Advanced Studies in Pure Mathematics 36, 2002
Algebraic Geometry 2000, Azumino
pp. 81–114

A Survey of the Hodge-Arakelov Theory of Elliptic Curves II

Shinichi Mochizuki [1]

Abstract.

The purpose of the present manuscript is to continue the survey of the *Hodge-Arakelov theory of elliptic curves* (cf. [7], [8], [9], [10], [11]) that was begun in [12]. This theory is a sort of "Hodge theory of elliptic curves" analogous to the classical *complex and p-adic* Hodge theories, but which exists in the *global arithmetic framework of Arakelov theory.* In particular, in the present manuscript, we focus on the aspects of the theory (cf. [9], [10], [11]) developed subsequent to those discussed in [12], but prior to the conference "Algebraic Geometry 2000" held in Nagano, Japan, in July 2000. These developments center around the natural connection that exists on the pair consisting of the *universal extension of an elliptic curve*, equipped with an *ample line bundle.* This connection gives rise to a natural object — which we call the *crystalline theta object* — which exhibits many interesting and unexpected properties. These properties allow one, in particular, to understand at a rigorous mathematical level the (hitherto purely "philosophical") relationship between the classical Kodaira-Spencer morphism and the Galois-theoretic *"arithmetic Kodaira-Spencer morphism"* of Hodge-Arakelov theory. They also provide a method (under certain conditions) for *"eliminating the Gaussian poles,"* which are the main obstruction to applying Hodge-Arakelov theory to diophantine geometry. Finally, these techniques allow one to give a new proof of the main result of [7] using *characteristic p methods.* It is the hope of the author to survey more recent developments (i.e., developments that occurred subsequent to "Algebraic Geometry 2000") in a sequel to the present manuscript.

Received January 22, 2001.

2000 *Mathematics Subject Classification*: Primary 14H52; Secondary 14H25. Keywords: elliptic curve, universal extension, Kodaira-Spencer morphism, Hodge Theory, crystalline, theta function, Galois action, Frobenius morphism, Verschiebung morphism.

[1] Part of the research discussed in this manuscript was carried out while the author was visiting the University of Tokyo during the Spring of 2000 as a "Clay Prize Fellow" supported by the Clay Mathematical Institute.

CONTENTS

§1. General Introduction

We begin our general introduction to the topics presented in the present manuscript by reviewing the *fundamental argument from algebraic geometry* whose *arithmetic analogue* is the central goal of the Hodge-Arakelov theory of elliptic curves.

Let S be a *smooth, proper, geometrically connected algebraic curve* over an *algebraically closed field of characteristic zero* k. Let

$$E \to S$$

be a *family of one-dimensional semi-abelian varieties* whose generic fiber is *proper*. Thus, (except for a finite number of exceptions) the fibers of $E \to S$ are *elliptic curves*. Let us write

$$\Sigma \subseteq S$$

for the finite set of points over which the fiber of $E \to S$ fails to be an elliptic curve, and

$$\omega_E \stackrel{\text{def}}{=} \Omega_{E/S}|_{0_E}$$

for the restriction of the sheaf of relative differentials to the zero section of $E \to S$. Then the *height* of the family $E \to S$ is defined to be:

$$\text{ht}_E \stackrel{\text{def}}{=} \deg_S(\omega_E^{\otimes 2})$$

(i.e., the degree on S of the line bundle in parentheses). The height is a measure of the *arithmetic complexity* of the family $E \to S$. For instance, the family is *isotrivial* (i.e., becomes trivial upon applying some finite flat base extension $T \to S$) if and only if $\text{ht}_E = 0$.

In some sense, the most important property of the height in this context is the fact that (in the nonisotrivial case) it is *universally bounded* by invariants depending only on the pair (S, Σ). This bound — *"Szpiro's conjecture for function fields"* — is as follows:

$$\text{(1)} \qquad \mathrm{ht}_E \leq 2g_S - 2 + |\Sigma|$$

(where g_S is the genus of S, and $|\Sigma|$ is the cardinality of Σ). The proof, in the present geometric context, is the following simple argument: Write $\overline{\mathcal{M}}_{\mathrm{ell}}$ for the *compactified moduli stack of elliptic curves over* k, and $\infty \subseteq \overline{\mathcal{M}}_{\mathrm{ell}}$ for the divisor at infinity of this stack. Thus, $E \to S$ defines a *classifying morphism*

$$\kappa : S \to \overline{\mathcal{M}}_{\mathrm{ell}}$$

whose (logarithmic) *derivative*

$$d\kappa : \omega_E^{\otimes 2} \cong \kappa^* \Omega_{\overline{\mathcal{M}}_{\mathrm{ell}}/k}(\infty) \to \Omega_S(\Sigma)$$

is *nonzero* (so long as we assume that the family $E \to S$ is nonisotrivial). Thus, since $d\kappa$ is a generically nonzero morphism between line bundles on the curve S, the degree of its domain (i.e., ht_E) is $\leq$ the degree of its range (i.e., $2g_S - 2 + |\Sigma|$), so we obtain the desired inequality.

Note that in the above argument, the most essential ingredient is the *Kodaira-Spencer morphism*, i.e., the *derivative* $d\kappa$. Until recently, no analogue of such a derivative existed in the "arithmetic case" (i.e., of elliptic curves over number fields). On the other hand:

> *The Hodge-Arakelov theory of elliptic curves gives rise to a natural analogue of the Kodaira-Spencer morphism in the arithmetic context of an elliptic curve over a number field.*

A survey of the basic theory of this arithmetic Kodaira-Spencer morphism, together with a detailed explanation of the sense in which it may be regarded as being analogous to the classical geometric Kodaira-Spencer morphism, may be found in [12].

At a more technical level, in some sense the most *fundamental result* of Hodge-Arakelov theory is the following: Let E be an *elliptic curve over a field* K *of characteristic zero*. Let d be a positive integer, and $\eta \in E(K)$ a torsion point of order not dividing d. Write

$$\mathcal{L} \stackrel{\mathrm{def}}{=} \mathcal{O}_E(d \cdot [\eta])$$

for the line bundle on E corresponding to the divisor of multiplicity d with support at the point η. Write

$$E^\dagger \to E$$

for the *universal extension of the elliptic curve*, i.e., *the moduli space of pairs* $(\mathcal{M}, \nabla_{\mathcal{M}})$ *consisting of a degree zero line bundle* $\mathcal{M}$ *on* E, *equipped with a connection* $\nabla_{\mathcal{M}}$. Thus, $E^{\dagger}$ is an affine torsor on E under the module ω_E of invariant differentials on E. In particular, since $E^{\dagger}$ is (Zariski locally over E) the spectrum of a polynomial algebra in one variable with coefficients in the sheaf of functions on E, it makes sense to speak of the "relative degree over E" – which we refer to in this paper as the *torsorial degree* – of a function on $E^{\dagger}$. Note that (since we are in characteristic zero) the subscheme $E^{\dagger}[d] \subseteq E^{\dagger}$ of d-torsion points of $E^{\dagger}$ maps isomorphically to the subscheme $E[d] \subseteq E$ of d-torsion points of E. Then in its simplest form, the main theorem of [7] states the following:

Theorem 1.1. (Simple Version of the Hodge-Arakelov Comparison Isomorphism) *Let E be an elliptic curve over a field K of characteristic zero. Write $E^{\dagger} \to E$ for its universal extension. Let d be a positive integer, and $\eta \in E(K)$ a torsion point whose order does not divide d. Write $\mathcal{L} \stackrel{\text{def}}{=} \mathcal{O}_E(d \cdot [\eta])$. Then the natural map*

$$\Gamma(E^{\dagger}, \mathcal{L})^{<d} \to \mathcal{L}|_{E^{\dagger}[d]}$$

given by restricting sections of $\mathcal{L}$ over $E^{\dagger}$ whose torsorial degree is $< d$ to the d-torsion points $E^{\dagger}[d] \subseteq E^{\dagger}$ is a **bijection** *between K-vector spaces of dimension d^2.*

The remainder of the main theorem essentially consists of specifying precisely *how one must modify the integral structure of* $\Gamma(E^{\dagger}, \mathcal{L})^{<d}$ *over more general bases* in order to obtain an isomorphism at the finite and infinite primes of a number field, as well as for degenerating elliptic curves.

The relationship between Theorem 1.1 and the classical Kodaira-Spencer morphism is discussed in detail — albeit at a rather *philosophical* level — in [12], §1.3, 1.4. The analogue in the arithmetic case of the geometric argument used above to prove (1) is discussed in [12], §1.5.1. The upshot of this argument in the arithmetic case is that in order to derive diophantine equalities analogous to (1) in the arithmetic case — i.e., *Szpiro's conjecture* — it is necessary to eliminate certain *unwanted poles* — called *Gaussian poles* — that occur in the construction of the arithmetic Kodaira-Spencer morphism.

In the present manuscript, we discuss the following further developments in the theory (cf. §3, 4):

(i) a method for *eliminating the Gaussian poles* under certain conditions (cf. Corollary 3.5);
(ii) an argument which shows that (under certain conditions) the reduction in positive characteristic of the arithmetic Kodaira-Spencer morphism *coincides* with the classical geometric Kodaira-Spencer morphism (cf. Corollary 3.6);
(iii) a *alternative proof* of Theorem 1.1 using characteristic p methods (cf. Theorem 4.3).

Thus, development (i) *brings us closer to the goal of applying Hodge-Arakelov theory to proving Szpiro's conjecture* (for elliptic curves over number fields). Unfortunately, the conditions under which the argument of (i) may be carried out *do not hold* (at least in the naive sense) for elliptic curves over number fields. Nevertheless, there is substantial hope that certain new constructions will allow us to realize these conditions even for elliptic curves over number fields (cf. §3 for more on this issue). Development (ii) is significant in that it shows that the *analogy between the arithmetic and classical geometric Kodaira-Spencer morphisms* is not just philosophy, but *rigorous mathematics*! Finally, the significance of development (iii) is that it provides a much more *conceptual*, as well as *technically simpler* proof of the "fundamental theorem of Hodge-Arakelov theory" (i.e., Theorem 1.1).

Underlying all of these new developments (especially (i), (ii)) is the theory of the *crystalline theta object*, to be discussed in §2. This object is a *locally free sheaf equipped with a connection and a Hodge filtration*, hence is reminiscent of the *"$\mathcal{MF}^{\nabla}$-objects"* of [2], §2. On the other hand, many of its properties, such as *"Griffiths semi-transversality"* and *the vanishing of the (higher) p-curvatures*, are somewhat different from (and indeed, somewhat surprising from the point of view of the theory of) $\mathcal{MF}^{\nabla}$-objects. Nevertheless, these properties are of crucial importance in the arguments that underly developments (i), (ii).

§2. The Crystalline Theta Object

2.1. The Complex Analogue

We begin the discussion of this § by motivating our construction in the abstract algebraic case by first examining the complex analogue of the abstract algebraic theory.

