The Galois-Theoretic Kodaira-Spencer Morphism of an Elliptic Curve

Shinichi Mochizuki

July 2000

Contents:

Section 0: Introduction

The purpose of this paper is to study in greater detail the *arithmetic Kodaira-Spencer morphism* of an elliptic curve introduced in [Mzk1], Chapter IX, in the general context of the *Hodge-Arakelov theory of elliptic curves*, developed in [Mzk1-3]. In particular, after correcting a minor error (cf. Corollary 1.6) in the construction of this arithmetic Kodaira-Spencer morphism in [Mzk1], Chapter IX, §3, we define (cf. §2.1) a slightly modified *"Lagrangian"* version of this arithmetic Kodaira-Spencer morphism which has the following *remarkable properties*:

(1) This Lagrangian arithmetic Kodaira-Spencer morphism is *free of Gaussian poles* (cf. Corollary 2.5).

(2) A certain portion of the reduction modulo p of this Lagrangian arithmetic Kodaira-Spencer morphism may be naturally identified with the usual *geometric Kodaira-Spencer morphism* (cf. Corollary 2.7).

We recall that property (1) is of substantial interest since it is the Gaussian poles that are *the main obstruction to applying the Hodge-Arakelov theory of elliptic curves to diophantine geometry* (cf. the discussion of [Mzk1], Introduction, §5.1, for more details). On the other hand, property (2) is of substantial interest in that

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

it shows quite definitively that the analogy asserted in [Mzk1], Chapter IX, between the arithmetic Kodaira-Spencer morphism of the Hodge-Arakelov theory of elliptic curves and the usual geometric Kodaira-Spencer morphism of a family of elliptic curves is *not just philosophy, but rigorous mathematics!* (cf. the Remark following Corollary 2.7 for more details). In fact, both properties (1) and (2) are essentially formal consequences of a property that we refer to as the *"crystalline nature of the Lagrangian Galois action"* (cf. Theorem 2.4). Interestingly, the theory of §2 of the present paper makes essential use not only of the theory of [Mzk1], but also of [Mzk2], [Mzk3].

Unfortunately, however, this Lagrangian arithmetic Kodaira-Spencer morphism, which is based on a certain *"Lagrangian Galois action,"* can only be defined when there is a natural (rank one) *multiplicative subspace* (i.e., "weight 1" subspace) of the Tate module of the elliptic curve in question. Since such a subspace is well-known to exist in a *formal neighborhood of infinity* (of the compactified moduli stack of elliptic curves), we work over such a base in §2. Ultimately, however, one would like to carry out this construction for elliptic curves over *number fields*. In §3, 4, we discuss a certain point of view that suggests that this may be possible — cf. especially, §4, "Conclusion." It is the hope of the author to complete the construction motivated in §3,4 in a future paper.

Notation and Conventions:

We will denote by $(\overline{\mathcal{M}}_{1,0}^{\log})_{\mathbb{Z}}$ 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. The open substack of $(\overline{\mathcal{M}}_{1,0})_{\mathbb{Z}}$ parametrizing (smooth) elliptic curves will be denoted by $(\mathcal{M}_{1,0})_{\mathbb{Z}} \subseteq (\overline{\mathcal{M}}_{1,0})_{\mathbb{Z}}$.

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

Section 1: Galois Actions on the Torsion Points

In this §, we study various *Galois actions* on the space of functions on the set of torsion points of an elliptic curve. In particular, we observe that these actions give rise to a natural action of the *"algebraic fundamental groupoid"* of the base of a family of elliptic curves on the scheme of torsion points over this base. This action allows us to *correct an error* made in [Mzk1], Chapter IX, in the definition given there of the *arithmetic Kodaira-Spencer morphism.*

Let $S^{\log}$ be a *fine noetherian log scheme* whose underlying scheme S is *connected and normal.* Write $U_S \subseteq S$ for the open subscheme where the log structure is trivial. In the following discussion, we shall assume that $U_S \neq \emptyset$. Next, let us assume that we are given a *log elliptic curve* (cf. §0, Notations and Conventions)

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

(whose associated one-dimensional semi-abelian scheme we denote by $E \to S$) and a *positive integer* $d \geq 1$ which is *generically invertible on* S (i.e., invertible on a schematically dense open subscheme of S). Next, let us write

$$U_T[d^{-1}] \subseteq E|_{U_S[d^{-1}]}$$

(where $U_S[d^{-1}] \stackrel{\text{def}}{=} U_S \otimes_{\mathbb{Z}} \mathbb{Z}[d^{-1}]$) for the kernel of the *finite, étale morphism* $[d] : E|_{U_S[d^{-1}]} \to E|_{U_S[d^{-1}]}$ of degree d^2 (given by multiplication by d). Thus, $U_T[d^{-1}] \to U_S[d^{-1}]$ is finite étale of degree d^2. Let us write

$$T \to S$$

for the *normalization* of S in $U_T[d^{-1}]$, $U_T \stackrel{\text{def}}{=} T|_{U_S}$ (so $U_T[d^{-1}] = U_T \otimes_{\mathbb{Z}} \mathbb{Z}[d^{-1}]$). Also, let us assume that we are given a connected, normal scheme Z over S such that if we write $U_Z \stackrel{\text{def}}{=} Z|_{U_S}$, $U_Z[d^{-1}] \stackrel{\text{def}}{=} U_Z \otimes_{\mathbb{Z}} \mathbb{Z}[d^{-1}]$, then $U_Z[d^{-1}] \to U_S[d^{-1}]$ is *finite étale and Galois*; $U_Z[d^{-1}] \to U_S[d^{-1}]$ dominates every connected component of $U_T[d^{-1}]$; and Z is the *normalization* of S in $U_Z[d^{-1}]$.

Next, we consider *étale fundamental groups.* Write

$$\Pi_S$$

for the fundamental group $\pi_1(U_S[d^{-1}])$ (for some choice of base-point, which we omit in the notation since it is irrelevant to our discussion). Then since $U_Z[d^{-1}] \to U_S[d^{-1}]$ is *Galois*, it follows that Π_S *acts naturally* on $U_Z[d^{-1}]$, hence also on Z (over S). In particular, Π_S acts naturally on the *module of d-torsion points*

$$M \stackrel{\text{def}}{=} \mathrm{Mor}_S(Z, T)$$

(where we observe that, as an abstract $\mathbb{Z}$-module, $M \cong (\mathbb{Z}/d\mathbb{Z})^2$). In the following discussion, we shall think of the action of Π_S on Z as an action from the *right*, and the action of Π_S on $\mathcal{O}_Z$, M as an action from the *left.*

Next, let us us consider the *$\mathcal{O}_Z$-algebra*

$$\mathcal{F} \stackrel{\text{def}}{=} \mathrm{Func}(M, \mathcal{O}_Z)$$

of *$\mathcal{O}_Z$-valued functions on the finite set M*. Then observe that Π_S *acts on $\mathcal{F}$ in several different ways*, e.g., via the action of Π_S on M, via the action of Π_S on $\mathcal{O}_Z$, etc.

Definition 1.1. We shall refer to the $\mathcal{O}_Z$-linear (respectively, semi-linear, relative to the action of Π_S on $\mathcal{O}_Z$) action of Π_S from the right (respectively, left) on $\mathcal{F}$ induced by the action of Π_S on M (respectively, $\mathcal{O}_Z$) as the *point-theoretic action* (respectively, *value-theoretic action*) of Π_S on $\mathcal{F}$. We shall refer to the $\mathcal{O}_Z$-semilinear action of Π_S on $\mathcal{F}$ from the left given by composing the value-theoretic action with the inverse of the point-theoretic action (i.e., if $\sigma \in \Pi_S$, and $\phi \in \mathcal{F}$, then σ maps ϕ to the function $M \ni m \mapsto \sigma(\phi(\sigma^{-1}m))$) as the *diagonal action* of Π_S on $\mathcal{F}$. We shall abbreviate the term "point-theoretic action" (respectively, "value-theoretic action"; "diagonal action") by the term *P-action* (respectively, *V-action*; *D-action*).

Proposition 1.2. *There is a natural inclusion $\iota : \mathcal{O}_T \hookrightarrow \mathcal{F}$ of $\mathcal{O}_S$-algebras which induces an isomorphism of $\mathcal{O}_T$ onto the subalgebra of $\mathcal{F}$ of Π_S-invariants with respect to the D-action. Moreover, this inclusion induces an isomorphism*

$$(\mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_Z)^{\mathrm{norm}} \xrightarrow{\sim} \mathcal{F}$$

(where the superscript "norm" denotes the normalization of the ring in parentheses) which is Π_S-equivariant with respect to the tensor product of the trivial action of Π_S on $\mathcal{O}_T$ and the natural action of Π_S on $\mathcal{O}_Z$ on the **left***, and the D-action of Π_S on $\mathcal{F}$ on the* **right***.*

Proof. It is a tautology (cf. the definition $M \stackrel{\mathrm{def}}{=} \mathrm{Mor}_S(Z, T)$) that elements of M define $\mathcal{O}_S$-algebra homomorphisms $\mathcal{O}_T \to \mathcal{O}_Z$. Thus, if we take the direct product of these various homomorphisms, then we get an $\mathcal{O}_S$-algebra homomorphism

$$\iota : \mathcal{O}_T \to \mathcal{F}$$

(cf. the definition of $\mathcal{F}$ — i.e., $\mathcal{F} \stackrel{\mathrm{def}}{=} \mathrm{Func}(M, \mathcal{O}_Z)$). Moreover, it is a tautology that $\mathcal{O}_T$ maps into the subalgebra of Π_S-invariants of $\mathcal{F}$ relative to the D-action. Since $\mathcal{O}_T$ and $\mathcal{F}$ are both *normal algebras*, in order to verify the remaining assertions of Proposition 1.2, it suffices to verify that these assertions hold over $U_S[d^{-1}]$. To simplify notation, *we assume (just for the remainder of this proof) that $S = U_S[d^{-1}]$*.

