Z, hence is *finite étale of degree* d. Moreover, we note that the q-parameter of E_{H_Z} is a d-th root of q. In particular, (unlike G^{μ}_Z) H_Z is *not* defined over S.

Next, let us assume that we have been given an *odd integer* $m > 1$, together with a *torsion point*

$$\eta \in E_{\infty,S}(S_{\infty})$$

of order precisely m which defines a *metrized line bundle*

$$\overline{\mathcal{L}} \stackrel{\text{def}}{=} \overline{\mathcal{L}}_{\text{st},\eta}$$

on $E_{\infty,S}$ (cf. [Mzk1], Chapter V, §1, for a discussion of the construction of the object "$\overline{\mathcal{L}}_{\text{st},\eta}$"). Thus, in particular, over U_S:

$$\overline{\mathcal{L}}|_{U_S} = \mathcal{O}_E(d \cdot [\eta])|_{U_S}$$

Here, we recall that S_{∞} is the *stack* (in the *finite, flat topology*) obtained from S by *gluing together* U_S ("away from infinity") to the profinite covering of S ("near infinity") defined by "adjoining a compatible system of M*-th roots of the q-parameter*" (as M ranges multiplicatively over the positive integers). Over S_{∞}, we have the group object

$$E_{\infty,S} \to S_{\infty}$$

which is equal to $E \to S$ over U_S ("away from infinity"), and whose "special fiber" consists of connected components indexed by $\mathbb{Q}/\mathbb{Z}$, each of which is isomorphic to a copy of $\mathbb{G}_m$ — cf. the discussion of [Mzk1], Chapter V, §2, for more details.

Note that $\overline{\mathcal{L}}$ has an associated *theta group* (cf. [Mzk1], Chapter IV, §1, §5, for a discussion of theta groups) $\mathcal{G}_Z$ over Z which fits into an exact sequence:

$$1 \to (\mathbb{G}_m)_Z \to \mathcal{G}_Z \to E_Z[d] \to 1$$

Also, let us assume that we are given a *lifting*

$$\mathcal{H}_Z \subseteq \mathcal{G}_Z$$

of H_Z (i.e., $\mathcal{H}_Z \xrightarrow{\sim} H_Z$ via $\mathcal{G}_Z \to E_Z[d]$). Thus, $\mathcal{H}_Z$ is a "Lagrangian subgroup" (cf. [MB], Chapitre V, Définition 2.5.1) of the theta group $\mathcal{G}_Z$. In particular, we get a *natural action of* $\mathcal{H}_Z \cong H_Z$ *on* $\overline{\mathcal{L}}$.

Remark. To see that such a lifting $\mathcal{H}_Z \subseteq \mathcal{G}_Z$ exists, one may, for instance, apply the *canonical section* of [Mzk1], Chapter IV, Theorem 1.6, (1), over a *double covering* $E'_{d,Z} \to E_{d,Z}$ (so $\overline{\mathcal{L}}|_{E'_{d,Z}}$ will be a (metrized) line bundle of degree $2d$) with the property that $H_Z \subseteq E_{d,Z}$ lifts to a subgroup scheme $H'_Z \subseteq E'_{d,Z}$ such that $H'_Z \xrightarrow{\sim} H_Z$. Note that since the q-parameter of $E'_{d,Z}$ will then necessarily be a square root of q, it follows that in order to ensure that H'_Z exist, we need to know the existence of a $2d$*-th root* of q in $\mathcal{O}_Z$. This is why we defined "Z" as we did (i.e., rather than with the "$2N \cdot d$" replaced by "$N \cdot d$," as was done in the case of *odd* p).

In the following discussion, we will always denote (by abuse of notation) *structure morphisms to* S, Z, $E_{\infty,S}$ *by* f (cf. the conventions of [Mzk1]). We would like to consider the *push-forward*

$$\mathcal{V}_{\overline{\mathcal{L}}} \stackrel{\text{def}}{=} f_*(\overline{\mathcal{L}}_{E^*_{[d],\text{et},Z}})$$