Let E be an *elliptic curve over* $\mathbb{C}$ (the field of complex numbers). In this discussion of the complex analogue, we shall regard E as a *complex manifold* (rather than an algebraic variety). Let us write $\mathcal{O}_E$ (respectively, $\mathcal{O}_{E_{\mathbb{R}}}$) for the sheaf of complex analytic (respectively, real analytic)

complex-valued functions on E. In both the complex and real analytic categories, we have *exponential exact sequences*:

$$0 \longrightarrow 2\pi i \cdot \mathbb{Z} \longrightarrow \mathcal{O}_E \xrightarrow{\exp} \mathcal{O}_E^{\times} \longrightarrow 0$$

$$0 \longrightarrow 2\pi i \cdot \mathbb{Z} \longrightarrow \mathcal{O}_{E_{\mathbb{R}}} \xrightarrow{\exp} \mathcal{O}_{E_{\mathbb{R}}}^{\times} \longrightarrow 0$$

Since (as is well-known from analysis) $H^1(E, \mathcal{O}_{E_{\mathbb{R}}}) = H^2(E, \mathcal{O}_{E_{\mathbb{R}}}) = H^2(E, \mathcal{O}_E) = 0$, taking cohomology thus gives rise to the following exact sequences:

$$\begin{aligned} 0 \longrightarrow H^1(E, 2\pi i \cdot \mathbb{Z}) \longrightarrow \quad & H^1(E, \mathcal{O}_E) \quad \longrightarrow H^1(E, \mathcal{O}_E^{\times}) \\ \xrightarrow{\deg} H^2(E, 2\pi i \cdot \mathbb{Z}) = \mathbb{Z} \longrightarrow \quad & 0 \end{aligned}$$

$$0 \longrightarrow H^1(E, \mathcal{O}_{E_{\mathbb{R}}}^{\times}) \xrightarrow{\deg} H^2(E, 2\pi i \cdot \mathbb{Z}) = \mathbb{Z} \longrightarrow 0$$

In other words, (as is well-known) the isomorphism class of a *holomorphic line bundle* on E is not determined just by its degree (which is a topological invariant), but also has *continuous holomorphic moduli* (given by $H^1(E, \mathcal{O}_E) \neq 0$), while the isomorphism class of a *real analytic line bundle* is completely determined by its degree. Thus, in particular, *the complex analytic pair* $(E, \mathcal{L})$ (*i.e., a "polarized elliptic curve"*) *has nontrivial moduli*, and in fact, even if the moduli of E are held fixed, $\mathcal{L}$ itself has nontrivial moduli. (Here, by "nontrivial moduli," we mean that there exist continuous families of such objects which are not locally isomorphic to the trivial family.) On the other hand, (if we write $\mathcal{L}_{\mathbb{R}} \overset{\text{def}}{=} \mathcal{L} \otimes_{\mathcal{O}_E} \mathcal{O}_{E_{\mathbb{R}}}$, then) *the real analytic pair* $(E_{\mathbb{R}}, \mathcal{L}_{\mathbb{R}})$ *has trivial moduli*, i.e., continuous families of such objects are always locally isomorphic to the trivial family. Put another way,

> *The real analytic pair* $(E_{\mathbb{R}}, \mathcal{L}_{\mathbb{R}})$ *is a* **topological invariant** *of the polarized elliptic curve* $(E, \mathcal{L})$.

Note that once one admits that $E_{\mathbb{R}}$ itself is a "topological invariant" of E (a fact which may be seen immediately by thinking of $E_{\mathbb{R}}$ as $H^1(E, \mathbf{S^1})$, where $\mathbf{S^1} \subseteq \mathbb{C}^{\times}$ is the unit circle), (one checks easily that) the fact that $\mathcal{L}_{\mathbb{R}}$ is also a topological invariant follows essentially from the fact that $H^1(E, \mathcal{O}_{E_{\mathbb{R}}}) = 0$. Note that if one thinks of the *universal extension* $E^{\dagger}$ as the *algebraic analogue* of $E_{\mathbb{R}}$, then the analogue of this fact in the algebraic context is given precisely by the (easily verified) fact:

$$H^1(E^\dagger, \mathcal{O}_{E^\dagger}) = 0$$

(that is, the first cohomology module of the algebraic coherent sheaf $\mathcal{O}_{E^\dagger}$ vanishes). In §2.3 below, we would like to exploit this fact to show that the pair $(E^\dagger, \mathcal{L}|_{E^\dagger})$ has a natural structure of *crystal* (valued in the category of "polarized varieties," or varieties equipped with an ample line bundle), and that — by placing an appropriate *integral structure* on $E^\dagger$ — one may show that this crystal exists naturally not only in characteristic 0, but also in *mixed characteristic*. Thus, in summary, the analogy that we wish to assert here is the following:

topological invariance of $(E_{\mathbb{R}}, \mathcal{L}_{\mathbb{R}})$ $\longleftrightarrow$ $(E^\dagger, \mathcal{L}|_E^\dagger)$ is a **crystal**

In fact, it is useful here to recall that in some sense:

> *The essential spirit of the "Hodge-Arakelov Theory of Elliptic Curves" may be summarized as being the Hodge theory of the pairs* $(E_{\mathbb{R}}, \mathcal{L}_{\mathbb{R}})$ *(at archimedean primes),* $(E^\dagger, \mathcal{L}|_E^\dagger)$ *(with appropriate integral structures — to be discussed in §2.3 below — at non-archimedean primes), as opposed to the "usual Hodge theory of an elliptic curve" which may be thought of as the Hodge theory of* $E_{\mathbb{R}}$ *(at archimedean primes) or* $E^\dagger$ *(at non-archimedean primes).*

In this connection, we note that the "Hodge-Arakelov theory of an elliptic curve at an archimedean prime" is discussed/reviewed in detail in [7], Chapter VII, §4.

2.2. The Case of Ordinary p-adic Elliptic Curves

Central to the theory of the mixed characteristic analogue of the ideas presented in §2.1 is the theory of the *étale integral structure on the universal extension* of an elliptic curve. In the present §, we would like to review the definition of the étale integral structure and discuss its structure in the case of an ordinary p-adic elliptic curve.

Let us work over a formal neighborhood of the point at infinity on the moduli stack of elliptic curves — i.e., say, the spectrum of a ring of power series of the form

$$S \stackrel{\text{def}}{=} \text{Spec}(\mathcal{O}[[q]])$$

where $\mathcal{O}$ is a Dedekind domain of mixed characteristic and q an indeterminate. Write $\widehat{S}$ for the completion of S with respect to the q-adic topology, and $E \to S$ for the *tautological degenerating elliptic curve* (more

precisely: one-dimensional semi-abelian scheme), with "q-parameter" equal to q. Then we have natural isomorphisms

$$E|_{\widehat{S}} \cong \mathbb{G}_m; \quad \omega_E = \mathcal{O}_S \cdot d\log(U); \quad E^\dagger|_{\widehat{S}} \cong \mathbb{G}_m \times \mathbb{A}^1$$

where we write U for the usual multiplicative coordinate on $\mathbb{G}_m$ (cf. [7], Chapter III, Theorem 2.1; the discussion of [7], Chapter III, §6, for more details). If we write "T" for the standard coordinate on this affine line, then near infinity, the *standard integral structure* on $E^\dagger$ may be described as that given by

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot T^r$$

On the other hand:

Definition 2.1. The *étale integral structure on* $E^\dagger$ (near infinity) is given by

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot \binom{T}{r}$$

where $\binom{T}{r} \stackrel{\text{def}}{=} \frac{1}{r!}T(T-1)\cdot\cdots\cdot(T-(r-1)))$.

Moreover, although the above definition of this integral structure is only valid near infinity, this integral structure *extends uniquely over the entire (compactified) moduli stack of elliptic curves* $\overline{\mathcal{M}}_{\text{ell}}$ (over $\mathbb{Z}$) — cf. [9], §1. (Note that this uniqueness is a consequence of the fact that $\overline{\mathcal{M}}_{\text{ell}}$ is a regular scheme of dimension 2.)

Thus, given a *family of elliptic curves* $E \to S$ over an arbitrary $\mathbb{Z}$-flat base S, we obtain a *naturally defined "étale integral structure"* on the universal extension $E^\dagger$, i.e., a group scheme

$$E^\dagger_{\text{et}} \to S$$

(which is not of finite type over S).

Next, we would like to examine this étale integral structure in more detail in the case of a *family of ordinary p-adic elliptic curves.* Thus, let S be a *p-adic formal scheme which is formally smooth over* $\mathbb{Z}_p$, and assume also that we are given a *family of ordinary elliptic curves*

$$E \to S$$

such that the associated classifying morphism $S \to (\mathcal{M}_{\text{ell}})_{\mathbb{Z}_p}$ is formally (i.e., relative to the p-adic topology) *étale.* (Here, by "ordinary," we

mean that the fibers of $E \to S$ over all the points of $S_{\mathbb{F}_p}$ have nonzero Hasse invariant.) For $n \geq 1$, write

$$E[p^n] \stackrel{\text{def}}{=} \mathrm{Ker}([p^n] : E \to E)$$

for the kernel of multiplication by p^n on E. Then, as is well-known (cf., e.g., [6], p. 150), there is a unique exact sequence

$$0 \to E[p^n]^{\boldsymbol{\mu}} \to E[p^n] \to E[p^n]^{\mathrm{et}} \to 0$$

of finite flat group schemes over E such that $E[p^n]^{\boldsymbol{\mu}}$ (respectively, $E[p^n]^{\mathrm{et}}$) is étale locally isomorphic to $\boldsymbol{\mu}_{p^n}$ (respectively, $\mathbb{Z}/p^n\mathbb{Z}$).

Let us write:

$$E^{\mathrm{F}^n} \stackrel{\text{def}}{=} E/E[p^n]^{\boldsymbol{\mu}}$$

Then since $E^{\mathrm{F}^n} \to S$ is a family of elliptic curves, and the classifying morphism associated to $E \to S$ is *étale*, it follows that $E^{\mathrm{F}^n} \to S$ defines a morphism:

$$\Phi_S^n : S \to S$$

One checks easily that $\Phi_S \stackrel{\text{def}}{=} \Phi_S^1$ is a *lifting of the Frobenius morphism in characteristic p*, and that Φ_S^n is the result of iterating Φ_S a total of n times (as the notation suggests). The morphism

$$\mathcal{V} : E^{\mathrm{F}} \to E$$

given by forming the quotient of E^{F} by the image in E^{F} of $E[p]$ will be referred to as the the *Verschiebung morphism* associated to E. For any $n \geq 1$, the morphism

$$\mathcal{V}^n : E^{\mathrm{F}^n} \to E$$

given by forming the quotient of E^{F^n} by the image in E^{F^n} of $E[p^n]$ is easily seen to be equal (as the notation suggests) to the "n-th iterate" (i.e., up to various appropriate base changes by iterates of Φ_S) of $\mathcal{V}$. Note that the kernel of $\mathcal{V}^n$ may be identified with $E[p^n]^{\mathrm{et}}$. In particular, it follows that $\mathcal{V}^n$ is *étale of degree* p^n.