Thus, $T \to S$ and $Z \to S$ are *finite étale*, so, by (Galois) étale descent (with respect to the morphism $Z \to S$), it follows that the Π_S-invariants of $\mathcal{F}$ form an $\mathcal{O}_S$-algebra $\mathcal{O}_{T'}$, whose spectrum T' over S is *finite étale* over S. Moreover, $T' \to S$ factors (cf. the discussion of the preceding paragraph) through T. Thus, since T' and T are both finite étale of degree equal to the cardinality of M (i.e., d^2) over S, we obtain that $T' = T$, as desired. The fact that the induced morphism $\mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_Z \xrightarrow{\sim} \mathcal{F}$ is an isomorphism then follows from elementary properties of étale descent. This completes the proof. $\bigcirc$

Next, we would like to use the V-action of Π_S on $\mathcal{F}$ to construct *"some sort of group action" on $\mathcal{F}$ which descends to an action on $\mathcal{O}_T$*. If, for instance, the V-action of Π_S on $\mathcal{F}$ were *equivariant* with respect to the D-action of Π_S on $\mathcal{F}$, then the V-action itself would define an action of Π_S on $\mathcal{F}$ that descends to an action on $\mathcal{O}_T$. In fact, however, *this sort of equivariance does not hold in the naive sense*, but only in the following *"twisted sense"*:

First, let us define the *profinite group with* Π_S*-action* Γ_S as follows: We take the underlying profinite group of Γ_S to be Π_S itself. The Π_S-action on Γ_S is defined to be the action given by: $\sigma(\gamma) \stackrel{\text{def}}{=} \sigma \cdot \gamma \cdot \sigma^{-1}$ (for $\sigma \in \Pi_S$, $\gamma \in \Gamma_S$). Next, we endow $\mathcal{F}$ with the Γ_S*-action* defined by thinking of Γ_S as Π_S and using the *V-action* of Π_S on $\mathcal{F}$ (cf. Definition 1.1). Then we have the following:

Proposition 1.3. *The* Γ_S*-action on* $\mathcal{F}$ *is compatible with the* Π_S*-actions on* Γ_S *and* $\mathcal{F}$ *(where we think of* Π_S *as acting on* $\mathcal{F}$ *by the D-action).*

Proof. Indeed, if $\sigma \in \Pi_S$, $\gamma \in \Gamma_S$, $\phi \in \mathcal{F}$, $m \in M$, then:

$$\begin{aligned}
\Big(\sigma^D\{\gamma(\phi)\}\Big)(m) &= \sigma \cdot \{\gamma(\phi)\}(\sigma^{-1} \cdot m) \\
&= \sigma \cdot \gamma \cdot \phi(\sigma^{-1} \cdot m) \\
&= \sigma \cdot \gamma \cdot \sigma^{-1} \cdot \sigma \cdot \phi(\sigma^{-1} \cdot m) \\
&= \sigma(\gamma) \cdot \sigma \cdot \phi(\sigma^{-1} \cdot m) \\
&= \sigma(\gamma) \cdot \{\sigma^D(\phi)\}(m) \\
&= \Big\{\sigma(\gamma) \cdot \Big(\{\sigma^D(\phi)\}\Big)\Big\}(m)
\end{aligned}$$

(where the superscript D denotes the D-action of the group element bearing the superscript). This completes the proof. ○

Let us write $\mathrm{Gal}(Z/S)$ for the Galois group of the Galois covering $U_Z[d^{-1}] \to U_S[d^{-1}]$. Then by forming the quotient of Z by the action of $\mathrm{Gal}(Z/S)$ *in the sense of stacks*, we obtain an *algebraic stack* S_Z^{sk}, together with morphisms

$$Z \to S_Z^{\mathrm{sk}} \to S$$

where the first morphism is *Galois, finite étale* (with Galois group $\mathrm{Gal}(Z/S)$), and the second morphism is an *isomorphism over* $U_S[d^{-1}]$. If we let Z range over all connected Galois, finite étale coverings of S, the inverse limit of the Z (respectively, S_Z^{sk}) thus defines a *"pro-scheme"* $\widetilde{S}$ (respectively, *"pro-algebraic stack"* S^{sk}) over S, together with morphisms:

$$\widetilde{S} \to S^{\mathrm{sk}} \to S$$

(where the first morphism is "Galois, profinite étale" (with Galois group Π_S) and the second morphism is an *isomorphism over* $U_S[d^{-1}]$). Moreover, by étale descent, the "profinite group with Π_S-action" Γ_S defines a *profinite étale group scheme* Γ_S^{sk} over S^{sk}.

Definition 1.4. We shall refer to Γ_S^{sk} as the *algebraic fundamental groupoid* of $S^{\log}$.

Note that since $Z \to S_Z^{\mathrm{sk}}$ is *finite (Galois) étale*, the D-action of Π_S on $Spec(\mathcal{F})$ (where "*Spec*" is to be understood as being taken with respect to the structure of $\mathcal{O}_Z$-algebra on $\mathcal{F}$) defines *descent data* for $Spec(\mathcal{F})$ with respect to $Z \to S_Z^{\mathrm{sk}}$ (hence, a fortiori, with respect to $\widetilde{S} \to S^{\mathrm{sk}}$). We shall denote the resulting descended object over S^{sk} by:

$$T^{\mathrm{sk}} \to S^{\mathrm{sk}}$$

Note that over $U_S[d^{-1}]$, we have $T^{\mathrm{sk}}|_{U_S[d^{-1}]} = T|_{U_S[d^{-1}]}$ (by Proposition 1.2).

Corollary 1.5. *The action of* Γ_S *on* $\mathcal{F}$ *descends to an action of the algebraic fundamental groupoid* Γ_S^{sk} *on* T^{sk}.

Proof. This follows immediately from Proposition 1.2, 1.3. ○

Remark. The terminology of Definition 1.4 may be justified as follows: First, let us recall the well-known analogy between algebraic fundamental groups (such as Π_S) and the usual topological fundamental groups of algebraic topology. This analogy gives us the freedom to phrase our justification in the language of *topological fundamental groups*. Thus, let X be a *topological manifold*. Note that for each point $x \in X$, we obtain (in a natural way) a *group*:

$$x \mapsto \pi_1(X, x)$$

i.e., the fundamental group with base-point x. This correspondence defines a local system of groups on X, which is known (in algebraic topology) as the *fundamental groupoid* of X. On the other hand, there is a well-known equivalence of categories between local systems of groups on X and groups G equipped with an action of $\pi_1(X, x)$ (given by associating to such a local system its fiber at x, together with the "monodromy action" of $\pi_1(X, x)$). Moreover, it is an easy exercise to check that, relative to this equivalence of categories, the fundamental groupoid corresponds to the "group with $\pi_1(X, x)$-action" defined by letting $\pi_1(X, x)$ *act on itself via conjugation* (cf. the definition given above for the Π_S-action on Γ_S). Thus, in summary, one may regard the object Γ_S^{sk} as the *algebraic analogue of the fundamental groupoid*. This justifies the terminology of Definition 1.4.

Remark. One other interesting observation relative to the appearance of the *algebraic fundamental groupoid* (cf. Definition 1.4 — i.e., as opposed to *group*) in the correct formulation of the arithmetic Kodaira-Spencer morphism (cf. Corollary 1.6 below) is the following. Recall that in the asserted *analogy* between the arithmetic Kodaira-Spencer morphism of [Mzk1], Chapter IX, and the usual geometric

Kodaira-Spencer morphism, the *Galois group/fundamental group(oid) of the base plays the role of the tangent bundle of the base*. On the other hand, the tangent bundle of the base (typically) does not admit a canonical global trivialization, but instead *varies from point to point* — i.e., at a given point, it consists of *infinitesimal motions originating from that point*. Thus, it is natural that the arithmetic analogue of the tangent bundle should be not the "static" fundamental group, but instead the fundamental groupoid, which *varies* from point to point, and indeed, at a given point, consists of *paths* (which may be thought of as a sort of "motion") *originating from that point*.

We are now ready to apply the above discussion to correct an *error* made in [Mzk1], Chapter IX, in the definition given there of the *arithmetic Kodaira-Spencer morphism*:

> In [Mzk1], Chapter IX, Theorem 3.3, and the discussion preceding it, it is *falsely* asserted that there is a natural action ("with denominators") of Π_S on $\mathcal{H}_{\mathrm{DR}}$ (notation of *loc. cit.*) arising from a natural action of Π_S on $T \to S$ (notation of the present discussion).

Although this assertion does indeed hold if the S-scheme T happens to be a *disjoint union of copies of* S, in general, it is false. That is to say, the correct formulation of this assertion is that the "twisted object" Γ_S^{sk} acts on T^{sk} (not that Π_S acts on T).