of the pull-back $\overline{\mathcal{L}}_{E^*_{[d],\text{et},Z}}$ of the metrized line bundle $\overline{\mathcal{L}}$ to $E^*_{[d],\text{et},Z}$. Here, we take the integral structure of this push-forward "near infinity" to be the unique $\mathcal{G}_Z$-stable integral structure determined by the "ζ_r^{CG}" — cf. [Mzk1], Chapter V, Theorem 4.8; the discussion of [Mzk3], §4.1, 4.2. Thus, $\mathcal{V}_{\overline{\mathcal{L}}}$ is a *quasi-coherent sheaf on* Z, equipped with a *filtration* $F^r(\mathcal{V}_{\overline{\mathcal{L}}}) \subseteq \mathcal{V}_{\overline{\mathcal{L}}}$, i.e., the subsheaf consisting of sections whose "torsorial degree" is $< r$. (Here, by "torsorial degree," we mean the relative degree with respect to the structure of "relative polynomial algebra" on $\mathcal{O}_{E^\dagger}$ over $\mathcal{O}_E$ (arising from the fact that $E^\dagger \to E$ is an affine torsor). Since $E^\dagger$ may be identified with $E^*_{[d],\text{et},Z}$ over $(U_Z)_{\mathbb{Q}}$, this definition also applies to sections of $\mathcal{V}_{\overline{\mathcal{L}}}$.) In particular, we shall write

$$\mathcal{H}_{\text{DR}} \stackrel{\text{def}}{=} F^d(\mathcal{V}_{\overline{\mathcal{L}}})$$

for the object which appears in [Mzk1], Introduction, Theorem A (cf. also [Mzk3], Theorem 9.2). Thus, $\mathcal{H}_{\text{DR}}$ is a *vector bundle of rank* d *on* Z. Finally, observe that *the theta group* $\mathcal{G}_Z$ *acts naturally on* $\mathcal{V}_{\overline{\mathcal{L}}}$, $F^r(\mathcal{V}_{\overline{\mathcal{L}}})$, $\mathcal{H}_{\text{DR}}$.

Now we come to the portion of the discussion involving *phenomena unique to the prime* $p = 2$.

Proposition 3.1. *The objects introduced above satisfy the following properties:*

> *(i) The integral structure of $E^*_{[d],\mathrm{et},Z}$ is equal to that of $E^\dagger_{[d],\mathrm{et},Z} \stackrel{\mathrm{def}}{=} E^\dagger_{[d],\mathrm{et}}|_Z$ (i.e., the pull-back via the multiplication by d morphism $E_{d,Z} \to E_Z$ of the universal extension $E^\dagger_{\mathrm{et}}|_Z$ over Z equipped with the étale integral structure — cf. the notation of [Mzk3], §9). In particular, the d-torsion subgroup scheme $E_Z[d] \subseteq E_{d,Z}$* **lifts** *naturally to a subgroup scheme $E^*_Z[d] \subseteq E^*_{[d],\mathrm{et},Z}$.*
>
> *(ii) The canonical section*
>
> $$(E_Z[d] \supseteq G^\mu_Z \supseteq)\ 2 \cdot G^\mu_Z \to \mathcal{G}_Z$$
>
> *(cf. [Mzk1], Chapter IV, Theorem 1.6, (1)) extends to all of G^μ_Z. In particular, (despite the fact that d is even!) we obtain a* **theta trivialization**
>
> $$\overline{\mathcal{L}}|_{G^\mu_Z} \cong \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^\mu_Z}$$

Here, $0_{E_Z} \in E_Z(Z)$ is the zero section of $E_Z \stackrel{\mathrm{def}}{=} E \times_S Z \to Z$.

Proof. Assertion (i) follows from the fact that the integral structure used to define $E^*_{[d],\mathrm{et},Z}$ is given by "$\binom{d\cdot(T-(i_\chi/2m))}{r}$" (in the notation of [Mzk3], §9), an expression which gives the same integral structure as "$\binom{d\cdot T}{r}$." Note that here we use the assumptions that (a.) m is *odd*; (b.) $d > 1$ is *even*.

Assertion (ii) is proven by observing that, if we descend $\overline{\mathcal{L}}$ to some $\overline{\mathcal{L}}_H$ (via the lifting $\mathcal{H}_Z \subseteq \mathcal{G}_Z$ discussed above) on E_{H_Z}, the resulting degree 1 (metrized) line bundle is (up to translation by an odd order torsion point) that defined by a *nonmultiplicative* (i.e., lying outside the image of G^μ_Z in E_{H_Z}) *order* 2 *torsion point.* In particular, the invariant "$i_\chi/2m$" associated to this $\overline{\mathcal{L}}_H$ is $\in \mathbb{Z}_2$ (cf. the theory of [Mzk1], Chapter V, §4; as well as [Mzk1], Chapter IV, Lemma 5.4; the discussion of [Mzk3], §4.3). Put another way, the essential phenomenon at work here is the elementary numerical fact that (for $D \geq 1$ an integer)

$$\frac{1}{D} \sum_{j=0}^{D-1} j = \frac{1}{2}(D-1)$$

lies $\in \mathbb{Z}$ if D is *odd*, and $\in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$ if D is *even*.