Thus, we obtain a tower

$$\cdots \to E^{\mathrm{F}^n} \to E^{\mathrm{F}^{n-1}} \to \cdots \to E^{\mathrm{F}} \to E$$

of étale isogenies of degree p. Let us denote the p-adic completion of the inverse limit of this system of isogenies by E^{F^∞}. Thus, in particular, we have a natural morphism

$$E^{\mathrm{F}^\infty} \to E$$

In [9], §2.2, a certain canonical section

$$\kappa[p^n] : E^{\mathrm{F}^n} \otimes \mathbb{Z}/p^n\mathbb{Z} \to E^\dagger \otimes \mathbb{Z}/p^n\mathbb{Z}$$

is constructed of the universal extension of E over E^{F^n}. This section is the "ordinary analogue" of the section near infinity (cf. the discussion at the beginning of the present §2.2) given by sending $T \mapsto 0$. Letting $n \to \infty$, we thus obtain a morphism

$$\kappa[p^\infty] : E^{\mathrm{F}^\infty} \to (E^\dagger)^\wedge$$

(where "$\wedge$" denotes p-adic completion). Finally, by computing near infinity, one shows that this morphism in fact *factors uniquely through the étale integral structure*, i.e., determines a morphism:

$$\kappa_{\mathrm{et}}^\infty : E^{\mathrm{F}^\infty} \to (E_{\mathrm{et}}^\dagger)^\wedge$$

Theorem 2.2. (Explicit Description of the Étale Integral Structure of an Ordinary Elliptic Curve) *The natural morphism*

$$\kappa_{\mathrm{et}}^\infty : E^{\mathrm{F}^\infty} \to (E_{\mathrm{et}}^\dagger)^\wedge$$

from the p-adic completion of the "Verschiebung tower" of E to the p-adic completion of the universal extension of E equipped with the étale integral structure is an isomorphism.

We refer to [9], §2.2, for more details. The essential idea of the proof is to apply the following *well-known bijection* (due to Mahler — cf., e.g., [5], §3.2):

$$\mathrm{Comb}(\mathbb{Z}_p)^\wedge \xrightarrow{\sim} \mathrm{Cont}(\mathbb{Z}_p, \mathbb{Z}_p)$$

from the p-adic completion of the free $\mathbb{Z}_p$-module $\mathrm{Comb}(\mathbb{Z}_p)$ on the generators $\binom{T}{r}$ to the space of continuous functions $\mathbb{Z}_p \to \mathbb{Z}_p$ (given by evaluating the indeterminate T on elements of $\mathbb{Z}_p$).

Remark 2.3. One way to think of the content of Theorem 2.2 is as the assertion that:

> *The étale integral structure on $E^\dagger$ is very closely related to the p-adic Hodge theory of E.*

Since $E^{\dagger}_{\text{et}}$ is defined globally over $\mathbb{Z}$ whenever E is defined globally over $\mathbb{Z}$, Theorem 2.2 may also be taken as asserting that $E^{\dagger}_{\text{et}}$ enjoys the following remarkable interpretation:

> *The universal extension of an elliptic curve equipped with the étale integral structure is a natural globalization over $\mathbb{Z}$ of the (very local!) p-adic Hodge theory of the elliptic curve.*

This interpretation is very much in line with the general philosophy of Hodge-Arakelov theory (cf., e.g., [12], §1.3).

2.3. Integral Structures and Connections

Let

$$f : E \to S$$

be a *family of elliptic curves* over a scheme S. In order to formulate the various versions of the comparison isomorphism of Hodge-Arakelov theory (cf., e.g., Theorem 1.1) properly in mixed characteristic, it is necessary to consider not only the universal extension $E^{\dagger}$, but also certain $E^{\dagger}$-torsors — which we shall refer to as *Hodge torsors* — as follows. Let $\mathcal{L}$ be a *line bundle on* E. For simplicity, we assume that the (relative) degree (over S) of $\mathcal{L}$ is *one*. Then we define

$$E^{\mathcal{L}} \to E$$

to be the ω_E-torsor over E parametrizing (over an open $U \subseteq E$) the ($\mathcal{O}_S$-linear) *connections $\nabla_{\mathcal{L}}$ on the line bundle $\mathcal{L}$*. Often to simplify the notation (as well as to emphasize the analogy with $E^{\dagger}$), we will denote $E^{\mathcal{L}}$ by

$$E^*$$

(where we think of the "$*$" as being set equal to $\mathcal{L}$).

Then E^* admits a *natural $E^{\dagger}$-action*, defined as follows. If $\nabla_{\mathcal{L}}$ is the connection corresponding to a section of $E^* \to E$ over some open $U \subseteq E$, and ∇_α is a connection on the degree zero line bundle $\mathcal{O}_E([0_E] - [\alpha])$ for some point $\alpha \in E(S)$, then we let the point (α, ∇_α) of $E^{\dagger}(S)$ act on E^* by

$$\nabla_{\mathcal{L}} \mapsto (\mathcal{T}_\alpha^* \nabla_{\mathcal{L}}) \otimes \nabla_\alpha$$

— where we denote by $\mathcal{T}_\alpha : E \to E$ the morphism "translation by α," and we observe that

$$(\mathcal{T}_\alpha^*\mathcal{L}) \otimes \mathcal{O}_E([0_E] - [\alpha]) \xrightarrow{\sim} \mathcal{L}$$

(by the elementary theory of line bundles on elliptic curves), so $(\mathcal{T}_\alpha^*\nabla_{\mathcal{L}}) \otimes \nabla_\alpha$ defines a connection on $\mathcal{L}$ over $\mathcal{T}_\alpha^* U$, i.e., a section of $E^* \to E$ over $\mathcal{T}_\alpha^* U$, as desired. Thus, we obtain an action of $E^\dagger$ on E^* which is *compatible* (via the projections $E^\dagger \to E$, $E^* \to E$) with the usual translation action of E on itself. Moreover, it is an easy exercise to show that *the action of $E^\dagger$ on E^* defines a structure of $E^\dagger$-torsor on E^*.*

When S is $\mathbb{Z}$-*flat*, and $\mathcal{L}$ is the degree one line bundle defined by a *torsion point* $\eta \in E(S)$, then there is also a natural analogue of the *étale integral structure* on $E^\dagger$ (cf. §2.2) for E^*. For simplicity, we restrict ourselves here to the case where $* = \mathcal{O}_E([0_E])$. Then (since $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$ is connected and regular of dimension two) the étale integral structure on E^* is uniquely determined over arbitrary S once it is determined "near infinity," i.e., in the case $S = \mathrm{Spec}(\mathbb{Z}[[q]])$. Now, as we saw at the beginning of §2.2, the *standard integral structure on $E^\dagger$* is given (near infinity) by:

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot T^r$$

Relative to this notation, the *standard integral structure on E^** is given by:

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot (T - \frac{1}{2})^r$$

Thus, just as the *étale integral structure on $E^\dagger$* is given by:

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot \binom{T}{r}$$

it should not surprise the reader that the *étale integral structure on E^** is given by:

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot \binom{T - \frac{1}{2}}{r}$$

Here, we note that in the case of a *more general torsion point* $\eta \in E(\mathcal{O}[[q^{1/N}]])$ (where $\mathcal{O}$ is the ring of integers of some number field), the "$\frac{1}{2}$" is replaced by a rational number of the form $\beta - \frac{1}{2}$, where $\beta \in \mathbb{Q}$ is any representative of the unique class in $\mathbb{Q}/\mathbb{Z}$ such that — if we think of $E(\mathcal{O}[[q^{1/N}]])$ as $\mathbb{G}_m(\mathcal{O}[[q^{1/N}]][q^{-1}])/q^{\mathbb{Z}}$ via the Schottky uniformization

of the Tate curve E — then η is equal to the point determined by $\zeta \cdot q^{\beta}$ for some root of unity ζ.

Just as in the case of $E^{\dagger}$, the étale integral structure on E^* extends over all of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$. At primes other than 2, this follows immediately from the case of $E^{\dagger}$. On the other hand, at the prime 2, this extension result is much more difficult to prove (cf. [9], §8.2, 8.3) and requires various complicated 2-adic computations involving higher p-curvatures (where $p = 2$). At any rate, once this extension is made, one obtains an S-scheme (which is not of finite type over S)

$$E^*_{\mathrm{et}}$$

equipped with a natural structure of $E^{\dagger}_{\mathrm{et}}$-*torsor*.

Next, let us assume that S is *smooth of finite type over* $\mathbb{Z}$. In this situation, it is proven in [9], Lemma 5.1, that the well-known connection on $E^{\dagger}$ determines natural connections on $E^{\dagger}_{\mathrm{et}}$ and E^*_{et}. Moreover, by using the fact (cf. [9], Theorem 4.3) that

$$f_*(\mathcal{O}_{E^*_{\mathrm{et}}}) = \mathcal{O}_S; \quad \mathbf{R}^1 f_*(\mathcal{O}_{E^*_{\mathrm{et}}}) = 0$$

(where, by abuse of notation, we denote all structure morphisms to S by "f") one derives (cf. [9], Theorem 5.2) the following *fundamental* (i.e., relative to the theory of [9]) *result* (cf. the discussion of §2.1):

Theorem 2.4. *Let $\epsilon \in E^*_{\mathrm{et}}(S)$ be a horizontal point of E^*_{et}. Then restriction to ϵ defines a natural bijection between connections (over $\mathbb{Z}$) on the pair $(E^*_{\mathrm{et}}, \mathcal{L}|_{E^*_{\mathrm{et}}})$ and connections on the line bundle $\mathcal{L}|_{\epsilon}$ on S.*

Remark 2.5. Typically, in the situations that we are interested in, there will be a natural choice of connection on $\mathcal{L}|_{\epsilon}$, so we shall not discuss this technical issue further in this survey. Thus, (once one chooses a connection on $\mathcal{L}|_{\epsilon}$) there is a *natural choice of connection on* $(E^*_{\mathrm{et}}, \mathcal{L}|_{E^*_{\mathrm{et}}})$. In particular, we thus obtain a natural *crystal valued in the category of schemes equipped with an ample line bundle* on the crystalline site of PD-thickenings of S over $\mathbb{Z}$.

Before proceeding, we observe that the crucial fact

$$f_*(\mathcal{O}_{E^*_{\mathrm{et}}}) = \mathcal{O}_S; \quad \mathbf{R}^1 f_*(\mathcal{O}_{E^*_{\mathrm{et}}}) = 0$$

— which is immediate in characteristic 0 — holds in mixed characteristic *only for the étale integral structure*, not for the standard integral structure on E^*. This is the *technical reason* for the appearance of the étale integral structure in Theorem 2.4. It is an interesting coincidence that this integral structure just happens to be the *same integral structure* as

the integral structure that was applied in [7] to make the comparison isomorphism (cf. Theorem 1.1) valid in mixed characteristic.

Once one has a connection on the pair $(E^*_{\text{et}}, \mathcal{L}|_{E^*_{\text{et}}})$, the next natural step is to consider the *resulting connection* $\nabla_{\mathcal{V}}$ on the locally free (albeit of infinite rank!) sheaf

$$\mathcal{V} \stackrel{\text{def}}{=} f_*(\mathcal{L}|_{E^*_{\text{et}}})$$

on S. Note that by considering the *"torsorial degree"* of sections of $\mathcal{L}$ over E^*_{et} (i.e., relative degree over E), one obtains a natural *"Hodge filtration"*

$$F^r(\mathcal{V}) \subseteq \mathcal{V}$$

whose subquotients are given by:

$$(F^{r+1}/F^r)(\mathcal{V}) = \frac{1}{r!} \cdot \tau_E^{\otimes r} \otimes_{\mathcal{O}_S} f_*(\mathcal{L})$$

(where $f_*(\mathcal{L})$ is the push-forward of the original line bundle $\mathcal{L}$ on E). The triple

$$(\mathcal{V}, F^r(\mathcal{V}), \nabla_{\mathcal{V}})$$

is referred to as the *crystalline theta object* (cf. [9], Theorem 8.1) and is the main object of study in [9].