Corollary 1.6. (Correction to Error in [Mzk1], Chapter IX, §3) *The phrase "natural action of* Π_S *on ...* $\mathcal{H}_{\mathrm{DR}}$*" in [Mzk1], Chapter IX, Theorem 3.3, should read*

$$\text{"natural action of } \Gamma_S^{\mathrm{sk}} \text{ on ... } \mathcal{H}_{\mathrm{DR}}|_{S^{\mathrm{sk}}}\text{"}$$

(where "$|_S^{\mathrm{sk}}$*" denotes the pull-back via the morphism* $S^{\mathrm{sk}} \to S$*), and the divisor of possible poles "*$[\eta \bigcap ({}_dE)] + V(4)$*" should read*

$$[\eta \bigcap ({}_dE)] + V(d)$$

In particular, the resulting **"arithmetic Kodaira-Spencer morphism"** $\kappa_E^{\mathrm{arith}} : \Pi_S \to \mathfrak{Filt}(\mathcal{H}_{\mathrm{DR}})(S)$ *((erroneous) notation of [Mzk1], Chapter IX, §3) should in fact be thought of as a morphism*

$$\kappa_E^{\mathrm{arith,\ sk}} : \Gamma_S^{\mathrm{sk}} \to \mathfrak{Filt}(\mathcal{H}_{\mathrm{DR}})|_{S^{\mathrm{sk}}}$$

of sheaves on the étale site of S^{sk}.

Proof. It remains only to remark that the reason for the divisor "$V(d)$" (i.e., the zero locus of the regular function determined by the integer d) is that the integral structure on the pull-back to Z (notation of the present discussion) of $\mathcal{O}_{{}_dE}$ differs from that of $\mathcal{F}$ (cf. the notation "norm" appearing in Proposition 1.2) by a factor which is bounded by the *different* of the algebra $\mathcal{O}_{_dE}$. Moreover, the fact that this different divides d follows from the fact that multiplication by d on an elliptic curve induces multiplication by d on the differentials of the elliptic curve. ○

Remark. Thus, in summary, what is done in [Mzk1], Chapter IX, §3, is *literally correct when $T \to S$ happens to be a disjoint sum of copies of S* (a condition which may be achieved by base-change). In general, however, there is a certain *"twist"* that must be taken into account, but which was overlooked in the discussion of [Mzk1], Chapter IX.

Section 2: Lagrangian Galois Actions

In this §, we study the Galois action on the torsion points of an elliptic curve, along with the resulting "arithmetic Kodaira-Spencer morphism" (cf. §1) *under the assumption that this Galois action preserves a "rank one multiplicative submodule " of the module of torsion points.* In this situation, we show that the resulting "Lagrangian Galois action" is defined *without Gaussian poles*, and, moreover, that a "certain piece" of the resulting arithmetic Kodaira-Spencer morphism *coincides with the classical Kodaira-Spencer morphism* (cf. §2.2). This further strengthens the analogy discussed in [Mzk1], Chapter IX, between the arithmetic (or "Galois-theoretic") Kodaira-Spencer morphism and the classical ("geometric") Kodaira-Spencer morphism.

§2.1. Definition and Construction

In this §, we maintain the notation of §1. Moreover, we assume that we are given a Π_S-submodule $M^\mu \subseteq M$ whose underlying $\mathbb{Z}/d\mathbb{Z}$-submodule is *free of rank one*. Thus, we obtain an exact sequence of Π_S-modules

$$0 \to M^\mu \to M \to M^{\mathrm{et}} \to 0$$

(where M^{et} is defined so as to make this sequence exact). Thus, restricting $\mathcal{O}_Z$-valued functions on M to M^μ gives rise to a *surjection*

$$\mathcal{F} = \mathrm{Func}(M, \mathcal{O}_Z) \twoheadrightarrow \mathcal{F}^\mu \stackrel{\mathrm{def}}{=} \mathrm{Func}(M^\mu, \mathcal{O}_Z)$$

of $\mathcal{O}_Z$-algebras. Observe that the *V-action* (cf. Definition 1.1) of Π_S on $\mathcal{F}$ manifestly preserves this surjection, so we get a natural *V-action of* Π_S *on* $\mathcal{F}^\mu$. Since, moreover, we are operating under the assumption that Π_S *preserves the submodule* $M^\mu \subseteq M$, it thus follows that the *P- and D-actions* (cf. Definition 1.) of Π_S on $\mathcal{F}$ also preserve this surjection, so we also get natural *P- and D-actions of* Π_S *on*

$\mathcal{F}^\mu$. In particular, (cf. Proposition 1.2) taking the spectrum (over S) of the Π_S-invariants of $\mathcal{F}^\mu$ with respect to the D-action gives rise to a scheme T^μ together with a morphism

$$T^\mu \to T$$

which is a *closed immersion over* $U_S[d^{-1}]$. (Note that since the operation of taking Π_S-invariants is not necessarily right exact, it is not clear whether or not $T^\mu \to T$ is a closed immersion over S.)

Next, let us suppose that we are given a *splitting*

$$M^{\mathrm{H}} \subseteq M$$

of the surjection of modules $M \twoheadrightarrow M^{\mathrm{et}}$ (i.e., a submodule $M^{\mathrm{H}} \subseteq M$ such that the morphism $M^{\mathrm{H}} \to M^{\mathrm{et}}$ is bijective), which is *not necessarily preserved by* Π_S. Even if M^{H} is not preserved by Π_S, however, since $M^\mu \subseteq M$ is preserved by Π_S, it follows that *an element* $\sigma \in \Pi_S$ *will always carry* $M^{\mathrm{H}} \subseteq M$ *to another splitting* ${M^{\mathrm{H}}}^\sigma \subseteq M$ *of the surjection* $M \twoheadrightarrow M^{\mathrm{et}}$.

Next, we return to the "de Rham point of view," and consider sections of line bundles on the *universal extension* of E. Also, for simplicity, we assume from now on that S is $\mathbb{Z}$-*flat*, and that d is *odd*. Then we would like to consider the *Hodge-Arakelov Comparison Isomorphism* (cf. [Mzk1], Introduction, Theorem A), so, in the following discussion, we will use the *notation of [Mzk1], Introduction, and [Mzk3], §9*. (Here, we recall that certain minor errors in [Mzk1], Introduction, Theorem A were corrected in [Mzk3], §9, Theorem 9.2.) Thus, we assume that we have been given an *integer* m *that does not divide* d, together with a *torsion point*

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

of order precisely m which defines a *metrized line bundle* $\overline{\mathcal{L}}_{\mathrm{st},\eta}$ on $E_{\infty,S}$ (cf. [Mzk1], Chapter V, §1). 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 N-th roots of the q-parameter" (as N 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. For simplicity, we shall also assume that $n \overset{\mathrm{def}}{=} 2m$ *is invertible on* S. In the following discussion, we shall simply write $\overline{\mathcal{L}}$ for $\overline{\mathcal{L}}_{\mathrm{st},\eta}$. Thus, in particular, over U_S:

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

Also, let us write

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

for the object which is equal to $E_Z \stackrel{\text{def}}{=} E \times_S Z$ over U_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 complement of the nodes of 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 $T \mapsto T + \frac{j}{d}$, $\forall j \in \mathbb{Z}$.

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:

$$1 \to (\mathbb{G}_m)_Z \to \mathcal{G}_Z \to {}_dE_Z \to 1$$

(where ${}_dE_Z$ $(\subseteq E_{d,Z})$ $\to Z$ is the finite flat group scheme of d-torsion points). Let us suppose that the submodules $M^\mu, M^{\text{H}} \subseteq M$ arise from the restriction to $U_Z[d^{-1}]$ of *finite flat group schemes*

$$G^\mu_Z, H_Z \subseteq {}_dE_Z$$

over Z such that the resulting morphism $G^\mu_Z \times_Z H_Z \to {}_dE_Z$ is an *isomorphism of group schemes.* Thus, (cf. Proposition 1.2) we have a *natural inclusion*

$$\mathcal{O}_{G^\mu_Z} \hookrightarrow \mathcal{F}^\mu$$

of finite $\mathcal{O}_Z$-algebras, which is an *isomorphism over* $U_Z[d^{-1}]$. In the following discussion, we also *assume that* G^μ_Z *has been chosen so that the subalgebra* $\mathcal{O}_{G^\mu_Z} \hookrightarrow \mathcal{F}^\mu$ *is preserved by the various actions (i.e., V-, P-, D-) of* Π_S *on* $\mathcal{F}^\mu$. Finally, 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 $\mathcal{G}_Z \to {}_dE_Z$). (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* $\overline{\mathcal{L}}$.

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*

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

of the pull-back $\overline{\mathcal{L}}_{E^*_{[d],\mathrm{et},Z}}$ of the metrized line bundle $\overline{\mathcal{L}}$ to $E^*_{[d],\mathrm{et},Z}$. (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. Also, often we would like to consider the *filtration* $F^r(\mathcal{V}_{\overline{\mathcal{L}}}) \subseteq \mathcal{V}_{\overline{\mathcal{L}}}$ *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 $E^*_{[d],\mathrm{et},Z}$ over $(U_Z)_{\mathbb{Q}}$, this definition also applies to sections of $\mathcal{V}_{\overline{\mathcal{L}}}$.) In particular, we shall write

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

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

Next, let us observe that (by the assumption that $n = 2m$ is invertible on S) the d-torsion subgroup scheme ${}_dE_Z \subseteq E_{d,Z}$ *lifts (uniquely!) to a subgroup scheme*:

$${}_dE^* \subseteq E^*_{[d],\mathrm{et},Z}$$

(Indeed, this 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 integral values $\in \mathcal{O}_S$ for all $T = \frac{j}{d}$ (for $j \in \mathbb{Z}$).) Moreover, we recall from [Mzk1], Chapter IX, §3, that (since d is *odd*) we have a *"theta trivialization"*

$$\overline{\mathcal{L}}|_{{}_dE_Z} \cong \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{{}_dE_Z}$$

(where $0_{E_Z} \in E_Z(Z)$ is the zero section of $E_Z \stackrel{\mathrm{def}}{=} E \times_S Z \to Z$) of the restriction of $\overline{\mathcal{L}}$ to ${}_dE_Z \subseteq E_{d,Z}$. Note, moreover, 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* $\overline{\mathcal{L}}_{0_{E_Z}}$.