On the other hand, (as one may recall from the discussion of [Mzk3], §4.3 — cf., especially, the proof of Lemma 4.1):

> The class of this invariant "$i_\chi/2m$" associated to $\overline{\mathcal{L}}_H$ in $\frac{1}{2}\mathbb{Z}_2/\mathbb{Z}_2$ is precisely the obstruction to the existence of the desired section $G^\mu_Z \to \mathcal{G}_Z$.

Thus, the fact that this invariant is $\in \mathbb{Z}_2$ implies that this obstruction is 0, as desired. ○

Remark. The description of $\overline{\mathcal{L}}_H$ given in the above proof shows that in fact, this (a priori) *metrized* line bundle is defined as an *ordinary line bundle* over some semi-stable model of $E_{H_Z} = E_{d,Z}/H_Z$ over Z. (More precisely, the semi-stable model with the property that the group of irreducible components of its special fiber is equal to $\frac{1}{2N}\mathbb{Z}/\mathbb{Z}$ is sufficient.) In particular, it follows that $\overline{\mathcal{L}}$ (respectively, $\mathcal{V}_{\overline{\mathcal{L}}}$) is defined as an *"ordinary line bundle"* (respectively, *"ordinary vector bundle"*) over some semi-stable model of $E_Z \to Z$ (respectively, over Z).

Next, let us note that since $\overline{\mathcal{L}}$ is defined over $E_{\infty,S}$ (i.e., without base-changing to Z), it follows that $\overline{\mathcal{L}}|_{0_{E_Z}}$ is, in fact, *defined over* S_∞ (i.e., in other words, it is defined over S, except that "near infinity," one may need to adjoin roots of the q-parameter). In particular, it follows that *there is a natural action of* $\mathrm{Gal}(Z/S)$ *— hence of* Π_S *(via the surjection* $\Pi_S \twoheadrightarrow \mathrm{Gal}(Z/S)$*) — on* $\overline{\mathcal{L}}_{0_{E_Z}}$.

Let us denote H_Z*-invariants* by means of a superscript H_Z. Then recall that $\mathcal{V}_{\overline{\mathcal{L}}}^{H_Z}$ admits the following interpretation: Since $\mathcal{H}_Z \cong H_Z$ acts on $E_{d,Z}$; $E_{\infty,S}$; $E^*_{[d],\mathrm{et},Z}$; $\overline{\mathcal{L}}$, we may form the *quotients* of these objects by this action. This yields objects $(E_{d,Z})_H$ (i.e., E_{H_Z}), $(E_{\infty,S})_H$, $(E^*_{[d],\mathrm{et},Z})_H$, $\overline{\mathcal{L}}_H$ (a metrized line bundle on $(E_{\infty,S})_H$). Then we have:

$$\mathcal{V}_{\overline{\mathcal{L}}}^{H_Z} = f_*\{\overline{\mathcal{L}}_H|_{(E^*_{[d],\mathrm{et},Z})_H}\}$$

(where f as usual denotes the structure morphism to Z) — cf., e.g., [Mzk1], Chapter IV, Theorem 1.4.

Thus, by restricting H_Z-invariant sections of $\overline{\mathcal{L}}$ over $E^*_{[d],\mathrm{et},Z}$ — i.e., sections of $\overline{\mathcal{L}}_H$ over $(E^*_{[d],\mathrm{et},Z})_H$ — to $G^\mu_Z \subseteq E_Z[d] \cong E^*_Z[d] \subseteq E^*_{[d],\mathrm{et},Z}$, and composing with the theta trivialization of Proposition 3.1, (ii), we obtain a morphism:

$$\Xi_{\mathcal{V}}^{H_Z} : \mathcal{V}_{\overline{\mathcal{L}}}^{H_Z} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^\mu_Z}$$

Similarly, if we introduce *Gaussian poles* (cf. [Mzk1], Introduction, Theorem A, (3); [Mzk3], Theorem 6.2), we get a morphism:

$$\Xi_{\mathcal{H}}^{\mathrm{GP},H_Z} : \mathcal{H}_{\mathrm{DR}}^{\mathrm{GP},H_Z} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^\mu_Z}$$

Then the main result of [Mzk1] may be summarized as follows:

Corollary 3.2. (Lagrangian Version of the Main Result of [Mzk1]) *Assume that d is a power of $p = 2$, and that m is* **odd**. *Then restriction of H_Z-invariant sections of $\mathcal{V}_{\overline{\mathcal{L}}}$ to G^μ_Z gives rise to a morphism*

$$\Xi_{\mathcal{V}}^{H_Z} : \mathcal{V}_{\overline{\mathcal{L}}}^{H_Z} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^\mu_Z}$$

whose restriction

$$\Xi^{H_Z}_{\mathcal{H}} : \mathcal{H}^{H_Z}_{\mathrm{DR}} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^{\mu}_Z}$$

to $\mathcal{H}^{H_Z}_{\mathrm{DR}} \stackrel{\mathrm{def}}{=} F^d(\mathcal{V}^{H_Z}_{\overline{\mathcal{L}}}) \subseteq \mathcal{V}^{H_Z}_{\overline{\mathcal{L}}}$ *satisfies: (i)* $\Xi^{H_Z}_{\mathcal{H}}$ *is an isomorphism over* U_Z*; (ii) if one introduces* **Gaussian poles***, i.e., if one considers*

$$\Xi^{\mathrm{GP},H_Z}_{\mathcal{H}} : \mathcal{H}^{\mathrm{GP},H_Z}_{\mathrm{DR}} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^{\mu}_Z}$$

then $\Xi^{\mathrm{GP},H_Z}_{\mathcal{H}}$ *is an isomorphism over* Z.

Proof. This Corollary is a special case of [Mzk1], Introduction, Theorem A, (2), (3). Note that the "zero locus of the determinant" is empty because of our assumption that m is *odd* (hence invertible on S). ◯

Definition 3.3. The natural action of Π_S on G^{μ}_Z, together with the isomorphism $\Xi^{\mathrm{GP},H_Z}_{\mathcal{H}}$ of Corollary 2.2, and the natural action of Π_S on $\overline{\mathcal{L}}|_{0_{E_Z}}$, define a natural action of Π_S on $\mathcal{H}^{\mathrm{GP},H_Z}_{\mathrm{DR}}$, which we shall refer to as the *Lagrangian Galois action on* $\mathcal{H}^{\mathrm{GP},H_Z}_{\mathrm{DR}}$.

Remark. Just as in [Mzk4], §2.1, (unlike the "naive" Galois action) the Lagrangian Galois action *depends on the choice of the additional data* G^{μ}_Z, H_Z. Also, just as in [Mzk4], §2.1, although *a priori*, the Lagrangian Galois action appears to require the *Gaussian poles* (i.e., it appears that it is not necessarily *integrally* defined on $\mathcal{H}^{H_Z}_{\mathrm{DR}}$), in fact, however, we shall see in §3.2 below that *the Lagrangian Galois action has the remarkable property that it is defined without introducing the Gaussian poles.*

§3.2. Crystalline Properties

We maintain the notation of §3.1.

The first portion of [Mzk4], §2.2, now goes through with little change: As in *loc. cit.*, we first would like to *relate the present discussion to the theory of connections in [Mzk3].* Thus, recall that $\overline{\mathcal{L}}|_{0_{E_Z}}$ is a *line bundle on* Z *equipped with a natural* Π_S*-action* derived from a *trivialization*

$$\tau : \overline{\mathcal{L}}|_{0_{E_Z}} \cong q^{-\frac{a}{2N\cdot d}} \cdot \mathcal{O}_Z$$

(where a is a nonnegative integer $< 2Nd$) — which, in the terminology of the discussion of [Mzk3], §5, determines a Π_S*-equivariant rigidification* τ of $\overline{\mathcal{L}}$ at 0_{E_Z}. In particular, τ defines a Π_S*-invariant logarithmic connection* on the line bundle $\overline{\mathcal{L}}|_{0_{E_Z}}$. Thus, by the theory of [Mzk3], §5, this rigidification gives rise to a Π_S-*invariant (logarithmic) connection*

$$\nabla_{\mathcal{V}^{H_Z}_{\overline{\mathcal{L}}}}$$

on $\mathcal{V}_{\mathcal{L}}^{H_Z}$ (cf. [Mzk3], Theorems 5.2, 8.1). Here, the logarithmic connections are relative to the log structure of $Z^{\log}$, and all connections, differentials, etc., are to be understood as being continuous with respect to the (p, q)-adic topology on $\mathcal{O}_Z$.