2.4. Comparison Isomorphism at Infinity

In this §, we would like to take a closer look at the *crystalline theta object* introduced in §2.3 in a neighborhood of infinity, i.e., over the base $S = \text{Spec}(\mathbb{Z}[[q]])$. In this case, if we think of the tautological elliptic curve over $U_S \stackrel{\text{def}}{=} S[q^{-1}]$, i.e., the *Tate curve*, as the quotient

$$\mathbb{G}_m/q^{\mathbb{Z}}$$

and write U for the standard multiplicative coordinate on $\mathbb{G}_m$, then sections of $\mathcal{V} \stackrel{\text{def}}{=} f_*(\mathcal{L}|_{E^*_{\text{et}}})$ may be thought of as linear combinations of the *theta function*

$$\Theta \stackrel{\text{def}}{=} \sum_{k \in \mathbb{Z}} (-1)^k \cdot q^{\frac{1}{2}k^2 - \frac{1}{2}k} \cdot U^{k-\frac{1}{2}} \cdot \theta$$

(where "$U^{-\frac{1}{2}} \cdot \theta$" is a certain natural trivialization of $\mathcal{L}$ over $\mathbb{G}_m$, and we note that the exponent of q is always *integral*) and its *derivatives* (i.e., the result of applying polynomials (with $\mathcal{O}_S$-coefficients) in $(U \cdot \partial/\partial U)$).

In fact, in the present context, it is natural to consider certain *specific derivatives* (i.e., *"congruence canonical Schottky-Weierstrass zeta functions"* — cf. [9], §6) of the theta function, as follows. For integers $r \geq 0$, let

$$\lambda_r \stackrel{\text{def}}{=} \lfloor \frac{r}{2} - \frac{1}{2} \rfloor$$

(i.e., the greatest integer $\leq$ the number inside the "$\lfloor - \rfloor$");

$$F^r(\mathbb{Z}) \stackrel{\text{def}}{=} \{0 - \lambda_r, 1 - \lambda_r, \dots, r - 1 - \lambda_r\} \subseteq \mathbb{Z}$$

Thus, $F^{r+1}(\mathbb{Z}) \supseteq F^r(\mathbb{Z})$ is obtained from $F^r(\mathbb{Z})$ by appending one more integer "$k[r]$" directly to the left/right of $F^r(\mathbb{Z})$ (where "left/right" depends only on the parity of r). In particular, the map $\mathbb{Z}_{\geq 0} \to \mathbb{Z}$ given by

$$r \mapsto k[r]$$

is a *bijection*. Also, let us write:

$$\Psi(k) \stackrel{\text{def}}{=} \frac{1}{2}k^2 - \frac{1}{2}k$$

Then a topological (with respect to the q-adic topology) $\mathcal{O}_{\widehat{S}}$-basis of $\mathcal{V}$ is given by $\zeta_0^{\text{CG}}, \zeta_1^{\text{CG}}, \dots, \zeta_r^{\text{CG}}, \dots \in \mathcal{V}$, where we define:

$$\zeta_r^{\text{CG}} = \sum_{k \in \mathbb{Z}} \binom{k + \lambda_r}{r} \cdot (-1)^k \cdot q^{\frac{1}{2}k^2 - \frac{1}{2}k} \cdot U^{k - \frac{1}{2}} \cdot \theta$$

(cf. [7], Chapter V, Theorem 4.8).

Next, let us recall that the integral structure on E^*_{et} was defined by:

$$\bigoplus_{r \geq 0} \mathcal{O}_{\mathbb{G}_m} \cdot \binom{T - \frac{1}{2}}{r}$$

hence that sending $T \mapsto 0$ defines a q-adic section

$$\kappa_{\mathbb{G}_m} : (\mathbb{G}_m)_{\widehat{S}} \to E^*_{\text{et}}|_{\widehat{S}}$$

(at least after one inverts 2). Then pulling back via $\kappa_{\mathbb{G}_m}$ and applying the *trivialization* of $\mathcal{L}|_{\mathbb{G}_m}$ given by "$U^{-\frac{1}{2}} \cdot \theta$" yields a natural *evaluation morphism*:

$$\Xi : \mathcal{V} \to \mathcal{L}|_{(\mathbb{G}_m)_{\widehat{S}}} \stackrel{\sim}{\to} \mathcal{O}_{(\mathbb{G}_m)_{\widehat{S}}}$$

which is, in fact, *integral over* $\mathbb{Z}$ (cf. [9], Theorem 6.1). Moreover, the connection $\nabla_{\mathcal{V}}$ is *projectively compatible* — that is, compatible up to a possible "error term" consisting of a *scalar-valued* (logarithmic) differential on S (cf. [9], Theorem 6.1, for more details) — with the natural connection on $\mathcal{O}_{(\mathbb{G}_m)_{\widehat{S}}}$ (regarded as a quasi-coherent $\mathcal{O}_{\widehat{S}}$-module) arising from the fact that $(\mathbb{G}_m)_{\widehat{S}}$ arises by pulling back to $\widehat{S}$ the $\mathbb{Z}$-*scheme* $\mathbb{G}_m$ (i.e., put another way, the unique connection for which integral powers of U are *horizontal*).

Next, let us observe (cf. [7], Chapter V, Theorem 4.8) that the sections ζ_r^{CG} introduced above have the following *congruence property*:

$$\Xi(\zeta_r^{\mathrm{CG}}) \equiv 0 \pmod{q^{\Psi(k[r])}}$$

Thus, it is natural to consider the sections

$$\widetilde{\zeta}_r^{\mathrm{CG}} \stackrel{\mathrm{def}}{=} q^{-\Psi(k[r])} \cdot \zeta_r^{\mathrm{CG}} \in q^{-\infty} \cdot \mathcal{V}$$

which define a *new integral structure* on $\mathcal{V}$, which we denote by

$$\mathcal{V}^{\mathrm{GP}}$$

— where the "GP" stands for *"Gaussian poles,"* i.e., the poles arising from the $q^{-\Psi(k[r])}$ — cf. [7], Chapter VI, Theorem 4.1 and the Remarks following that theorem. In particular, the $\widetilde{\zeta}_r^{\mathrm{CG}}$ form a *topological* $\mathcal{O}_{\widehat{S}}$-*basis* for $\mathcal{V}^{\mathrm{GP}}$, and Ξ factors through $\mathcal{V}^{\mathrm{GP}}$ to form a morphism:

$$\Xi^{\mathrm{GP}} : \mathcal{V}^{\mathrm{GP}} \to \mathcal{O}_{(\mathbb{G}_m)_{\widehat{S}}}$$

Now we have the following *Schottky-theoretic analogue* (i.e., d-torsion points are replaced by "$\mathbb{G}_m$") of the original *Hodge-Arakelov comparison isomorphism* (cf., Theorem 1.1):

Theorem 2.6. (Schottky-Theoretic Hodge-Arakelov Comparison Isomorphism) *The evaluation map introduced above is an isomorphism:*

$$\Xi^{\mathrm{GP}} : \mathcal{V}^{\mathrm{GP}} \stackrel{\sim}{\to} \mathcal{O}_{(\mathbb{G}_m)_{\widehat{S}}}$$

which is **projectively horizontal** *with respect to the natural (logarithmic) connection* $\nabla_{\mathcal{V}}$ *(cf. Theorem* 2.4*) on the left and the trivial connection (i.e., for which the integral powers of* U *are horizontal) on the right.*

Proof. This is essentially a combination of [9], Theorems 6.1, 6.2. The main idea is that, since the integral powers of U form a topological $\mathcal{O}_{\widehat{S}}$-basis of $\mathcal{O}_{(\mathbb{G}_m)_{\widehat{S}}}$, it suffices to prove the result modulo q, in which case

it essentially follows from the fact that the binomial coefficient functions form a $\mathbb{Z}$-basis of the space of integer-valued polynomial functions on $\mathbb{Z}$. Q.E.D.

A number of interesting corollaries may be read off of Theorem 2.6, as follows. The first such corollary is the *computation of the monodromy* of $(\mathcal{V}, \nabla_{\mathcal{V}})$ at the point at infinity, i.e., $V(q) \subseteq S$ (cf. [9], Corollary 6.3). More important from the point of view of the further development of the theory is the *vanishing of the p-curvature* (cf. [3], §5,6, for a discussion of the notion of "p-curvature") — cf. [9], Corollary 6.4.

In fact, in the present context, in addition to the p-curvature, the *higher p-curvatures* of the pair $(\mathcal{V}, \nabla_{\mathcal{V}})$ may also be defined (cf. [9], §7.1). Then one has the following result (cf. [9], Corollary 7.6):

Corollary 2.7. *All of the higher p-curvatures of the crystalline theta object vanish (over an arbitrary $\mathbb{Z}$-smooth base S).*

Proof. Note that since these higher p-curvatures all form sections of *locally free sheaves* (at least in, say, the universal case $S = (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$) it suffices to check that they are zero in a neighborhood of infinity, i.e., for the present $S = \mathrm{Spec}(\mathbb{Z}[[q]])$. Thus, we may apply the isomorphism of Theorem 2.6, so Corollary 2.7 follows from the fact that $\mathcal{O}_{(\mathbb{G}_m)_{\widehat{S}}}$ is (topologically) generated by its *horizontal sections.* Q.E.D.

In more down-to-earth terms, Corollary 2.7 may be interpreted as follows. It follows from the general theory of integrable connections that in any *PD formal neighborhood* (where, "PD" stands for "puissances divisées," i.e., divided powers) of a point of S, sections of $\mathcal{V}$ may be *PD formally integrated* to form *horizontal sections of* $(\mathcal{V}, \nabla_{\mathcal{V}})$ in the given PD formal neighborhood. In general, such horizontal sections are not defined on a *formal neighborhood* of the given point of S, i.e., (if, for instance, t is a local coordinate on a relatively one-dimensional smooth S over $\mathbb{Z}$, then) such horizontal sections are only defined once one introduces the *divided powers*:

$$\frac{t^n}{n!}$$

(where $n \geq 0$ is an integer). To state then that *"all the higher p-curvatures vanish"* means that *such horizontal sections exist as formal power series in t with integral coefficients.*

The above discussion motivates the following point of view. Near infinity, the horizontal sections of the above discussion are simply the integral powers of U. Thus, the *classical theta expansion*

$$\Theta \stackrel{\text{def}}{=} \sum_{k \in \mathbb{Z}} (-1)^k \cdot q^{\frac{1}{2}k^2 - \frac{1}{2}k} \cdot U^{k-\frac{1}{2}} \cdot \theta$$

may be thought of (in the present context) as the *"expansion of a generator of $F^1(\mathcal{V})$ in terms of local horizontal sections of $(\mathcal{V}, \nabla_{\mathcal{V}})$."* In particular, if one takes this point of view, then it is natural to consider the expansion of a generator of $F^1(\mathcal{V})$ in terms of local horizontal sections of $(\mathcal{V}, \nabla_{\mathcal{V}})$ at points of $(\overline{\mathcal{M}}_{\text{ell}})_{\mathbb{Z}}$ other than the point at infinity. These *crystalline theta expansions* are discussion in more detail in [9], §7.2.