Thus, by restricting sections of $\mathcal{L}$ over $E^*_{[d],\mathrm{et},Z}$ to ${}_dE^* \subseteq E^*_{[d],\mathrm{et},Z}$, and composing with the theta trivialization reviewed above, we obtain a morphism:

$$\Xi_{\mathcal{V}} : \mathcal{V}_{\overline{\mathcal{L}}} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{{}_dE_Z}$$

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

$$\Xi^{\mathrm{GP}}_{\mathcal{V}} : \mathcal{V}^{\mathrm{GP}}_{\overline{\mathcal{L}}} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{{}_dE_Z}$$

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

Theorem 2.1. **(Review of the Main Result of [Mzk1])** *Assume that d is* **odd** *and that $n \stackrel{\mathrm{def}}{=} 2m$ is* **invertible on** *S. Then restriction of sections of $\overline{\mathcal{L}}$ over $E^*_{[d],\mathrm{et},Z}$ to the d-torsion points, composed with the canonical "theta trivialization" of $\overline{\mathcal{L}}$ over the d-torsion points yields a morphism*

$$\Xi_{\mathcal{V}} : \mathcal{V}_{\overline{\mathcal{L}}} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{{}_dE_Z}$$

whose restriction

$$\Xi_{\mathcal{H}} : \mathcal{H}_{\mathrm{DR}} \to \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{{}_dE_Z}$$

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

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

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

Proof. We refer to [Mzk1], Introduction, Theorem A, especially (2), (3). Note that the "zero locus of the determinant" is empty because of our assumption that n is invertible on S. ◯

Next, let us observe that it follows from the fact that the morphism $G^\mu_Z \times_Z H_Z \to {}_dE_Z$ is an *isomorphism of group schemes* that the composite

$$\mathcal{O}^{H_Z}_{{}_dE_Z} \subseteq \mathcal{O}_{{}_dE_Z} \twoheadrightarrow \mathcal{O}_{G^\mu_Z}$$

(where $\mathcal{O}^{H_Z}_{{}_dE_Z}$ denotes the subalgebra of $\mathcal{O}_{{}_dE_Z}$ of functions which are invariant with respect to the natural action of H_Z on $\mathcal{O}_{{}_dE_Z}$) is an *isomorphism.* Thus, by applying this isomorphism to the various morphisms obtained by taking $\mathcal{H}_Z \cong H_Z$-invariants of the various morphisms of Theorem 2.1, we obtain the following result:

Corollary 2.2. **(Lagrangian Version of the Main Result of [Mzk1])** *Assume that d is* **odd** *and that $n \stackrel{\text{def}}{=} 2m$ is* **invertible on** *S. Then by applying the isomorphism $\mathcal{O}_{{}_dE_Z}^{H_Z} \subseteq \mathcal{O}_{{}_dE_Z} \twoheadrightarrow \mathcal{O}_{G_Z^\mu}$ to the result of taking $\mathcal{H}_Z \cong H_Z$-invariants of the various morphisms of Theorem 2.1, we obtain a morphism*

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

whose restriction

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

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

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

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

Proof. This follows from Theorem 2.1, together with the elementary observation that taking the $\mathcal{H}_Z \cong H_Z$-invariants of an $\mathcal{H}_Z \cong H_Z$-equivariant isomorphism is again an isomorphism. ○

Before proceeding, we 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 $(E_{d,Z})_H$, $(E_{\infty,S})_H$, $(E^*_{[d],\mathrm{et},Z})_H$, $(\overline{\mathcal{L}})_H$ (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.

Definition 2.3. The V-, P-, and D-actions of Π_S on G_Z^μ, together with the isomorphism $\Xi_{\mathcal{H}}^{\mathrm{GP},H_Z}$ of Corollary 2.2, and the natural action of Π_S on $\overline{\mathcal{L}}|_{0_{E_Z}}$, define V-, P-, and D-actions of Π_S on $\mathcal{H}_{\mathrm{DR}}^{\mathrm{GP},H_Z}$, which we shall refer to as the *Lagrangian Galois actions on* $\mathcal{H}_{\mathrm{DR}}^{\mathrm{GP},H_Z}$.

Remark. Thus, unlike the "naive" Galois actions of §1, the Lagrangian Galois actions *depend on the choice of the additional data* M^μ, M^{H}.

Remark. Thus, *a priori*, the Lagrangian Galois actions appear to require the *Gaussian poles* (i.e., it appears that they are not necessarily *integrally* defined on $\mathcal{H}_{\mathrm{DR}}^{H_Z}$). In fact, however, we shall see in §2.2 below that (under certain assumptions) *the*

Lagrangian Galois D-action has the remarkable property that it is defined without introducing the Gaussian poles. This property is *not* possessed by the "naive" (non-Lagrangian) Galois actions of §1.

§2.2. Relation to the Crystalline Theta Object

In this §, we continue to use the notations of §2.1, except that we further *specialize* them as follows. Let A be a *complete discrete valuation ring of mixed characteristic* $(0,p)$*, with perfect residue field.* Write K (respectively, k) for the *quotient field* (respectively, *residue field*) of A. In this §, we suppose that S is of the form:

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

for some positive integer N *prime to* d, and that the *log structure* on S is that defined by the divisor $V(q^{\frac{1}{N}}) \subseteq S$. Also, we suppose that the given *log elliptic curve* $C^{\log} \to S^{\log}$ is the "Tate curve," i.e., that it has "q-parameter" equal to $q \in \mathcal{O}_S$.

Thus, if we take A sufficiently large, we may assume that Z is of the form:

$$Z = \mathrm{Spec}(A[[q^{\frac{1}{N \cdot d}}]])$$

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

Write $E_Z \stackrel{\mathrm{def}}{=} E \times_S Z$. Thus, $E_Z \to Z$ is a one-dimensional semi-abelian scheme over Z. Note that E_Z has a unique finite flat subgroup scheme annihilated by d. This subgroup scheme is naturally isomorphic to $\boldsymbol{\mu}_d$. We take this subgroup scheme for our

$$\boldsymbol{\mu}_d \cong G^{\mu}_Z \subseteq {}_dE_Z \subseteq E_Z$$

(and note that it is easy to see that this G^{μ}_Z *satisfies the condition* (cf. §2.1) that $\mathcal{O}_{G^{\mu}_Z} \subseteq \mathcal{F}^{\mu}$ be preserved by the V-, P-, and D-actions of Π_S on $\mathcal{F}^{\mu}$). Moreover, since $({}_dE_Z)/G^{\mu}_Z$ 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 $H_Z \subseteq {}_dE_Z$ such that the natural morphism

$$G^{\mu}_Z \times_Z H_Z \to {}_dE_Z$$

is an *isomorphism of group schemes.* Thus, if we write $E_{H_Z} \stackrel{\mathrm{def}}{=} (E_{d,Z})_H$, 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. Finally, we note that the q-parameter of E_{H_Z} is a d-th root of q. *This completes our description of the specializations of the objects of §2.1 that we will use in the present §.*

Next, we would like to *relate the present discussion to the theory of connections in [Mzk3].* To begin with, we recall that $\overline{\mathcal{L}}|_{0_{E_Z}}$ (where $0_{E_Z} \in E_Z(Z)$ is the zero section of $E_Z \to Z$) is a *line bundle on* Z *equipped with a natural* Π_S*-action*; moreover, this Π_S-action is derived from the fact that $\overline{\mathcal{L}}|_{0_{E_Z}}$ in fact arises from a "line bundle on S_∞." Thus, there exists a *trivialization*

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

(where a is a nonnegative integer $< Nd$) — i.e., in the terminology of the discussion of [Mzk3], §5, a *rigidification* of $\overline{\mathcal{L}}$ at 0_{E_Z} — which is Π_S*-equivariant.* In the following discussion, we *fix* such a "Π_S-equivariant rigidification" τ.

Observe that τ defines, in particular, a *logarithmic connection* on the line bundle $\overline{\mathcal{L}}|_{0_{E_Z}}$ which is *stable under the action of* Π_S. Thus, according to the theory of [Mzk3], §5, this rigidification gives rise to *(logarithmic) connections*

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

on $\mathcal{V}_{\overline{\mathcal{L}}}$, $\mathcal{V}_{\overline{\mathcal{L}}}^{H_Z}$, respectively (cf. [Mzk3], Theorems 5.2, 8.1), which are *stabilized by the action of* Π_S. 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 $\mathcal{O}_Z$.

Moreover, 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 $\mathcal{V}_{\overline{\mathcal{L}}}$, $\mathcal{V}_{\overline{\mathcal{L}}}^{H_Z}$ define *"crystals"* on the site

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

of *infinitesimal thickenings over* A *of open sub-log schemes of* $Z^{\log} \otimes k = Z^{\log} \otimes (A/\mathfrak{m}_A)$. That is to say, usually, "crystals" are defined on sites of *PD-thickenings* (cf., e.g., [BO], §6, for a discussion of this theory), but here, since *all of the higher* p*-curvatures vanish*, we obtain crystals on the site of thickenings which do not necessarily admit PD-structures. Since the definitions and proofs of basic properties of such "crystals on Inf" are entirely similar to the divided power case, we leave the unenlightening details to the reader. Thus, in summary, we may think of the pairs

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

as *crystals on Inf*($Z^{\log} \otimes k/A$).