Just as in [Mzk4], §2.2, since *all higher p-curvatures of these connections vanish* (cf. [Mzk3], §7.1, for a discussion of the general theory of higher p-curvatures; [Mzk3], Corollary 7.6, for the vanishing result just quoted), we thus conclude that the pair

$$(\mathcal{V}_{\mathcal{L}}^{H_Z}, \nabla_{\mathcal{V}_{\mathcal{L}}^{H_Z}})$$

defines a *crystal* on the site

$$\mathrm{Inf}(Z^{\log} \otimes k/A)$$

of (*all* — i.e., not just PD-) *infinitesimal thickenings over A of open sub-log schemes of $Z^{\log} \otimes k = Z^{\log} \otimes (A/\mathfrak{m}_A)$.*

One verifies immediately (using the simple explicit structures of S, Z) that the action of Π_S on $\mathcal{O}_Z$ satisfies:

$$\sigma(\phi) \equiv \phi \pmod{\mathfrak{m}_A \cdot \mathcal{O}_Z}$$

$\forall \sigma \in \Pi_S, \phi \in \mathcal{O}_Z$, and that the correspondence

$$\Pi_S \ni \sigma \mapsto \sigma(q^{\frac{1}{2N \cdot d}})/q^{\frac{1}{2N \cdot d}}$$

defines morphisms:

$$\Pi_S \twoheadrightarrow \mathrm{Gal}(Z/S) \xrightarrow{\sim} (\mathbb{Z}/2d\mathbb{Z})(1)$$

(where the first (respectively, second) arrow is a surjection (respectively, isomorphism)).

Next, let us observe that the property just discussed concerning the action of Π_S on $\mathcal{O}_Z$ implies that every $\sigma \in \Pi_S$ defines an *A-linear isomorphism*

$$\sigma: \ Z^{\log} \xrightarrow{\sim} Z^{\log}$$

which is the identity on $Z^{\log} \otimes k$. It thus follows from:

(i) the fact that $Z^{\log}$ defines a(n) (inductive system of) thickening(s) in the category $\mathrm{Inf}(Z^{\log} \otimes k/A)$; and

(ii) the fact that $(\mathcal{V}_{\mathcal{L}}^{H_Z}, \nabla_{\mathcal{V}_{\mathcal{L}}^{H_Z}})$ forms a crystal on $\mathrm{Inf}(Z^{\log} \otimes k/A)$

that σ induces a *σ-semi-linear isomorphism*

$$\int_\sigma : \widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z} \to \widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z}$$

(where "σ-semi-linear" means semi-linear with respect to the action of σ on $\mathcal{O}_Z$, and the "hat" denotes p-adic completion).

As in [Mzk4], §2.2, the justification for the notation "$\int_\sigma$" is that this isomorphism is the analogue of the isomorphism obtained in differential geometry by "parallel transporting" — i.e., *"integrating"* — sections of $\widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z}$ along the "path" σ (where we think of σ as an "element of the (algebraic) fundamental group" Π_S). That is to say, we obtain a *natural* Π_S*-semi-linear action of* Π_S *on* $\widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z}$.

Theorem 3.4. (Crystalline Nature of the Lagrangian Galois Action) *The action of* Π_S *on* $\widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z}$ *is compatible with* $\Xi_{\widehat{\mathcal{V}}}^{H_Z}$ *(cf. Corollary 3.2; here the "hat" denotes p-adic completion) and the natural action of* Π_S *on* G_Z^μ *in the following sense: For* $\sigma \in \Pi_S$*, the following diagram commutes:*

$$\begin{array}{ccc} \widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z} & \stackrel{\Xi_{\widehat{\mathcal{V}}}^{H_Z}}{\longrightarrow} & \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G_Z^\mu} \\ \Big\downarrow \int_\sigma & & \Big\downarrow \sigma \\ \widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z} & \stackrel{\Xi_{\widehat{\mathcal{V}}}^{H_Z}}{\longrightarrow} & \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G_Z^\mu} \end{array}$$

(where the σ *on the right denotes the result of applying* σ *to* $\mathcal{O}_{G_Z^\mu}$ *via the natural action of* Π_S *on* $\mathcal{O}_{G_Z^\mu}$*).*

Proof. As in [Mzk4], §2.2, this follows from the naturality of all the morphisms involved, together with the compatibility (cf. [Mzk3], Theorem 6.1) over G_Z^μ of the connection $\nabla_{\mathcal{V}_{\underline{\mathcal{L}}}^{H_Z}}$ with the "theta trivialization" of Proposition 3.1, (ii). ○

Corollary 3.5. (Absence of Gaussian Poles in the Lagrangian Galois Action) *Relative to the objects of the present discussion, the Lagrangian Galois action of* Π_S *on* $\mathcal{H}_{\mathrm{DR}}^{\mathrm{GP},H_Z}$ *(cf. Definition 3.3) is defined* **without Gaussian poles***, i.e., it arises from an action of* Π_S *on* $\mathcal{H}_{\mathrm{DR}}^{H_Z}$*.*

Proof. As in [Mzk4], §2.2, this follows formally from the commutative diagram of Theorem 3.4, together with Lemma 3.6 below. ○