2.5. The Associated Kodaira-Spencer Morphism

Let

$$f : E \to S$$

be a *family of elliptic curves* over a *smooth $\mathbb{Z}$-scheme S*. We shall write $(\mathcal{V}, F^r(\mathcal{V}), \nabla_{\mathcal{V}})$ for the associated *crystalline theta object* (cf. §2.3).

In this §, we would like to consider the relationship between $\nabla_{\mathcal{V}}$ and $F^r(\mathcal{V})$. The first, most fundamental property of this relationship is that, unlike the $\mathcal{MF}^{\nabla}$-objects of [2], §2, which satisfy *Griffiths transversality*, i.e., the connection maps F^r into F^{r+1}, the crystalline theta object only satisfies the following weaker property (cf. [9], Theorem 8.1):

Theorem 2.8. (Griffiths Semi-transversality) *The crystalline theta object satisfies "Griffiths semi-transversality," i.e., $\nabla_{\mathcal{V}}$ maps $F^r(\mathcal{V})$ into $F^{r+2}(\mathcal{V})$ for all integers $r \geq 0$.*

Remark 2.9. The reason that the crystalline theta object is only "semi-transversal" is the following: The connection of Theorem 2.4 is defined in *two steps*. If one thinks in terms of isomorphisms between pull-backs to "nearby points" that differ by a square nilpotent ideal, *first* one must establish the isomorphism between the two pull-backs of E^*_{et}. This causes the Hodge filtration to jump *once*. *Then* (once one has an isomorphism between the underlying schemes, i.e., between the two pull-backs of E^*_{et}) one must establish an isomorphism between the two pull-backs of $\mathcal{L}$. This causes the Hodge filtration to jump *once more*. We refer to the discussion of [9], §8.1, for more details.

Thus, by analogy to the usual Kodaira-Spencer morphism in the Griffiths-transversal case (which measures the extent to which the connection fails to *preserve* the Hodge filtration, i.e., map F^r into F^r), it is natural to define the *Kodaira-Spencer morphism of the crystalline theta object* as follows: By Theorem 2.8, $\nabla_{\mathcal{V}}$ defines a morphism:

$$F^1(\mathcal{V}) \to F^3(\mathcal{V}) \otimes_{\mathcal{O}_S} \Omega_{S/\mathbb{Z}}$$

If we then compose with the projection $F^3 \twoheadrightarrow F^3/F^2$, then we obtain an $\mathcal{O}_S$-linear morphism:

$$\kappa_{\mathcal{V}} : F^1(\mathcal{V}) \to (F^3/F^2)(\mathcal{V}) \otimes_{\mathcal{O}_S} \Omega_{S/\mathbb{Z}} \xrightarrow{\sim} \frac{1}{2} \cdot \tau_E^{\otimes 2} \otimes_{\mathcal{O}_S} F^1(\mathcal{V}) \otimes_{\mathcal{O}_S} \Omega_{S/\mathbb{Z}}$$

Moreover, since $F^1(\mathcal{V}) = f_*\mathcal{O}_E([0_E])$ is a *line bundle*, it follows that we may regard $\kappa_{\mathcal{V}}$ as an $\mathcal{O}_S$-linear morphism:

$$\omega_E^{\otimes 2} \to \frac{1}{2} \cdot \Omega_{S/\mathbb{Z}}$$

On the other hand, we recall that the *"classical Kodaira-Spencer morphism"* of the family $E \to S$ is defined as follows: If we write

$$\mathcal{E} \stackrel{\text{def}}{=} \mathbf{R}^1 f_{\mathrm{DR},*}\mathcal{O}_E$$

for the first relative de Rham cohomology module of $E \to S$, and $F^1(\mathcal{E}) \subseteq \mathcal{E}$ (respectively, $\nabla_{\mathcal{E}}$) for its Hodge filtration (respectively, Gauss-Manin connection), then $\nabla_{\mathcal{E}}$ defines a morphism

$$F^1(\mathcal{E}) \to \mathcal{E} \otimes_{\mathcal{O}_S} \Omega_{S/\mathbb{Z}}$$

which may be composed with the projection $\mathcal{E} \twoheadrightarrow \mathcal{E}/F^1(\mathcal{E}) \xrightarrow{\sim} F^1(\mathcal{E}) \otimes_{\mathcal{O}_S} \tau_E^{\otimes 2}$ to obtain a morphism:

$$\kappa_{\mathcal{E}} : F^1(\mathcal{E}) \to F^1(\mathcal{E}) \otimes_{\mathcal{O}_S} \tau_E^{\otimes 2} \otimes_{\mathcal{O}_S} \Omega_{S/\mathbb{Z}}$$

Since $F^1(\mathcal{E}) = \omega_E$ is a line bundle, $\kappa_{\mathcal{E}}$ may thus be regarded as a morphism:

$$\omega_E^{\otimes 2} \to \Omega_{S/\mathbb{Z}}$$

Then we have the following result (cf. [9], Theorem 8.1):

Theorem 2.10. (The Kodaira-Spencer Morphism of the Crystalline Theta Object) *The Kodaira-Spencer morphism*

$$\kappa_{\mathcal{V}} : \omega_E^{\otimes 2} \to \frac{1}{2} \cdot \Omega_{S/\mathbb{Z}}$$

associated to the crystalline theta object $(\mathcal{V}, F^r(\mathcal{V}), \nabla_{\mathcal{V}})$ *is equal to* $\frac{1}{2}$ *times the classical Kodaira-Spencer morphism*

$$\kappa_{\mathcal{E}} : \omega_E^{\otimes 2} \to \Omega_{S/\mathbb{Z}}$$

associated to the relative first de Rham cohomology module of the family $E \to S$.

Proof. It suffices to prove this result in the universal case, i.e., when $S = (\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$. Moreover, the asserted equality clearly holds over all of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{Z}}$ if and only if it holds in a neighborhood of infinity. Thus, we may assume that $S = \mathrm{Spec}(\mathbb{Z}[[q]])$. Now the main idea is to consider the theta expansion:

$$\Theta \stackrel{\mathrm{def}}{=} \sum_{k \in \mathbb{Z}} (-1)^k \cdot q^{\frac{1}{2}k^2 - \frac{1}{2}k} \cdot U^k \cdot (U^{-\frac{1}{2}} \cdot \theta)$$

By Theorem 2.6, the connection $\nabla_{\mathcal{V}}$ amounts (in the context of such expansions) to the (logarithmic) partial derivative $q \cdot \partial/\partial q$. On the other hand, generators of $F^r(\mathcal{V})$ for $r > 1$ are obtained by taking various derivatives of Θ with respect to U. Since applying $q \cdot \partial/\partial q$ to the k-th term of the expansion amounts to multiplying the k-th term by $\frac{1}{2}k^2 - \frac{1}{2}k$, it follows that (if we ignore the trivialization "$(U^{-\frac{1}{2}} \cdot \theta)$," then) applying $q \cdot \partial/\partial q$ to the k-th term of the expansion gives the same result as applying $\frac{1}{2}(U \cdot \partial/\partial U)^2 - \frac{1}{2}(U \cdot \partial/\partial U)$ to this term. That is to say, we have:

$$\{q \cdot \partial/\partial q\} \cdot \Theta = \{\frac{1}{2}(U \cdot \partial/\partial U)^2 - \frac{1}{2}(U \cdot \partial/\partial U)\} \cdot \Theta$$

On the other hand, near infinity, the classical Kodaira-Spencer morphism amounts to the identification of "$q \cdot \partial/\partial q$" with "$(U \cdot \partial/\partial U)^2$." This completes the proof of the asserted equality. Q.E.D.

Remark 2.11. The *vanishing* of the p-curvatures (cf. Corollary 2.7) in the presence of a Kodaira-Spencer morphism which is an *isomorphism* (cf. Theorem 2.10) is somewhat surprising from the point of view of the classical theory of $\mathcal{MF}^{\nabla}$-objects arising from families of varieties, in which *vanishing of the p-curvature is related to vanishing of the Kodaira-Spencer morphism* (cf. [4]).

§3. Lagrangian Galois Actions

In this §, we apply the theory of §2 to

(i) show how to *eliminate the Gaussian poles* from (a certain version of) the arithmetic Kodaira-Spencer morphism under certain conditions (cf. Corollary 3.5);

(ii) show that the reduction in positive characteristic of (a certain version of) the arithmetic Kodaira-Spencer morphism *coincides* with

the classical geometric Kodaira-Spencer morphism (cf. Corollary 3.6).

The ideas surveyed in this § are discussed in more detail in [10], §2 (in the case of odd p); [11], §3 (in the case of $p = 2$). The key idea here is that the theory of the *crystalline theta object* allows one to study the (globally defined) *discrete* arithmetic Kodaira-Spencer morphism from a (local p-adic) *continuous* point of view.

Let p be an *odd prime*. Let $K \stackrel{\text{def}}{=} \mathbb{Q}_p(\zeta_p)$, where ζ_p is a *primitive p-th root of unity*. Write $\mathcal{O}_K$ (respectively, $\mathfrak{m}$; k) for the ring of integers of K (respectively, maximal ideal of $\mathcal{O}_K$; residue field of $\mathcal{O}_K$);

$$U_S \stackrel{\text{def}}{=} S \backslash V(q) \subseteq S \stackrel{\text{def}}{=} \operatorname{Spec}(\mathcal{O}_K[[q]])$$

and

$$E \to S$$

for the tautological *degenerating elliptic curve* (more precisely: one-dimensional semi-abelian scheme) with "q-parameter" equal to q over S. Also, let us write:

$$Z \stackrel{\text{def}}{=} \operatorname{Spec}(\mathcal{O}_K[[q^{\frac{1}{p}}]])$$

Thus, over $\mathbb{Q}$, $Z_{\mathbb{Q}} \to S_{\mathbb{Q}}$ is finite, étale over $(U_S)_{\mathbb{Q}}$, and Galois, with Galois group

$$G = \mathbb{F}_p(1)$$

(where the "(1)" denotes a Tate twist). As is well-known, over U_S, the *p-torsion points* of $E \to S$ fit into a natural exact sequence:

$$0 \to \boldsymbol{\mu}_p|_{U_S} \to E[p]|_{U_S} \to \mathbb{F}_p|_{U_S} \to 0$$

which splits over $U_Z \stackrel{\text{def}}{=} U_S \times_S Z$. In the following discussion, we consider the *particular splitting*

$$H|_{U_Z} \subseteq E[p]|_{U_Z}$$

(i.e., subgroup scheme $H|_{U_Z}$ that projects isomorphically onto $\mathbb{F}_p|_{U_Z}$) of this exact sequence defined by the p-th root of q given by $q^{\frac{1}{p}}$.

Next, let us write $C \to S$ for the unique *semi-stable model* compactifying $E \to S$. Thus, C is *regular*, and the complement of its unique node is equal to E. On the other hand, $C_Z \stackrel{\text{def}}{=} C \times_S Z$ is no longer regular. Let us denote by

$$C'_Z \to Z$$

the unique *regular semi-stable model* over Z compactifying $E|_{U_Z}$. Thus, the complement

$$E'_Z \to Z$$

of the nodes of C'_Z has a natural group scheme structure whose special fiber (i.e., fiber over $V(q^{\frac{1}{p}})$) is a disjoint union of p copies of $\mathbb{G}_m$.