In the following discussion, we will not use the entire group Π_S, but only its "$\mathfrak{m}$-*inertia subgroup*" $\Pi_S^{\mathfrak{m}} \subseteq \Pi_S$, defined as follows:

$$(\Pi_S \supseteq)\ \Pi_S^{\mathfrak{m}} \stackrel{\text{def}}{=} \{\sigma \in \Pi_S \mid \sigma(\phi) \equiv \phi \pmod{\mathfrak{m}_A \cdot \mathcal{O}_Z},\ \forall \phi \in \mathcal{O}_Z\}$$

Thus, in particular, one verifies easily that the image $\mathrm{Gal}^{\mathfrak{m}}(Z/S)$ of $\Pi_S^{\mathfrak{m}}$ in $\mathrm{Gal}(Z/S)$ is a *p-group*. More precisely, if we write

$$d = d_p \cdot d_{\neq p}$$

(where d_p, $d_{\neq p}$ are positive integers; d_p is a power of p; and $d_{\neq p}$ is prime to p), then one verifies immediately (using the simple explicit structures of S, Z) that the correspondence

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

defines isomorphisms:

$$\begin{array}{ccccc}
\Pi_S^{\mathfrak{m}} & \twoheadrightarrow & \mathrm{Gal}^{\mathfrak{m}}(Z/S) & \stackrel{\sim}{\to} & (\mathbb{Z}/d_p\mathbb{Z})(1) \\
\downarrow & & \downarrow & & \downarrow \\
\Pi_S & \twoheadrightarrow & \mathrm{Gal}(Z/S) & \stackrel{\sim}{\to} & (\mathbb{Z}/d\mathbb{Z})(1)
\end{array}$$

(where the vertical arrows are the natural inclusions, and the horizontal arrows are defined by the correspondence just mentioned).

Next, let us observe that it follows immediately from the definition of $\Pi_S^{\mathfrak{m}}$ that every $\sigma \in \Pi_S^{\mathfrak{m}}$ defines an *A-linear isomorphism*

$$\sigma : \quad Z^{\log} \stackrel{\sim}{\to} Z^{\log}$$

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

(iii) the fact that $(\mathcal{V}_{\underline{\mathcal{L}}}^{H_Z}, \nabla_{\mathcal{V}_{\underline{\mathcal{L}}}^{H_Z}})$ 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). Here, 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 $\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$ 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* $\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$. (In fact, the same holds for "$\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$" replaced by "$\widehat{\mathcal{V}}_{\overline{\mathcal{L}}}$," but since this action is more interesting for $\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$, we restrict ourselves to the case of $\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$ in the following discussion.)

Theorem 2.4. **(Crystalline Nature of the Lagrangian Galois Action)** *The action of* Π_S *on* $\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$ *is compatible with* $\Xi^{H_Z}_{\widehat{\mathcal{V}}}$ *(cf. Corollary 2.2; here the "hat" denotes* p*-adic completion) and the D-action on* G^μ_Z *in the following sense: For* $\sigma \in \Pi_S$*, the following diagram commutes:*

$$\begin{array}{ccc}
\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}} & \stackrel{\Xi^{H_Z}_{\widehat{\mathcal{V}}}}{\longrightarrow} & \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^\mu_Z} \\
\Big\downarrow \int_\sigma & & \Big\downarrow \sigma^D \\
\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}} & \stackrel{\Xi^{H_Z}_{\widehat{\mathcal{V}}}}{\longrightarrow} & \overline{\mathcal{L}}|_{0_{E_Z}} \otimes_{\mathcal{O}_Z} \mathcal{O}_{G^\mu_Z}
\end{array}$$

(where σ^D *denotes the result of applying* σ *to* $\mathcal{O}_{G^\mu_Z}$ *via the D-action of* Π_S *on* $\mathcal{O}_{G^\mu_Z}$*).*

Proof. This follows from the naturality of all the morphisms involved, together with the compatibility (cf. [Mzk3], Theorem 6.1) over G^μ_Z of the connection $\nabla_{\mathcal{V}^{H_Z}_{\overline{\mathcal{L}}}}$ with the "theta trivialization" reviewed in §2.1. ○

Corollary 2.5. **(Absence of Gaussian Poles in the Lagrangian Galois Action)** *Relative to the objects of the present discussion, the Lagrangian Galois D-action of* Π_S *on* $\mathcal{H}^{\mathrm{GP},H_Z}_{\mathrm{DR}}$ *(cf. Definition 2.3) is defined* **without Gaussian poles***, i.e., it arises from an action of* Π_S *on* $\mathcal{H}^{H_Z}_{\mathrm{DR}}$*.*

Proof. This follows immediately from the commutative diagram of Theorem 2.4, together with Lemma 2.6 below: Indeed, since the morphism "$\int_\sigma$" is *integral* (i.e., in particular, defined without Gaussian poles), restricting this commutative diagram to $\mathcal{H}^{H_Z}_{\mathrm{DR}} \subseteq \widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$ (i.e., where "$\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$" denotes the "$\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$" in the upper left-hand corner of the diagram) shows that by computing the Lagrangian D-action *inside* $\widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$ and then applying Lemma 2.6 to the lower horizontal arrow of the diagram, we obtain the asserted integrality. ○

Lemma 2.6. *The image of the morphism* $\Xi^{H_Z}_{\widehat{\mathcal{V}}}$ *(cf. Corollary 2.2) is the same as the image of its restriction* $\Xi^{H_Z}_{\mathcal{H}}$ *to* $\mathcal{H}^{H_Z}_{\mathrm{DR}} \subseteq \widehat{\mathcal{V}}^{H_Z}_{\overline{\mathcal{L}}}$*.*

Proof. In a word, these two images coincide because both images are equal to the image of the *theta convolution* (studied in detail in [Mzk2], cf. especially §10). Indeed, this is essentially the content of the proof of [Mzk2], Theorem 10.1. In this proof, only the image of $\Xi_{\mathcal{H}}^{H_Z}$ — i.e., more concretely, the span of the derivatives of the theta function "Θ" of order $< d$ — is discussed, and this image is shown to be the same as that of the theta convolution; but the argument never uses that the derivatives are of order $< d$ — i.e., the exact same argument shows that the image of $\Xi_{\widehat{\mathcal{V}}}^{H_Z}$ (= the span of the derivatives of the theta function "Θ" of arbitrary order) is equal to the image of the theta convolution.

For the convenience of the reader, however, we review the argument briefly as follows: If we write "U" for the standard coordinate on $\mathbb{G}_m$, then the image of $\Xi_{\mathcal{H}}^{H_Z}$ (respectively, $\Xi_{\widehat{\mathcal{V}}}^{H_Z}$) may be identified with the span of the restrictions to $\boldsymbol{\mu}_d \subseteq \mathbb{G}_m$ of the derivatives $(\frac{\partial}{\partial U})^j \Theta$ — where

$$\Theta \stackrel{\mathrm{def}}{=} \sum_{k \in \mathbb{Z}} q^{\frac{1}{d}(\frac{1}{2}\cdot k^2 + (i_\chi/n)\cdot k)} \cdot U^k \cdot \chi(k)$$

(and χ (a character $\mathbb{Z} \to \boldsymbol{\mu}_n$), i_χ (an integer) are invariants associated to the torsion point η) — of *order* $< d$ (respectively, *arbitrary order*). On the other hand, a basis of the functions on $\boldsymbol{\mu}_d$ is given by $U^0, \ldots, U^{d-1}$. If one computes the coordinates (relative to this basis) of $\Theta|_{\boldsymbol{\mu}_d}$, one sees that the coefficient of the smallest power of q appearing in each coordinate is *either* a root of unity *or* a root of unity times a nonzero sum of two n-th roots of unity (cf. [Mzk2], Theorem 4.4, where we take d_{ord} to be 1). Since we have assumed that n is *invertible on* S (cf. Theorem 2.1), we thus obtain that this coefficient is always a *unit*. On the other hand, to give an element in the span in question is to consider the restriction to $\boldsymbol{\mu}_d \subseteq \mathbb{G}_m$ of a series

$$\sum_{k \in \mathbb{Z}} q^{\frac{1}{d}(\frac{1}{2}\cdot k^2 + (i_\chi/n)\cdot k)} \cdot P(k) \cdot U^k \cdot \chi(k)$$

where $P(-)$ is a polynomial (with coefficients in $\mathcal{O}_Z \otimes \mathbb{Q}$, but which maps $\mathbb{Z}$ into $\mathcal{O}_Z$) of degree $< d$ (respectively, arbitrary degree) in the case of $\Xi_{\mathcal{H}}^{H_Z}$ (respectively, $\Xi_{\widehat{\mathcal{V}}}^{H_Z}$). Thus, in short, the assertion of Lemma 2.6 amounts to the claim that the span of

$$\{P(k) \cdot q^{\Phi(k)} \cdot U^k\}_{k=0,\ldots,d-1}$$

(for some function $\Phi : \{0, \ldots, d-1\} \to \frac{1}{N\cdot d} \cdot \mathbb{Z}$) is the same, regardless of whether one restricts the degree of $P((-)$ to be $< d$ or not. But this is easily verified. ○

Finally, we observe that:

> *Theorem 2.4 allows us to relate the "arithmetic Kodaira-Spencer morphism" arising from the Lagrangian Galois action to the classical geometric Kodaira-Spencer morphism.*

as follows: Let

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

be a *subgroup of order* > 2. Write $d_\Gamma \stackrel{\mathrm{def}}{=} |\Gamma|$ for the order of Γ. Thus, $d_\Gamma \neq 1$ divides d_p, and we have a *natural isomorphism* $\Gamma \cong (\mathbb{Z}/d_\Gamma\mathbb{Z})(1)$ (cf. the discussion above immediately following the definition of $\Pi_S^{\mathfrak{m}}$). 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* $Z \otimes (A/\mathfrak{m}_\Gamma)$ (mod $\mathfrak{m}_\Gamma$). 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, we would like to consider a *"certain portion" of the "arithmetic Kodaira-Spencer morphism" associated to the Lagrangian Galois action*, which will turn out to be related to the classical Kodaira-Spencer morphism. Let $\gamma \in \Gamma$. Then since γ acts on $\mathcal{H}_{\mathrm{DR}}^{H_Z}$ via the Lagrangian Galois D-action (Definition 2.3, Corollary 2.5), we see that γ defines a morphism $\gamma^D : \mathcal{H}_{\mathrm{DR}}^{H_Z} \to \mathcal{H}_{\mathrm{DR}}^{H_Z}$. 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 one verifies easily — by using the fact that γ is the identity on $\mathcal{H}_{\mathrm{DR}}^{H_Z} \otimes_A k$, $\mathcal{H}_{\mathrm{DR}}^{H_Z} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$) vanishes on $\mathfrak{m}_\Gamma \cdot F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z})$ and maps into $\{\mathcal{H}_{\mathrm{DR}}^{H_Z}/F^2(\mathcal{H}_{\mathrm{DR}}^{H_Z})\} \otimes_A \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$). Thus, we obtain a morphism

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

which we would like to analyze by applying Theorem 2.4. If one reduces the commutative diagram of Theorem 2.4 modulo $\mathfrak{m}_\Gamma^2$, it follows that κ_γ *may be computed by applying the (logarithmic) connection* $\nabla_{\mathcal{V}_{\mathcal{L}}^{H_Z}}$ *on* $\mathcal{V}_{\mathcal{L}}^{H_Z}$ *in the logarithmic tangent direction*

$$\frac{\partial}{\partial \log(q^{\frac{1}{N \cdot d}})} \cdot \delta_\Gamma(\gamma)$$

— where we observe that

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

(cf. the definition of δ_Γ, λ_Γ given above). That is to say, Applying $\nabla_{\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}}$ in this logarithmic tangent direction to $F^1(\mathcal{H}^{H_Z}_{\mathrm{DR}}) \otimes k = F^1(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}) \otimes k \subseteq \mathcal{V}_{\underline{\mathcal{L}}} \otimes k$ and then projecting via $\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}} \otimes k \twoheadrightarrow \mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}/F^2(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}) \otimes k$ defines a morphism:

$$F^1(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}) \otimes k \to \mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}/F^2(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}) \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

On the other hand, by [Mzk3], Theorem 8.1 (i.e., the property which was called *"Griffiths semi-transversality"* in *loc. cit.*), this morphism in fact maps into the submodule $F^3(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}})/F^2(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}) \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$. Moreover, $(F^3/F^2)(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}})$ is naturally isomorphic to $\frac{1}{2} \cdot F^1(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}) \otimes \tau^{\otimes 2}_{E_{H_Z}}$ (where we write $\tau_{E_{H_Z}}$ for the tangent bundle to E_{H_Z} at the origin $0_{E_{H_Z}}$). In particular, we obtain that κ_γ *also maps into* $F^3(-)$. (Note that here we use that $d \geq d_p \geq d_\Gamma \geq 3$.) Thus, by letting γ *vary*, we obtain a homomorphism:

$$\kappa_\Gamma : \Gamma \to \mathrm{Hom}_{\mathcal{O}_Z}(F^1(\mathcal{H}^{H_Z}_{\mathrm{DR}}) \otimes k, (F^3/F^2)(\mathcal{H}^{H_Z}_{\mathrm{DR}}) \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) = \frac{1}{2} \cdot \tau^{\otimes 2}_{E_{H_Z}} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

arising from the *Lagrangian Galois action, taken modulo* $\mathfrak{m}_\Gamma^2$, which, when regarded as an element

$$\kappa_\Gamma \in \mathrm{Hom}(\Gamma, \frac{1}{2} \cdot \tau^{\otimes 2}_{E_{H_Z}} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) = \mathrm{Hom}(\Gamma, \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) \otimes \frac{1}{2} \cdot \tau^{\otimes 2}_{E_{H_Z}}$$

is equal to the result of evaluating the *geometric Kodaira-Spencer morphism of the "crystalline theta object"* $(\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}, \nabla_{\mathcal{V}^{H_Z}_{\underline{\mathcal{L}}}})$ (cf. [Mzk3], Theorem 8.1)

$$\kappa_\nabla : (\Omega_{Z^{\log}/A})^\vee \to \frac{1}{2} \cdot \tau^{\otimes 2}_{E_{H_Z}}$$

on $\frac{\partial}{\partial \log(q^{\frac{1}{N\cdot d}})} \in (\Omega_{Z^{\log}/A})^\vee$ and multiplying the result by δ_Γ. We summarize this discussion as follows:

Corollary 2.7. (Relation to the Classical Geometric Kodaira-Spencer Morphism) *Let*

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

be a **subgroup of order** > 2. *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* $q^{\frac{1}{N\cdot d}}$ *modulo* $\mathfrak{m}_\Gamma^2$*). Then the morphism*

$$\kappa_\Gamma : \Gamma \to \mathrm{Hom}_{\mathcal{O}_Z}(F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes k, (F^3/F^2)(\mathcal{H}_{\mathrm{DR}}^{H_Z}) \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2) = \frac{1}{2} \cdot \tau_{E_{H_Z}}^{\otimes 2} \otimes \mathfrak{m}_\Gamma/\mathfrak{m}_\Gamma^2$$

obtained purely from the **Lagrangian Galois D-action** *of* Γ *on* $\mathcal{H}_{\mathrm{DR}}^{H_Z}$ *(cf. Definition 2.3, Corollary 2.5) by restricting this action to* $F^1(\mathcal{H}_{\mathrm{DR}}^{H_Z})$ *and then reducing modulo* $\mathfrak{m}_\Gamma^2$ **coincides** *with the morphism obtained by evaluating the* **"geometric Kodaira-Spencer morphism of the crystalline theta object"** $(\mathcal{V}_{\underline{\mathcal{L}}}^{H_Z}, \nabla_{\mathcal{V}_{\underline{\mathcal{L}}}^{H_Z}})$ *(cf. [Mzk3], Theorem 8.1)*

$$\kappa_\nabla : (\Omega_{Z^{\log}/A})^\vee \to \frac{1}{2} \cdot \tau_{E_{H_Z}}^{\otimes 2}$$

in the logarithmic tangent direction $\frac{\partial}{\partial \log(q^{\frac{1}{N\cdot d}})} \in (\Omega_{Z^{\log}/A})^\vee$ *and multiplying the result by* δ_Γ. *Moreover, by [Mzk3], Theorem 8.1, this Kodaira-Spencer morphism associated to the crystalline theta object coincides (up to a factor of* $\frac{1}{2}$*) with the usual Kodaira-Spencer morphism associated to the Gauss-Manin connection on the first de Rham cohomology group. Thus, in summary, the* **arithmetic Kodaira-Spencer morphism** *associated to the Lagrangian Galois D-action coincides modulo* $\mathfrak{m}_\Gamma^2$ *(and up to a factor of* $\frac{1}{2}$*) with the* **usual Kodaira-Spencer morphism**.

Remark. Note, moreover, that the correspondence between the logarithmic tangent direction $\frac{\partial}{\partial \log(q^{\frac{1}{N\cdot d}})} \in (\Omega_{Z^{\log}/A})^\vee$ 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). In particular:

> *Corollary 2.7 shows that the analogy discussed in [Mzk1], Chapter IX, between the (usual)* **geometric Kodaira-Spencer morphism** *(cf. especially, [Mzk1], Chapter IX, Theorem 2.6) and the* **arithmetic Kodaira-Spencer morphism** *is more than just philosophy — it is rigorous mathematics!*

(cf. also the discussion of [Mzk3], Theorem 6.2, in [Mzk3], §0).

Section 3: Global Multiplicative Subspaces

In this §, we show how to construct a sort of *global analogue* of the crucial subgroup scheme "$G_Z^\mu \subseteq {}_dE_Z$" of §2.2. The author believes that this construction indicates the proper approach to *globalizing the local theory of §2* — cf. §4, "Conclusion."

In this §, let us write $\overline{\mathcal{M}}_{\mathbb{Z}}$ for the *moduli stack* $(\overline{\mathcal{M}}_{1,0})_{\mathbb{Z}}$ (cf. §0, Notations and Conventions); $\mathcal{M}_{\mathbb{Z}} \subseteq \overline{\mathcal{M}}_{\mathbb{Z}}$ for the open substack parametrizing *smooth elliptic curves*. We denote base change to $\mathbb{Q}$ by a subscript $\mathbb{Q}$. Also, let us write

$$\Pi_{\mathcal{M}_{\mathbb{Q}}} \stackrel{\text{def}}{=} \pi_1(\mathcal{M}_{\mathbb{Q}})$$

(for some choice of base-point).