Lemma 3.6. *The image of the morphism* $\Xi_{\widehat{\mathcal{V}}}^{H_Z}$ *(cf. Corollary 3.2) is the same as the image of its restriction* $\Xi_{\mathcal{H}}^{H_Z}$ *to* $\mathcal{H}_{\mathrm{DR}}^{H_Z} \subseteq \widehat{\mathcal{V}}_{\underline{\mathcal{L}}}^{H_Z}$*.*

Proof. The proof is entirely similar to that of [Mzk4], §2.2, Lemma 2.6. ○

Finally, just as in [Mzk4], §2.2, we observe that:

> *Theorem 3.4 allows us to relate the "arithmetic Kodaira-Spencer morphism" arising from the Lagrangian Galois action to the classical geometric Kodaira-Spencer morphism.*

The argument in the case $p = 2$, however, *differs somewhat* from the case of odd p.

We begin as in [Mzk4], §2.2. Let

$$\Gamma \subseteq \mathrm{Gal}(Z/S)$$

be a *subgroup of order* > 1. Write $d_\Gamma \stackrel{\mathrm{def}}{=} |\Gamma|$ for the order of Γ. Thus, $d_\Gamma \neq 1$ divides $2d$, and we have a *natural isomorphism* $\Gamma \cong (\mathbb{Z}/d_\Gamma\mathbb{Z})(1)$. Write

$$(p \cdot A \subseteq) \;\; \mathfrak{m}_\Gamma \;\; \subsetneq A$$

for the ideal generated by elements of the form $1 - \zeta$, where ζ is a d_Γ-th root of unity. Note that Γ *acts trivially on* $Z \otimes (A/\mathfrak{m}_\Gamma) \pmod{\mathfrak{m}_\Gamma}$. Moreover, we have a *homomorphism*

$$\lambda_\Gamma : \boldsymbol{\mu}_{d_\Gamma}(A) \to \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

given by $\zeta \mapsto \zeta - 1 \pmod{\mathfrak{m}_\Gamma^2}$. Thus, if we think of $\boldsymbol{\mu}_{d_\Gamma}(A)$ as "$(\mathbb{Z}/d_\Gamma\mathbb{Z})(1)$" (which is naturally isomorphic to Γ), then we see that λ_Γ defines a homomorphism

$$\delta_\Gamma : \Gamma \to \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

which is easily seen (by the definition of the ideal $\mathfrak{m}_\Gamma$) to induce an *injection* $\Gamma \otimes (\mathbb{Z}/p\mathbb{Z}) \hookrightarrow \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$.

Next, as in [Mzk4], §2.2, we would like to consider a *"certain crucial portion" of the "arithmetic Kodaira-Spencer morphism" associated to the Lagrangian Galois action*. Ultimately, however, this crucial portion in the case of $p = 2$ will *differ* somewhat from the crucial portion in the case of p odd.

Let $\gamma \in \Gamma$. Then since γ acts on $\mathcal{H}_{\mathrm{DR}}^{H_Z}$ via the Lagrangian Galois action (Definition 3.3, Corollary 3.5), we see that γ defines a morphism $\mathcal{H}_{\mathrm{DR}}^{H_Z} \to \mathcal{H}_{\mathrm{DR}}^{H_Z}$. If we *restrict this morphism to* $F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z})$, and *compose with the surjection* $\mathcal{H}_{\mathrm{DR}}^{H_Z} \twoheadrightarrow \{\mathcal{H}_{\mathrm{DR}}^{H_Z}/F^2(\mathcal{H}_{\mathrm{DR}}^{H_Z})\} \otimes_A (A/\mathfrak{m}_\Gamma^2)$, we thus obtain a morphism

$$F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \to \{\mathcal{H}_{\mathrm{DR}}^{H_Z}/F^2(\mathcal{H}_{\mathrm{DR}}^{H_Z})\} \otimes_A (A/\mathfrak{m}_\Gamma^2)$$

which, as in [Mzk4], §2.2, defines a morphism

$$F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes k \to \{(F^3/F^2)(\mathcal{H}_{\mathrm{DR}}^{H_Z})\} \otimes_A \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2 = \frac{1}{2} \cdot F^1(\mathcal{V}_{\overline{\mathcal{L}}}^{H_Z}) \otimes \tau_{E_{H_Z}}^{\otimes 2} \otimes_A \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

i.e., we get a section $\in \frac{1}{2} \cdot \tau_{E_{H_Z}}^{\otimes 2} \otimes_A \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$. Just as in [Mzk4], §2.2, this section describes how the *moduli of* E_{H_Z} *are affected modulo* $\mathfrak{m}_\Gamma^2$ by the action of γ — i.e., (up to the factor of $\frac{1}{2}$) it is the *usual Kodaira-Spencer morphism* (cf. [Mzk3], Theorem 8.1) of the family $E_{H_Z} \to Z$. On the other hand, since the q-parameter of E_{H_Z} is equal (up to multiplication by a $2d$-root of unity) to