Next, let us observe that $H|_{U_Z}$ determines (by taking the closure in E'_Z) a *closed subgroup scheme*

$$H \subseteq E'_Z$$

of E'_Z. We may then form the *quotient*:

$$E_Z \subseteq E'_Z \twoheadrightarrow E_H \stackrel{\text{def}}{=} E'_Z/H$$

Thus, $E_H \to Z$ is a *one-dimensional semi-abelian scheme* with "q-parameter" equal to $q^{\frac{1}{p}}$. Let us write

$$\mathcal{L}_H \stackrel{\text{def}}{=} \mathcal{O}_{E_H}([0_{E_H}])$$

and $\mathcal{L}'_Z \stackrel{\text{def}}{=} \mathcal{L}_H|_{E'_Z}$; $\mathcal{L}_Z \stackrel{\text{def}}{=} \mathcal{L}'_Z|_{E_Z}$. Moreover, it may be shown (cf. [10], §2.1, for more details) that, if we denote by $\epsilon \in E_Z(Z)$ the unique section of order 2, then although *a priori*,

$$\mathcal{L}_\epsilon \stackrel{\text{def}}{=} \mathcal{L}_Z|_\epsilon$$

appears only to be defined over Z, in fact, it *admits a natural G-action* (compatible with the G-action on $\mathcal{O}_Z$), as if it arose as the pull-back to Z of a line bundle on S.

On the other hand, note (cf. the exact sequence discussed above) that $\boldsymbol{\mu}_p$ may be regarded as a *closed subgroup scheme*:

$$(\boldsymbol{\mu}_p)_Z \subseteq E_H$$

In addition, one has a natural closed subgroup scheme

$$\{\pm 1\} \hookrightarrow E_H$$

so we shall write "$(-\boldsymbol{\mu}_p)_Z \subseteq E_H$" for the *translate* of $(\boldsymbol{\mu}_p)_Z$ by the element "-1."

If we now *substitute* the pair $(E_H, \mathcal{L}_H)$ into the theory of §2.3, 2.4, we obtain the corresponding *crystalline theta object*

$$(\mathcal{V}_H, F^r(\mathcal{V}_H), \nabla_{\mathcal{V}_H})$$

over Z by considering sections of $\mathcal{L}_H$ over the *Hodge torsor equipped with its étale integral structure* $E^*_{H,\mathrm{et}}$ associated to this pair. Moreover, it follows immediately from the definition of the integral structure on $E^*_{H,\mathrm{et}}$ that the subgroup schemes $(\boldsymbol{\mu}_p)_Z, \{\pm 1\} \subseteq E_H$ *lift naturally* to closed subschemes

$$(\boldsymbol{\mu}_p)_Z, \{\pm 1\} \subseteq E^*_{H,\mathrm{et}}$$

hence that we obtain a natural lifting

$$(-\boldsymbol{\mu}_p)_Z \subseteq E^*_{H,\mathrm{et}}$$

of $(-\boldsymbol{\mu}_p)_Z \subseteq E_H$. On the other hand, by the *theory of theta groups* (cf., e.g., [7], Chapter IV, §1), we have a natural *theta trivialization*

$$\mathcal{L}_H|_{(-\boldsymbol{\mu}_p)_Z} \xrightarrow{\sim} \mathcal{L}_\epsilon \otimes_{\mathcal{O}_Z} \mathcal{O}_{(\boldsymbol{\mu}_p)_Z}$$

of the restriction of $\mathcal{L}_H$ to $(-\boldsymbol{\mu}_p)_Z$.

In particular, if we *restrict* sections of $\mathcal{L}_H$ over $E^*_{H,\mathrm{et}}$ to $(-\boldsymbol{\mu}_p)_Z$ and then apply the *theta trivialization*, we obtain a *morphism*

$$\Xi_{\mathcal{V}_H} : \mathcal{V}_H \to \mathcal{L}_\epsilon \otimes_{\mathcal{O}_Z} \mathcal{O}_{(\boldsymbol{\mu}_p)_Z}$$

whose restriction

$$\Xi_{\mathcal{H}_{\mathrm{DR}}} : \mathcal{H}_{\mathrm{DR}} \to \mathcal{L}_\epsilon \otimes_{\mathcal{O}_Z} \mathcal{O}_{(\boldsymbol{\mu}_p)_Z}$$

to $\mathcal{H}_{\mathrm{DR}} \overset{\mathrm{def}}{=} F^p(\mathcal{V}_H) \subseteq \mathcal{V}_H$ is "essentially" (i.e., up to taking H-invariants) the *restriction morphism appearing in the original Hodge-Arakelov Comparison Isomorphism* (cf. Theorem 1.1). That is to say, it follows from the main theorem of [7] that:

$$\Xi_{\mathcal{H}_{\mathrm{DR}}}|_{U_Z} \textit{ is an isomorphism.}$$

(In order to make it an isomorphism over Z, one must introduce the *"Gaussian poles"* on $\mathcal{H}_{\mathrm{DR}}$.) In particular, since the Galois group G *acts naturally on the range of* $\Xi_{\mathcal{H}_{\mathrm{DR}}}$, we get a natural action of G on the domain of $\Xi_{\mathcal{H}_{\mathrm{DR}}}$, at least over U_Z.

Definition 3.1. This action of G on $\mathcal{H}_{\mathrm{DR}}|_{U_Z}$ will be referred to as the *Lagrangian Galois action* on $\mathcal{H}_{\mathrm{DR}}$.

Remark 3.2. Note, in particular, that, unlike the Galois actions considered in [7], Chapter IX, §3; [10], §1 (cf. [12], §1.4.1, for a survey of this theory), the *Lagrangian Galois action depends on the choice of the subgroup H.* In fact, however, the choice of different splittings H does not affect the present theory very much. What is, however, essential here, is the existence of the natural *multiplicative subgroup scheme*:

$$\boldsymbol{\mu}_p|_{U_S} \subseteq E[p]|_{U_S}$$

Indeed, *this is the essential element of the present discussion in a "neighborhood of infinity" that does not exist in the number field case.* We will say more on this later (cf. Remark 3.7 below).

Remark 3.3. Just as was done in [12], §1.4.1, for the usual Galois action, once one has defined the Lagrangian Galois action, one may consider the corresponding *Lagrangian arithmetic Kodaira-Spencer morphism* by looking at the *extent to which the Hodge filtration $F^r(\mathcal{H}_{\mathrm{DR}})$ is preserved by the action of G.* We leave it to the reader to make the routine details (entirely similar to [12], §1.4.1) explicit. For more on this Lagrangian arithmetic Kodaira-Spencer morphism, we refer to Corollary 3.6 below.

Next, let us write

$$Z^{\log};\quad S^{\log}$$

for the *log schemes* obtained by equipping Z (respectively, S) with the log structure defined by the divisor $V(q^{\frac{1}{p}}) \subseteq Z$ (respectively, $V(q) \subseteq S$) and

$$\mathrm{Inf}(Z^{\log} \otimes k/\mathcal{O}_K)$$

for the site of *infinitesimal thickenings* of $Z^{\log} \otimes k$ over $\mathcal{O}_K$. Note that here, we do *not* assume that we are given a divided power structure on the ideal defining a thickening. Since, however, *all the higher p-curvatures of $(\mathcal{V}_H, \nabla_{\mathcal{V}_H})$ vanish* (cf. Corollary 2.7), it follows that the p-adic completion $(\widehat{\mathcal{V}}_H, \nabla_{\widehat{\mathcal{V}}_H})$ of $(\mathcal{V}_H, \nabla_{\mathcal{V}_H})$ defines a *crystal* on the site $\mathrm{Inf}(Z^{\log} \otimes k/\mathcal{O}_K)$.

In particular, since elements $\sigma \in G$ are all *congruent to the identity morphism on $Z^{\log}$* modulo $\mathfrak{m}$, it follows from the general theory of crystals on sites of thickenings that σ defines an automorphism

$$\int_\sigma : \widehat{\mathcal{V}}_H \xrightarrow{\sim} \widehat{\mathcal{V}}_H$$

which we denote by $\int_\sigma$, by analogy to *"integration/parallel transport along the (closed) path σ"* in the classical complex case. Now, taking into account the functoriality/naturality of all the definitions involved, we obtain the following *fundamental result* (cf. [10], Theorem 2.4):

Theorem 3.4. (The Crystalline Nature of the Lagrangian Galois Action) *For any $\sigma \in G$, the following diagram commutes:*

$$\begin{array}{ccc} \widehat{\mathcal{V}}_H & \xrightarrow{\Xi_{\widehat{\mathcal{V}}_H}} & \mathcal{L}_\epsilon \otimes_{\mathcal{O}_Z} \mathcal{O}_{(\boldsymbol{\mu}_p)_Z} \\ {\scriptstyle \int_\sigma}\downarrow & & \downarrow{\scriptstyle \sigma} \\ \widehat{\mathcal{V}}_H & \xrightarrow{\Xi_{\widehat{\mathcal{V}}_H}} & \mathcal{L}_\epsilon \otimes_{\mathcal{O}_Z} \mathcal{O}_{(\boldsymbol{\mu}_p)_Z} \end{array}$$

(where the "hats" denote p-adic completion, and the vertical morphisms are the natural morphisms associated to σ).

Put another way, Theorem 3.4 asserts that *the Lagrangian Galois action can be computed via "crystalline methods."* Thus, if one restricts the commutative diagram of Theorem 3.4 to $\mathcal{H}_{\mathrm{DR}} \subseteq \widehat{\mathcal{V}}_H$ and then applies a certain lemma (cf. [10], Lemma 2.6) derived from the theory of the *theta convolution* (cf. [8]; [12], §2) to the effect that $\Xi_{\widehat{\mathcal{V}}_H}$ and $\Xi_{\mathcal{H}_{\mathrm{DR}}}$ have the *same image* in $\mathcal{L}_\epsilon \otimes_{\mathcal{O}_Z} \mathcal{O}_{(\boldsymbol{\mu}_p)_Z}$, one obtains the following result (cf. [10], Corollary 2.5):

Corollary 3.5. (Elimination of Gaussian Poles) *The Lagrangian Galois action on $\mathcal{H}_{\mathrm{DR}}|_{U_Z}$ is, in fact, defined on $\mathcal{H}_{\mathrm{DR}}$ (i.e., without Gaussian poles).*