Next, let us fix a *prime number* p. Thus, the p-power torsion points of the tautological elliptic curve over $\mathcal{M}_{\mathbb{Q}}$ define a *p-adic Tate module*

$$\mathcal{F}$$

— i.e., $\mathcal{F}$ is a free $\mathbb{Z}_p$-module of rank two equipped with a continuous $\Pi_{\mathcal{M}_{\mathbb{Q}}}$-action $\rho_{\mathcal{F}} : \Pi_{\mathcal{M}_{\mathbb{Q}}} \to GL(\mathcal{F})$. Write

$$\mathcal{T}_{\mathbb{Q}} \to \mathcal{M}_{\mathbb{Q}}$$

for the *profinite étale covering* defined by the subgroup $\mathrm{Ker}(\rho_{\mathcal{F}}) \subseteq \Pi_{\mathcal{M}_{\mathbb{Q}}}$. Since $\rho_{\mathcal{F}}$ is *surjective* (cf., e.g., [Shi], Theorem 6.23, together with the fact that the cyclotomic character $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^{\times}$ is *surjective*), it follows that $\mathcal{T}_{\mathbb{Q}} \to \mathcal{M}_{\mathbb{Q}}$ is *Galois*, with Galois group

$$\mathrm{Gal}(\mathcal{T}_{\mathbb{Q}}/\mathcal{M}_{\mathbb{Q}}) \cong GL_2(\mathbb{Z}_p)$$

(where the isomorphism is determined by a choice of $\mathbb{Z}_p$-basis for $\mathcal{F}$). Write

$$\overline{\mathcal{T}}_{\mathbb{Z}} \to \overline{\mathcal{M}}_{\mathbb{Z}}$$

for the *normalization* of $\overline{\mathcal{M}}_{\mathbb{Z}}$ in $\mathcal{T}_{\mathbb{Q}}$; $\mathcal{T}_{\mathbb{Z}} \stackrel{\text{def}}{=} \overline{\mathcal{T}}_{\mathbb{Z}} \times_{\overline{\mathcal{M}}_{\mathbb{Z}}} \mathcal{M}_{\mathbb{Z}}$. Also, in the following discussion, we will denote the *p-adic formal schemes* (or stacks) defined by p-adically completing various schemes (or stacks) by means of a superscript "$\wedge$."

Now note that the natural $\Pi_{\mathcal{M}_{\mathbb{Q}}}$-actions on $\widehat{\overline{\mathcal{T}}}_{\mathbb{Z}}$ and $\mathcal{F}$ define a *natural* $\Pi_{\mathcal{M}_{\mathbb{Q}}}$-*action* on

$$\mathcal{O}_{\widehat{\overline{\mathcal{T}}}_{\mathbb{Z}}} \otimes_{\mathbb{Z}_p} \mathcal{F}$$

(which we regard as a coherent sheaf on $\widehat{\overline{\mathcal{T}}}_{\mathbb{Z}}$). Let us write ω_E for the line bundle on $\overline{\mathcal{M}}_{\mathbb{Z}}$ defined by the cotangent bundle at the origin of the tautological log elliptic curve over $\overline{\mathcal{M}}_{\mathbb{Z}}$. Then we recall the following result, which is essentially an immediate corollary of the *p-adic Hodge theory of elliptic curves*:

Theorem 3.1. **(Global Multiplicative Subspace)** *There is a natural* $\Pi_{\mathcal{M}_{\mathbb{Q}}}$*-equivariant morphism*

$$\psi_\omega : \mathcal{O}_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}} \otimes_{\mathbb{Z}_p} \mathcal{F} \to \omega_E|_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}}$$

whose image contains $(1-\zeta_p)\cdot \omega_E|_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}}$*, where* ζ_p *is a primitive* p*-th root of unity. Moreover, away from the supersingular points of* $\overline{\mathcal{T}}_{\mathbb{Z}} \otimes \mathbb{F}_p$*, this morphism is a surjection, and (in a formal neighborhood of infinity) its kernel is the subspace defined by the multiplicative subgroup schemes "*$G^\mu_Z \subseteq {}_dE_Z$*" (cf. §2.2) where we take* $d \stackrel{\mathrm{def}}{=} p^n$*,* $n \to \infty$*.*

Proof. The morphism ψ_ω is what is usually referred to in p-adic Hodge theory as the *p-adic period map.* There are many ways to construct the p-adic period map. Over the *smooth locus* $\mathcal{M}_{\mathbb{Z}}$, one way to construct the period map (cf. [Mzk3], §2, the Remark following the proof of Theorem 2.2) is to use the *canonical section* (defined modulo p^n — cf. [Mzk3], §1, the discussion following Lemma 1.1 for more details on this canonical section)

$$\kappa_H : H \otimes (\mathbb{Z}/p^n\mathbb{Z}) \to E^\dagger \otimes (\mathbb{Z}/p^n\mathbb{Z})$$

of the *universal extension* $E^\dagger \to E$ (where $E \to \mathcal{M}_{\mathbb{Z}}$ is the tautological elliptic curve) over the covering H ($\stackrel{\mathrm{def}}{=} E$) $\to E$ of E given by multiplication by p^n (where we let $n \to \infty$). By looking at "fibers (of H, $E^\dagger$) over the origin of E," we thus see that κ_H determines a *homomorphism* from the p^n-torsion points of $E|_{\widehat{\mathcal{T}}_{\mathbb{Z}}}$, i.e., in particular, from $\mathcal{F} \otimes (\mathbb{Z}/p^n\mathbb{Z}) \hookrightarrow E(\widehat{\mathcal{T}}_{\mathbb{Z}})$, to $\omega_E \otimes (\mathbb{Z}/p^n\mathbb{Z})|_{\widehat{\mathcal{T}}_{\mathbb{Z}}}$, as desired. Note that although only the smooth case is discussed in *loc. cit.*, one verifies immediately that this approach may be extended over $\overline{\mathcal{M}}_{\mathbb{Z}}$ (by using the canonical section of the universal extension near infinity). Letting $n \to \infty$ and tensoring over $\mathbb{Z}_p$ with $\mathcal{O}_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}}$ thus *completes the construction of* ψ_ω.

The remaining statements concerning the various properties of ψ_ω may be verified by using another approach to constructing the p-adic period map, which is discussed in [Mzk1], Chapter IX, §2. This approach has the slight disadvantage that it is not immediately clear that the resulting period map is *defined over* $\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}$ (i.e., *a priori*, it is only defined over locally constructed "$\widehat{\widehat{R}}$'s"). Nevertheless, one may check easily (by working over the ordinary locus) that these two approaches yield the same period map (cf. [Mzk3], §2, the Remark following the proof of Theorem 2.2). On the other hand, the approach of [Mzk1], Chapter IX, §2, has the advantage that it makes it clear that the morphism $\psi_\omega : \mathcal{O}_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}} \otimes_{\mathbb{Z}_p} \mathcal{F} \to \omega_E|_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}}$ in question is the *composite* (at least *locally* on $\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}$, but this is sufficient for our purposes) of a morphism — which we shall denote ψ_1 — from $\mathcal{O}_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}} \otimes_{\mathbb{Z}_p} \mathcal{F}$ to a certain *rank two vector bundle* on $\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}$, followed by a *surjection* — which we shall denote ψ_2 — from this vector bundle onto the line bundle $\omega_E|_{\widehat{\widehat{\mathcal{T}}}_{\mathbb{Z}}}$ (cf. the morphism "$\Psi_{\mathbb{Z}_p}$" — or, more precisely, its *dual* — of [Mzk1], Chapter IX, Theorem 2.5). Moreover, the determinant of ψ_1 is equal to $1-\zeta_p$ times a unit (cf. [Mzk1], Chapter IX, Theorem

2.5, as well as the proof of this theorem). On the other hand, since the range of the morphism ψ_ω is a *line bundle*, it follows that the image of ψ_ω determines an *ideal* $\mathcal{J} \subseteq \mathcal{O}_{\hat{\overline{\mathcal{T}}}_{\mathbb{Z}}}$ with the property that $\det(\psi_1)$ *vanishes modulo* $\mathcal{J}$. Thus, we conclude that $1 - \zeta_p \in \mathcal{J}$, as desired. Finally, the assertions of Theorem 3.1 over the ordinary locus and near infinity follow from the theory of either [Mzk3], §2, or [Mzk1], Chapter IX, §2. This completes the proof ◯

Remark. Usually, in the context of p-adic Hodge theory, one constructs the p-adic period map not over *global bases* such as $\overline{\mathcal{M}}_{\mathbb{Z}}$, but over *$p$-adic bases*, such as $\overline{\mathcal{M}}_{\mathbb{Z}_p}$. It is immediate, however, from the first approach discussed in the proof of Theorem 3.1 to constructing the p-adic period map that *exactly the same construction works over* $\overline{\mathcal{M}}_{\mathbb{Z}}$ and gives rise to a morphism that is *equivariant with respect to* $\Pi_{\mathcal{M}_{\mathbb{Q}}} = \pi_1(\mathcal{M}_{\mathbb{Q}})$ (i.e., not just $\pi_1(\mathcal{M}_{\mathbb{Q}_p})$). (The author wishes to thank A. Tamagawa for remarks that led to a simplification of the proof of Theorem 3.1.)

Remark. Thus, in particular, we obtain that *if E is a log elliptic curve over $\mathbb{Z}$, then (by pull-back via the classifying morphism to $\overline{\mathcal{M}}_{1,0}$ defined by E) the morphism ψ_ω defines a* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-*equivariant morphism*:

$$\psi_\omega(E) : T_p(E) \otimes_{\mathbb{Z}_p} \mathcal{O}_{\hat{\overline{\mathbb{Q}}}} \to \omega_E \otimes_{\mathcal{O}_F} \mathcal{O}_{\hat{\overline{\mathbb{Q}}}}$$

(where $T_p(E)$ is the p-adic Tate module of E; $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$; and the "hat" denotes p-adic completion) whose *image contains* $p \cdot \omega_E$ (cf. Theorems 3.1, 3.2). In particular, since the completions of $\overline{\mathbb{Q}}$ at each of its primes over p are all *valuation rings*, we thus conclude that $\psi_\omega(E)$ defines a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-*equivariant surjection*

$$\psi'_\omega(E) : T_p(E) \otimes_{\mathbb{Z}_p} \mathcal{O}_{\hat{\overline{\mathbb{Q}}}} \to \omega'_E$$

(where $\omega'_E \subseteq \omega_E \otimes_{\mathbb{Z}} \mathcal{O}_{\hat{\overline{\mathbb{Q}}}}$ is a free $\mathcal{O}_{\hat{\overline{\mathbb{Q}}}}$-submodule of rank one) which coincides with $\psi_\omega(E)$ over $\mathbb{Q}_p$. *Thus, the kernel of $\psi'_\omega(E)$ may be regarded as a global generalization of the multiplicative subspace "$\mathbb{Z}_p(1) \subseteq T_p(E)$" of the Tate curve E over* $\mathbb{Z}[[q]]$.