$$q^{\frac{1}{d}} = (q^{\frac{1}{2N \cdot d}})^{2N}$$

if follows that the effect of γ on the moduli of E_{H_Z} may be computed as follows:

$$\gamma(q^{\frac{1}{2N \cdot d}}) \equiv q^{\frac{1}{2N \cdot d}} + \delta_\Gamma(\gamma) \cdot q^{\frac{1}{2N \cdot d}} \pmod{\mathfrak{m}_\Gamma^2}$$

hence

$$\gamma(q^{\frac{1}{d}}) \equiv q^{\frac{1}{d}} + 2N \cdot \delta_\Gamma(\gamma) \cdot q^{\frac{1}{d}} \equiv q^{\frac{1}{d}} \pmod{\mathfrak{m}_\Gamma^2}$$

i.e., the moduli of E_{H_Z} are *unaffected by* γ. In particular, we see that the morphism $F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \to \{\mathcal{H}_{\mathrm{DR}}^{H_Z}/F^2(\mathcal{H}_{\mathrm{DR}}^{H_Z})\} \otimes_A (A/\mathfrak{m}_\Gamma^2)$ considered above is *identically zero*.

Thus, in summary, we see that, in the present context, *the action of* γ *determines a morphism*

$$\kappa_\gamma : F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes k \to \{(F^2/F^1)(\mathcal{H}_{\mathrm{DR}}^{H_Z})\} \otimes_A \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2 = F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes \tau_{E_{H_Z}} \otimes_A \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

i.e., by letting γ *vary* (as in [Mzk4], §2.2), we obtain a homomorphism:

$$\kappa_\Gamma : \Gamma \to \mathrm{Hom}_{\mathcal{O}_Z}(F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes k, (F^2/F^1)(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) = \tau_{E_{H_Z}} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

arising from the *Lagrangian Galois action, taken modulo* $\mathfrak{m}_\Gamma^2$. If we regard κ_Γ as an element

$$\kappa_\Gamma \in \mathrm{Hom}(\Gamma, \tau_{E_{H_Z}} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) = \mathrm{Hom}(\Gamma, \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) \otimes \tau_{E_{H_Z}}$$

then it follows immediately from the discussion (in terms of deformations) of *Griffiths semi-transversality* in [Mzk3], §8.1 (specialized to the case where the moduli of the elliptic curve do not vary) that κ_Γ *may be identified* with the result of evaluating the *"geometric Kodaira-Spencer morphism of the line bundle* $\overline{\mathcal{L}}_H$*"*

$$\kappa_{\overline{\mathcal{L}}_H} : (\Omega_{Z^{\log}/A})^\vee \to \tau_{E_{H_Z}}$$

(i.e., the morphism that describes the variation in the moduli of this line bundle) on $\frac{\partial}{\partial \log(q^{\frac{1}{2N \cdot d}})} \in (\Omega_{Z^{\log}/A})^\vee$ and (as in [Mzk4], §2.2) multiplying the result by δ_Γ.

Moreover, since the line bundle $\overline{\mathcal{L}}_H$ is defined by some *torsion point* (cf. the proof of Proposition 3.1, together with the Remark following this proposition), i.e., if we think of E_{H_Z} as "$\mathbb{G}_m/q^{\frac{1}{d}\mathbb{Z}}$," the point defined by some

$$\zeta \cdot q^{\frac{a_1}{2a_2 \cdot d}}$$

(where $a_1, a_2 \in \mathbb{Z}$ are relatively prime and *odd*), we conclude that *the effect of the action of* γ *on the moduli of* $\overline{\mathcal{L}}_H$ *is given by*

$$\gamma(q^{\frac{\alpha}{2\cdot d}}) \equiv q^{\frac{\alpha}{2\cdot d}} + (\alpha \cdot N) \cdot \delta_\Gamma(\gamma) \cdot q^{\frac{\alpha}{2\cdot d}} \equiv q^{\frac{\alpha}{2\cdot d}} \cdot \{1 + \delta_\Gamma(\gamma)\} \pmod{\mathfrak{m}_\Gamma^2}$$

(where $\alpha \stackrel{\text{def}}{=} a_1/a_2$, and, in the second congruence, we use the fact that a_1, a_2, and N are odd).