Finally, we would like to apply Theorem 3.4 to *relate the Lagrangian arithmetic Kodaira-Spencer morphism to the classical Kodaira-Spencer morphism.* To do this, we must consider the Lagrangian Galois action *modulo* $\mathfrak{m}^2$. First, we observe that it follows immediately from Theorems 2.8, 3.4 that for any $\sigma \in G$, the Lagrangian Galois action of σ on $\mathcal{H}_{\mathrm{DR}}$ maps

$$F^1(\mathcal{H}_{\mathrm{DR}}) \to F^3(\mathcal{H}_{\mathrm{DR}}) \otimes_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{m}^2)$$

in such a way that modulo $\mathfrak{m}$, $F^1(\mathcal{H}_{\mathrm{DR}})$ maps into $F^1(\mathcal{H}_{\mathrm{DR}})$. In particular, if we compose this map with the projection $F^3 \twoheadrightarrow F^3/F^2$ (cf. the discussion of §2.5), then we obtain an $\mathcal{O}_Z$-linear morphism

$$\begin{aligned} F^1(\mathcal{H}_{\mathrm{DR}}) \otimes_{\mathcal{O}_K} k &\to (F^3/F^2)(\mathcal{H}_{\mathrm{DR}}) \otimes_{\mathcal{O}_K} (\mathfrak{m}/\mathfrak{m}^2) \\ &\xrightarrow{\sim} (\tau_{E_H}^{\otimes 2} \otimes_{\mathcal{O}_Z} F^1(\mathcal{H}_{\mathrm{DR}})) \otimes_{\mathcal{O}_K} (\mathfrak{m}/\mathfrak{m}^2) \end{aligned}$$

— i.e., if we let $\sigma \in G$ *vary*, we obtain a homomorphism

$$\begin{aligned}\kappa_G : G = \mathbb{F}_p(1) &\to Hom_{\mathcal{O}_Z}(F^1(\mathcal{H}_{\mathrm{DR}}) \otimes_{\mathcal{O}_K} k, (\tau_{E_H}^{\otimes 2} \otimes_{\mathcal{O}_Z} F^1(\mathcal{H}_{\mathrm{DR}})) \otimes_{\mathcal{O}_K} (\mathfrak{m}/\mathfrak{m}^2)) \\ &= \tau_{E_H}^{\otimes 2} \otimes_{\mathcal{O}_K} (\mathfrak{m}/\mathfrak{m}^2).\end{aligned}$$

On the other hand, if we *forget about families of elliptic curves* and form the natural *exact sequence of differentials* associated to the triple $Z^{\log} \to S^{\log} \to \mathrm{Spec}(\mathcal{O}_K)$, we obtain an *extension of G-modules*:

$$\begin{aligned}0 \to \Omega_{\mathcal{O}_K/\mathbb{Z}_p} \otimes_{\mathcal{O}_K} \mathcal{O}_Z = (p^{-1} \cdot \mathfrak{m} \cdot \mathcal{O}_Z) \otimes_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{m}^{p-2}) &\to \Omega_{Z^{\log}/\mathbb{Z}_p} \\ &\to \Omega_{Z^{\log}/S^{\log}} = \Omega_{Z^{\log}/\mathcal{O}_K} \otimes \mathbb{F}_p \to 0\end{aligned}$$

(where all differentials involving $S^{\log}$, $Z^{\log}$ are understood to be *q-adically continuous*). By considering the extent to which sections of $\Omega_{Z^{\log}/\mathcal{O}_K} \otimes \mathbb{F}_p$ lift to G-invariant sections of $\Omega_{Z^{\log}/\mathbb{Z}_p}$, we thus obtain a homomorphism

$$G \otimes_{\mathbb{F}_p} (\Omega_{Z^{\log}/\mathcal{O}_K} \otimes \mathbb{F}_p) \to (p^{-1} \cdot \mathfrak{m} \cdot \mathcal{O}_Z) \otimes_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{m}^{p-2})$$

whose composite with the morphism induced by the projection $\mathfrak{m} \twoheadrightarrow \mathfrak{m}/\mathfrak{m}^2$ is easily verified to be an *isomorphism*

$$\delta : G \otimes_{\mathbb{F}_p} \mathcal{O}_{Z \otimes k} \xrightarrow{\sim} \Theta_{Z^{\log}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathfrak{m}/\mathfrak{m}^2$$

(cf. the theory of [1], I., §4) *relating the Galois group G to the (logarithmic) tangent bundle* $\Theta_{Z^{\log}/\mathcal{O}_K} \overset{\text{def}}{=} Hom_{\mathcal{O}_Z}(\Omega_{Z^{\log}/\mathcal{O}_K}, \mathcal{O}_Z)$ *modulo* $\mathfrak{m}$.

Thus, if we combine δ with κ_G, we obtain a morphism:

$$\kappa_G^{\delta} : \Theta_{Z^{\log}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} k \to \tau_{E_H}^{\otimes 2} \otimes_{\mathcal{O}_K} k$$

On the other hand, if we compute κ_G^{δ} by means of Theorems 2.10, 3.4, it follows that:

Corollary 3.6. (Relation to the Classical Kodaira-Spencer Morphism) *The morphism*

$$\kappa_G^{\delta} : \Theta_{Z^{\log}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} k \to \tau_{E_H}^{\otimes 2} \otimes_{\mathcal{O}_K} k$$

constructed by considering the Lagrangian Galois action modulo $\mathfrak{m}^2$ and applying the natural isomorphism

$$\delta : G \otimes_{\mathbb{F}_p} \mathcal{O}_{Z \otimes k} \xrightarrow{\sim} \Theta_{Z^{\log}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathfrak{m}/\mathfrak{m}^2$$

between the Galois group G and the (logarithmic) tangent bundle modulo $\mathfrak{m}$ is equal to $\frac{1}{2}$ the classical Kodaira-Spencer morphism associated to the family $E_H \to Z$.

Remark 3.7. From the point of view of *applications to diophantine geometry* (cf. [12], §1.5.1), one would like to develop an *analogue of the theory* of the present § over *number fields* — i.e., as opposed to over "formal neighborhoods of infinity" (cf. the base $S \stackrel{\text{def}}{=} \text{Spec}(\mathcal{O}_K[[q]])$), as in the present discussion. Indeed, as discussed in [12], §1.5.1, the main essential "missing link" necessary to apply Hodge-Arakelov theory to diophantine geometry is the *elimination of the Gaussian poles* — i.e., the number field analogue of Corollary 3.5. As discussed above (cf. Remark 3.2), the main ingredient that one needs in order to realize such a theory over number fields is an analogue over number fields of the *multiplicative subgroup scheme*:

$$\boldsymbol{\mu}_p|_{U_S} \subseteq E[p]|_{U_S}$$

— i.e., a *"global multiplicative subspace"* of the Tate module (of an elliptic curve over a number field). A first step towards realizing such a global multiplicative subspace is taken in [10], §3, where a global multiplicative subspace is constructed over the base:

$$(\overline{\mathcal{M}}_{\text{ell}})_{\mathbb{Q}}$$

It is then proposed in *loc. cit.* that perhaps by *restricting* this subspace over $(\overline{\mathcal{M}}_{\text{ell}})_{\mathbb{Q}}$ to a $\mathbb{Q}$-valued point, one may achieve the goal of constructing a global multiplicative subspace for elliptic curves over $\mathbb{Q}$. Unfortunately, this operation of restriction is not so straightforward, since it involves numerous intricacies related to the issue of *keeping track of basepoints* (of the various fundamental groups involved). Moreover, this issue of keeping track of basepoints appears to be related to Grothendieck's *anabelian geometry* (cf. [16]). It is the hope of the author to expose these ideas (cf. [17]) in a future sequel to the present manuscript.

§4. Hodge-Arakelov Theory in Positive Characteristic

In this §, we explain how a certain extension of the theory of §2.2 for ordinary elliptic curves to supersingular elliptic curves in positive characteristic can be used to give an alternate proof of Theorem 1.1. More details on the theory discussed here may be found in [11], §1, 2.

Let

$$E \to S$$

be a *family of elliptic curves* over an $\mathbb{F}_p$-scheme S such that the associated classifying morphism

$$S \to (\mathcal{M}_{\mathrm{ell}})_{\mathbb{F}_p}$$

is *étale*. In the following discussion, we will write $\Phi_S : S \to S$ for the *Frobenius morphism* on S, and denote the result of base-changing objects over S via Φ_S by means of a superscript F. Thus, the morphism

$$[p] : E \to E$$

(multiplication by p) factors as a composite of morphisms:

$$E \xrightarrow{\Phi_E} E^{\mathrm{F}} \xrightarrow{\mathcal{V}} E$$

where Φ_E is the *relative Frobenius morphism* of $E \to S$, and $\mathcal{V}$ is the *Verschiebung morphism*. As is well-known, the kernels of Φ_E and $\mathcal{V}$ are *Cartier dual* to one another:

$$E[\Phi_E] \xrightarrow{\sim} E^{\mathrm{F}}[\mathcal{V}]^*$$

Next, let us observe that the *pull-back*

$$\mathcal{V}^* E^\dagger \to E^{\mathrm{F}}$$

of the *universal extension* $E^\dagger \to E$ via $\mathcal{V}$ admits a *canonical section*:

$$\kappa : E^{\mathrm{F}} \to \mathcal{V}^* E^\dagger$$

Indeed, if we can show that the ω_E-torsor $\mathcal{V}^* E^\dagger \to E^{\mathrm{F}}$ is *trivial locally on* S, then κ may be defined as the unique section that takes the origin $0_{E^{\mathrm{F}}}$ of E^{F} to the origin of $\mathcal{V}^* E^\dagger$ (which is determined by the origin $0_{E^\dagger}$ of $E^\dagger$). Thus, it suffices to show that the ω_E-torsor in question is trivial locally on S. Since $\mathbf{R}^1 f_*(\omega_E)$ (where, by abuse of notation, we denote all structure morphisms to S by f) is a *line bundle* on S, it suffices to prove this local triviality in the case that $E \to S$ is *ordinary*. But then,

$\mathcal{V}^*$ induces an isomorphism $\omega_E \xrightarrow{\sim} \omega_{E^{\mathrm{F}}}$, so it follows that the morphism (again induced by $\mathcal{V}^*$)

$$\mathcal{O}_S \cong \mathbf{R}^1 f_*(\omega_E|_E) \to \mathbf{R}^1 f_*(\omega_{E^{\mathrm{F}}}|_{E^{\mathrm{F}}}) \cong \mathcal{O}_S$$

(where the isomorphisms on the two ends are the "trace maps" of the "residues and duality theory" of E, E^{F}) is given by multiplication by $p = \deg(\mathcal{V})$. Since we are working in characteristic p, this completes the proof that the ω_E-torsor $\mathcal{V}^*E^\dagger \to E^{\mathrm{F}}$ is trivial (locally on S).

Next, let us consider *structure sheaves*. Let us regard $\mathcal{O}_E^\dagger$ as a *quasi-coherent sheaf of $\mathcal{O}_E$-algebras* (via the projection $E^\dagger \to E$). Similarly, $\mathcal{V} : E^{\mathrm{F}} \to E$ allows us to regard $\mathcal{O}_{E^{\mathrm{F}}}$ as a *coherent sheaf of $\mathcal{O}_E$-algebras*. Thus, the morphism $\kappa : E^{\mathrm{F}} \to \mathcal{V}^*E^\dagger$ induces a morphism of quasi-coherent $\mathcal{O}_E$-modules:

$$\kappa^* : \mathcal{O}_E^\dagger \to \mathcal{O}_{E^{\mathrm{F}}}$$

Let us write $\mathcal{O}_{E^\dagger}^{<p} \subseteq \mathcal{O}_E^\dagger$ for the coherent subsheaf consisting of sections whose *torsorial degree* (i.e., relative degree over E) is $< p$. Thus, if we restrict κ^* to $\mathcal{O}_{E^\dagger}^{<p}$, we obtain a morphism

$$\mathcal{O}_{E^\dagger}^{<p} \to \mathcal{O}_{E^{\mathrm{F}}}$$

between *locally free $\mathcal{O}_E$-modules of rank p*. Now one has the following positive characteristic, degree $< p$ version of Theorem 2.2:

Theorem 4.1. (Verschiebung-Theoretic Analogue of the Hodge-Arakelov Comparison Isomorphism) *The morphism*

$$\mathcal{O}_{E^\dagger}^{<p} \to \mathcal{O}_{E^{\mathrm{F}}}$$

is an isomorphism.