Section 4: The Group Tensor Product

In this §, we present a *very general construction that applies to arbitrary commutative group schemes*, but which will be of fundamental importance for motivating the theory that we wish to pursue in subsequent papers.

We begin with the following definition, which is motivated by *infinite abelian group theory* (cf. [Fchs], p. 94):

Definition 4.1. We shall call a torsion-free abelian group R *ind-free* if every finite subset of R is contained in a finitely generated direct summand of R.

Remark. It is known that *every countable subgroup of an ind-free group is free* (cf. [Fchs], pp. 93-94). Thus, in particular, *every countable ind-free group is free.* On the other hand, groups such as an infinite direct product of infinite cyclic groups are *ind-free, but not free* (cf. [Fchs], p. 94). The reason that we wish to consider ind-free groups is because we wish to allow just such groups — i.e., such as the additive group of power series $\mathbb{Z}[[q]]$ — in the theory to be developed in the present and subsequent papers.

Now let S be a *noetherian scheme*, and G a *commutative group scheme* over S. (Note: we do not necessarily assume that G is smooth or of locally of finite type over S.) Thus, G defines a *functor*

$$T \mapsto G(T)$$

from the category of S-schemes (such as $T \to S$) to the category of *abelian groups.*

Next, let us assume that we are given an *ind-free $\mathbb{Z}$-module R* (cf. Definition 4.1). Then let us consider the functor

$$T \mapsto G(T) \otimes_{\mathbb{Z}} R$$

— which we denote by $G \overset{\mathrm{gp}}{\otimes} R$ — from the category of S-schemes (such as $T \to S$) to the category of *abelian groups.*

Definition 4.2. We shall refer to as an *ind-group scheme* an inductive system (indexed by a filtered set) of group schemes in which the transition morphisms are all closed immersions.

Remark. Thus, a *Barsotti-Tate group* (e.g., the p-divisible group defined by an abelian variety) is a typical example of an ind-group scheme. Note that it is important to assume that the transition morphisms are *closed immersions.* Indeed, so long as one assumes this, taking the inverse limit of sheaves of functions on the group schemes in the system gives rise to a sheaf of *"functions on the ind-group scheme"* which surjects onto the sheaves of functions on each of the group schemes in the system. If, on the other hand, one considers an inductive system such as

$$E \to E \to E \to E \to E \to \dots$$

(where E is an elliptic curve, and all of the arrows are multiplication by some positive integer d), then the inverse limit of the functions on the group schemes in the system contains only the *constant functions*. Thus, *it is difficult to treat this sort of inductive system as a single geometric object.*

Proposition 4.3. *This functor* $G \overset{\mathrm{gp}}{\otimes} R$ *is* **representable** *by an ind-group scheme over* S*, which, by abuse of notation, we also denote by* $G \overset{\mathrm{gp}}{\otimes} R$*. Moreover:*

(1) $G \overset{\mathrm{gp}}{\otimes} R$ *is* **functorial** *with respect to* G *and* R*.*

(2) *If* R *is finitely generated, then* $G \overset{\mathrm{gp}}{\otimes} R$ *is representable by a (single) group scheme.*

(3) *If* R *and* R' *are finitely generated free* $\mathbb{Z}$*-modules, and* $R \hookrightarrow R'$ *is a* **split** *injection, then the resulting arrow* $G \overset{\mathrm{gp}}{\otimes} R \to G \overset{\mathrm{gp}}{\otimes} R'$ *is a closed immersion.*

Proof. First, note that any ind-free R can be written as an inductive limit $\varinjlim_{J} R_j$ of *finitely generated free* $\mathbb{Z}$*-submodules* R_j (for j in some filtered index set J) such that the injections $R_j \hookrightarrow R$ are *split*. Moreover, when $j < j'$ (so $R_j \subseteq R_{j'}$), the fact that $R_j \hookrightarrow R$ is split implies that $R_j \subseteq R_{j'}$ is split. Thus, the representability of $G \overset{\mathrm{gp}}{\otimes} R$ (for a general ind-free R) by an ind-group scheme over S follows formally from assertions (1), (2), (3).

Let us prove (2), (3). Thus, for the remainder of this paragraph, let us assume that R is *finitely generated* (and free). But then R is (noncanonically) isomorphic to $\mathbb{Z}^r$ (for some positive integer r), so $G \overset{\mathrm{gp}}{\otimes} R$ can be represented by the group scheme $G \times_S G \times_S \ldots \times_S G$ (the fibered product over S of r copies of G). This proves (2). Since any split injection $\mathbb{Z}^r \hookrightarrow \mathbb{Z}^{r'}$ is isomorphic to the injection $\mathbb{Z}^r = \mathbb{Z}^r \times \{0\} \hookrightarrow \mathbb{Z}^r \times \mathbb{Z}^{r'-r} = \mathbb{Z}^{r'}$, assertion (3) follows immediately.

Finally, assertion (1) follows immediately from the functorial definition of $G \overset{\mathrm{gp}}{\otimes} R$. $\bigcirc$

Definition 4.4. By abuse of notation, we denote the ind-group scheme of Proposition 4.3 by $G \overset{\mathrm{gp}}{\otimes} R$, and refer to this ind-group scheme as the *group tensor product of* G *with* R.

Remark. We shall principally be interested in the case where G is an elliptic curve E, or its universal extension equipped with some integral structure — e.g., $E^*_{[d],\mathrm{et}}$ — and R is a ring closely related to the base scheme over which E is defined — e.g., $R = \mathcal{O}_F$ *(the ring of integers) for some number field* F.

Remark. Note that *automorphisms of the module R induce automomorphisms of $G \overset{\mathrm{gp}}{\otimes} R$*. Moreover, if, for instance, R is *finitely generated*, and G is equipped with an *ample line bundle $\mathcal{L}$*, then *any choice of basis $e_1, \ldots, e_r$ of R* determines an isomorphism $G \overset{\mathrm{gp}}{\otimes} R \cong \prod_{j=1}^{r} G$, hence (by taking the tensor product of the pull-backs of $\mathcal{L}$ relative to each of the factors in the product), *a natural choice of ample line bundle on $G \overset{\mathrm{gp}}{\otimes} R$*. This ample line bundle, however, *depends on the choice of basis*, i.e., it will not be preserved in general by automorphisms of R. Thus, in summary:

> Although (for, say, finitely generated R) the correspondence $G \mapsto G \overset{\mathrm{gp}}{\otimes} R$ defines a natural functor from group schemes to group schemes, it does *not* define a natural functor from *polarized* group schemes to polarized group schemes.

Since, in Hodge-Arakelov theory, it is of fundamental importance to work with *polarized group schemes*, the rather superficial general nonsense of the present § will not be sufficient for working with group tensored elliptic curves in Hodge-Arakelov theory. *The resolution of this technical issue forms one of the main obstacles relative to developing a theory of the sort that the author envisions for globalizing the theory of §2.*

One important property of the group tensor product is the following:

Proposition 4.5. *Let $d \geq 1$ be an integer, and write ${}_dG \subseteq G$ (respectively, ${}_d(G \overset{\mathrm{gp}}{\otimes} R) \subseteq G \overset{\mathrm{gp}}{\otimes} R$) for the kernel of the morphism $[d] : G \to G$ (respectively, $[d] : G \overset{\mathrm{gp}}{\otimes} R \to G \overset{\mathrm{gp}}{\otimes} R$), i.e., multiplication by d. Then we have a natural isomorphism:*

$${}_d(G \overset{\mathrm{gp}}{\otimes} R) \cong ({}_dG) \otimes_{\mathbb{Z}/d\mathbb{Z}} (R/d \cdot R)$$

Proof. This follows immediately from the functorial definition of $G \overset{\mathrm{gp}}{\otimes} R$. ◯

Conclusion:

If we formally combine Proposition 4.5 with the content of the second Remark following Theorem 3.1, we thus obtain the following:

> *If E is a log elliptic curve over $\mathbb{Z}$; $d = p^r$ (where p is a prime number, and $r \geq 1$ is an integer); and $R \overset{\mathrm{def}}{=} \mathcal{O}_K$ is the ring of integers of some finite Galois extension K of $\mathbb{Q}$ (which may*

> *depend on the choice of d), then the rank* 2 (R/dR)*-module of d-torsion points of* $E \overset{\text{gp}}{\otimes} R$ *contains a rank* 1 *submodule stabilized by* $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *and which coincides with the usual "multiplicative subspace" at primes of bad (multiplicative) reduction.*

In particular, this conclusion suggests that *if we could somehow develop a "Hodge-Arakelov theory for objects such as* $E \overset{\text{gp}}{\otimes} R$*," then we should be able to define for such objects a Lagrangian Galois-theoretic Kodaira-Spencer morphism which is free of Gaussian poles* (cf. Corollary 2.5). In subsequent papers, it is the hope of the author to develop just such a theory.

Bibliography

[BO] P. Berthelot and A. Ogus, *Notes on Crystalline Cohomology*, Princeton Univ. Press (1978).

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

[Fchs] L. Fuchs, *Infinite Abelian Groups*, Volume I, Pure and Applied Mathematics **36**, Academic Press (1970).

[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).

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