We summarize this discussion as follows:

Corollary 3.7. (Relation to the Classical Geometric Kodaira-Spencer Morphism) *Let*

$$\Gamma \subseteq \text{Gal}(Z/S)$$

be a **subgroup of order** > 1*. This subgroup* Γ *gives rise to a natural ideal* $\mathfrak{m}_\Gamma \subseteq A$ *(minimal among ideals modulo which* Γ *acts trivially on* $Z^{\log}$*) and a natural morphism*

$$\delta_\Gamma : \Gamma \to \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

(defined by considering the action of Γ *on* $q^{\frac{1}{2N\cdot d}}$ *modulo* $\mathfrak{m}_\Gamma^2$*). Then the morphism*

$$\kappa_\Gamma : \Gamma \to \text{Hom}_{\mathcal{O}_Z}(F^1(\mathcal{H}_{\text{DR}}^{H_Z}) \otimes k, (F^2/F^1)(\mathcal{H}_{\text{DR}}^{H_Z}) \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) = \tau_{E_{H_Z}} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

obtained purely from the **Lagrangian Galois action** *of* Γ *on* $\mathcal{H}_{\text{DR}}^{H_Z}$ *(cf. Definition 3.3, Corollary 3.5) by restricting this action to* $F^1(\mathcal{H}_{\text{DR}}^{H_Z})$ *and then reducing modulo* $\mathfrak{m}_\Gamma^2$ **coincides** *with the morphism obtained by evaluating the* **"geometric Kodaira-Spencer morphism of the line bundle $\overline{\mathcal{L}}_H$ on E_{H_Z}"**

$$\kappa_{\overline{\mathcal{L}}_H} : (\Omega_{Z^{\log}/A})^\vee \to \tau_{E_{H_Z}}$$

in the logarithmic tangent direction $\frac{\partial}{\partial \log(q^{\frac{1}{2N\cdot d}})} \in (\Omega_{Z^{\log}/A})^\vee$ *and multiplying the result by* δ_Γ*.*

Moreover, if we trivialize $(\Omega_{Z^{\log}/A})^{\vee}$ *via this logarithmic tangent direction and* $\tau_{E_{H_Z}}$ *via the logarithmic tangent direction* $\frac{\partial}{\partial U}$ *(where* U *is the standard multiplicative coordinate on the copy of* $\mathbb{G}_m$ *that naturally uniformizes* E_{H_Z}*), then* $\kappa_{\overline{\mathcal{L}}_H}$ *is the* **identity morphism** *modulo* $\mathfrak{m}_\Gamma$*.*

Thus, in summary, the **arithmetic Kodaira-Spencer morphism** *associated to the Lagrangian Galois action in the case* $p = 2$ *coincides modulo* $\mathfrak{m}_\Gamma^2$ *with the* **usual geometric Kodaira-Spencer morphism of the ample line bundle under consideration***.*

Remark. Just as in [Mzk4], §2.2, the correspondence between the logarithmic tangent direction $\frac{\partial}{\partial \log(q^{\frac{1}{2N\cdot d}})} \in (\Omega_{Z^{\log}/A})^{\vee}$ and the morphism δ_Γ is essentially the same as the correspondence arising from Faltings' theory of almost étale extensions between the logarithmic tangent bundle of $Z^{\log}$ and a certain Galois cohomology group (cf., e.g., [Mzk1], Chapter IX, §2, especially Theorem 2.6, for more details).

Bibliography

[MB] L. Moret-Bailly, *Pinceaux de variétés abéliennes*, *Astérisque* **129**, Soc. Math. France (1985).

[Mumf1,2,3] D. Mumford, On the equations defining abelian varieties I, II, III, *Invent. Math.* **1** (1966), pp. 287-354; **2** (1967), pp. 71-135; **3** (1967), pp. 215-244.

[Mumf4] D. Mumford, *Abelian Varieties*, Oxford Univ. Press (1974).

[Mzk1] S. Mochizuki, *The Hodge-Arakelov Theory of Elliptic Curves: Global Discretization of Local Hodge Theories*, RIMS Preprint Nos. 1255, 1256 (October 1999).

[Mzk2] S. Mochizuki, *The Scheme-Theoretic Theta Convolution*, RIMS Preprint No. 1257 (October 1999).

[Mzk3] S. Mochizuki, *Connections and Related Integral Structures on the Universal Extension of an Elliptic Curve*, RIMS Preprint No. 1279 (May 2000).

[Mzk4] S. Mochizuki, *The Galois-Theoretic Kodaira-Spencer Morphism of an Elliptic Curve*, RIMS Preprint No. 1287 (July 2000).

[Mzk5] S. Mochizuki, *Foundations of p-adic Teichmüller Theory*, AMS/IP Studies in Advanced Mathematics **11**, American Mathematical Society/International Press (1999).