Proof. First, we remark that the above discussion extends naturally to *degenerating elliptic curves* and hence is compatible with all natural integral structures in a neighborhood of infinity. For more details on this issue, we refer the reader to [11], §1.

Next, we observe that it essentially follows from Theorem 2.2 that the morphism in question is an *isomorphism over the ordinary locus in S*. Indeed, this is a consequence of the fact that the $\mathbb{F}_p$-vector space of all (set-theoretic) functions on $\mathbb{F}_p$ is spanned by the polynomial function on $\mathbb{F}_p$ of degree $< p$. Thus, in particular, the morphism in question is an isomorphism over a *dense open substack of* $(\overline{\mathcal{M}}_{ell})_{\mathbb{F}_p}$.

Thus, (by working over the *proper* stack $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$) it suffices to consider *determinants*. That is to say, it suffices to show (strictly speaking, not just over $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{F}_p}$, but also over $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$) that:

$$\det(\mathcal{O}_{E^\dagger}^{<p}) = \det(\mathcal{O}_{E^{\mathrm{F}}}) \in \mathrm{Pic}(E)_{\mathbb{Q}} \stackrel{\mathrm{def}}{=} \mathrm{Pic}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

Since $E^\dagger \to E$ is an ω_E-torsor, it follows immediately that

$$\det(\mathcal{O}_{E^\dagger}^{<p}) = \sum_{j=0}^{p-1} j \cdot [\tau_E] = -\frac{1}{2} p(p-1) \cdot [\omega_E]$$

(where we think of $\mathrm{Pic}(E)_{\mathbb{Q}}$ as an *additive* group). On the other hand, since $E^{\mathrm{F}}[\mathcal{V}] \stackrel{\sim}{\to} E[\Phi_E]^*$, we have:

$$\mathcal{O}_{E^{\mathrm{F}}[\mathcal{V}]} \stackrel{\sim}{\to} Hom_{\mathcal{O}_E}(\mathcal{O}_{E[\Phi_E]}, \mathcal{O}_E)$$

(as coherent $\mathcal{O}_E$-modules). Thus, since $E^{\mathrm{F}} \to E$ is a $E^{\mathrm{F}}[\mathcal{V}]$-*torsor*, we conclude that:

$$\begin{aligned} \det(\mathcal{O}_{E^{\mathrm{F}}}) &= \det(\mathcal{O}_{E^{\mathrm{F}}[\mathcal{V}]}) = -\det(\mathcal{O}_{E[\Phi_E]}) \\ &= -\sum_{j=0}^{p-1} j \cdot [\omega_E] = -\frac{1}{2} p(p-1) \cdot [\omega_E] \end{aligned}$$

(since $E[\Phi_E] \subseteq E$ is just an infinitesimal neighborhood of the origin 0_E). This completes the proof. Q.E.D.

Remark 4.2. A version of Theorem 4.1 where "$< p$" is replaced by "$< p^n$" (where $n \geq 1$ is an integer) is given in [11], Theorem 1.1.

Next, we consider *line bundles*. Let

$$\eta \in E(S)$$

be a *torsion point of order prime to p*. Write $\eta^{\mathrm{F}} \stackrel{\mathrm{def}}{=} \Phi_E(\eta) \in E^{\mathrm{F}}(S)$ and set:

$$\mathcal{L}^{\mathrm{F}} \stackrel{\mathrm{def}}{=} \mathcal{O}_{E^{\mathrm{F}}}([\eta^{\mathrm{F}}]); \quad \mathcal{M} \stackrel{\mathrm{def}}{=} \Phi_E^*(\mathcal{L}^{\mathrm{F}})$$

Thus, $\mathcal{L}^{\mathrm{F}}$ (respectively, $\mathcal{M}$) is a *line bundle of degree* 1 (respectively, *degree p*) on E^{F} (respectively, E). Since the order of η is *prime to p*, it follows that η^{F} *does not intersect* $0_{E^{\mathrm{F}}}$, hence that we have an isomorphism

$$f_*(\mathcal{L}^{\mathrm{F}}) \stackrel{\sim}{\to} \mathcal{L}^{\mathrm{F}}|_{0_{E^{\mathrm{F}}}}$$

given by restricting sections over E^{F} to $0_{E^{\mathrm{F}}}$. Now we are ready to apply the method of the above discussion to prove the following *positive characteristic version of Theorem* 1.1:

Theorem 4.3. (Positive Characteristic Version of the Hodge-Arakelov Comparison Isomorphism) *The natural restriction morphisms*

$$\Xi_{E^{\mathrm{F}}} : f_*(\mathcal{L}^{\mathrm{F}}|_{\mathcal{V}^* E^\dagger})^{<p} \to \mathcal{L}^{\mathrm{F}}|_{E^{\mathrm{F}}[\mathcal{V}]}$$

and

$$\Xi_E : f_*(\mathcal{M}|_{[p]^* E^\dagger})^{<p} \to \mathcal{M}|_{E[p]}$$

(*where the superscripted "$< p$'s" denote the subsheaves of sections of torsorial degree $< p$) induced by κ are isomorphisms.*

Proof. First, we observe that by the *theory of theta groups* (applied to descent via the Frobenius morphism $\Phi_E : E \to E^{\mathrm{F}}$) the bijectivity of $\Xi_{E^{\mathrm{F}}}$ is *equivalent* to that of Ξ_E. We refer to [11], §2, for more details.

Next, we observe that this discussion extends to the case of *degenerating elliptic curves* (cf. [11], §2, for more details). Thus, we may work over the proper stack $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$, so (just as in the proof of Theorem 4.1) it suffices to show that $\Xi_{E^{\mathrm{F}}}$ is *generically an isomorphism* and that the *determinant bundles* associated to its domain and range define the same element of $\mathrm{Pic}((\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p})_{\mathbb{Q}}$.

The fact that $\Xi_{E^{\mathrm{F}}}$ (or, equivalently, Ξ_E) is an isomorphism over an open dense substack of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$ follows from the theory of the comparison isomorphism near infinity developed in [7], Chapter V (cf. [11], §2, for more details).

On the other hand, the isomorphism

$$f_*(\mathcal{L}^{\mathrm{F}}) \xrightarrow{\sim} \mathcal{L}^{\mathrm{F}}|_{0_{E^{\mathrm{F}}}}$$

implies that (just as in the proof of Theorem 4.1) the determinants of the domain and range of $\Xi_{E^{\mathrm{F}}}$ are both equal to:

$$-\sum_{j=0}^{p-1} j \cdot [\omega_E] = -\frac{1}{2} p(p-1) \cdot [\omega_E]$$

This completes the proof. Q.E.D.

Remark 4.4. Thus, although in the above proof of Theorem 4.3, we use the (relatively easy) portion of the theory of [7] concerning the comparison isomorphism near infinity, the *intricate degree computations* of [7], Chapter VI, §3, are *not* used in the proof of Theorem 4.3. Also, we observe that although Theorem 4.3 is a positive characteristic result,

reduction modulo p implies Theorem 1.1, at least in the case $d = p$. Moreover, since the truth of the characteristic zero result Theorem 1.1 for arbitrary d is equivalent to the equality of the degrees of two specific line bundles, both of which are *polynomials in* d (cf. the complicated degree computations of [7], Chapter VI), the fact that these two polynomials are equal whenever d is a prime number implies that they are equal for all d. Thus, in summary, *the above technique yields a simple proof of Theorem 1.1 for arbitrary* d. We refer to [11], §2, for more details.

Remark 4.5. One way to interpret the preceding Remark 4.4 is the following:

> *The characteristic p methods (involving the Frobenius and Verschiebung morphisms) of the above discussion yield a new proof of the various combinatorial identities inherent in the computation of degrees in* [7]*, Chapter VI, proof of Theorem* 3.1.

This situation is rather reminiscent of the situation of [14], 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 4.6. One interesting feature of the above proof is the crucial use of the *Frobenius morphism* $\Phi_E : E \to E^{\mathrm{F}}$. Put another way, this amounts to the use of the subgroup scheme $E[\Phi_E] \subseteq E$ (i.e., the kernel of Φ_E), 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 the theory surveyed in §3. That is to say, it is interesting to note that just as in the context of §3, 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" $E[\Phi_E] \subseteq E$ (which is defined over all of $(\overline{\mathcal{M}}_{\mathrm{ell}})_{\mathbb{F}_p}$).

Remark 4.7. 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 the *Gaussian poles* (cf., e.g., [7], Introduction, §1).

References

[1] G. Faltings, p-adic Hodge Theory, *Journal of the Amer. Math. Soc.*, **1** (1988), pp. 255–299.

[2] G. Faltings, Crystalline Cohomology and p-adic Galois Representations, *Proceedings of the First JAMI Conference*, Johns-Hopkins University Press, 1990, pp. 25–79.

[3] N. Katz, Nilpotent Connections and the Monodromy Theorem: Applications of a Result of Turritin, *Publ. Math. IHES*, **39** (1970), pp. 355–412.

[4] N. Katz, Algebraic solutions of differential equations (p-curvature and the Hodge filtration), *Invent. Math.*, **18** (1972), pp. 1–118.

[5] N. Katz, The Eisenstein Measure and p-adic Interpolation, *Amer. Journ. of Math.*, **99**, No. 2 (1977), pp. 238–311.

[6] N. Katz, Serre-Tate Local Moduli, in *Surfaces algébriques, Séminaire de Géométrie Algébrique, 1976–78*, edited by Jean Giraud, Luc Illusie and Michel Raynaud, Lecture Notes in Mathematics, **868**, Springer-Verlag, 1981.

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

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

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

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

[11] S. Mochizuki, *The Hodge-Arakelov Theory of Elliptic Curves in Positive Characteristic*, RIMS Preprint, No. 1298 (October 2000).

[12] S. Mochizuki, *A Survey of the Hodge-Arakelov Theory of Elliptic Curves I*, to appear in *Moduli of Profinite Aspects of Arithmetic Covers* (M. Fried, editor), AMS Publications.

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

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

[15] S. Mochizuki, The Profinite Grothendieck Conjecture for Closed Hyperbolic Curves over Number Fields, *J. Math. Sci., Univ. Tokyo*, **3** (1996), pp. 571–627.
[16] S. Mochizuki, The Local Pro-p Anabelian Geometry of Curves, *Inv. Math.*, **138** (1999), pp. 319–423.
[17] S. Mochizuki, *The Geometry of Anabelioids*, manuscript in preparation.
[18] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, *Grundlehren der Mathematischen Wissenschaften*, **323**, Springer-Verlag, 2000.

Research Institute for Mathematical Sciences
Kyoto University
Kyoto, 606-8502
Japan