The Absolute Anabelian Geometry of Canonical Curves

Shinichi Mochizuki

Received: September 27, 2002
Revised: January 13, 2003

Abstract. In this paper, we continue our study of the issue of the extent to which a *hyperbolic curve over a finite extension of the field of p-adic numbers* is determined by the profinite group structure of its *étale fundamental group*. Our main results are that: (i) the theory of *correspondences* of the curve — in particular, its *arithmeticity* — is completely determined by its fundamental group; (ii) when the curve is a *canonical lifting* in the sense of *"p-adic Teichmüller theory"*, its *isomorphism class* is functorially determined by its fundamental group. Here, (i) is a consequence of a *"p-adic version of the Grothendieck Conjecture for algebraic curves"* proven by the author, while (ii) builds on a previous result to the effect that the *logarithmic special fiber* of the curve is functorially determined by its fundamental group.

2000 Mathematics Subject Classification: 14H25, 14H30
Keywords and Phrases: *hyperbolic curve, étale fundamental group, anabelian, correspondences, Grothendieck Conjecture, canonical lifting, p-adic Teichmüller theory*

Contents:

Introduction

Let X_K be a *hyperbolic curve* (cf. §0 below) over a *field* K *of characteristic* 0. Denote its *algebraic fundamental group* by Π_{X_K}. Thus, we have a *natural surjection*

$$\Pi_{X_K} \twoheadrightarrow G_K$$

of Π_{X_K} onto the *absolute Galois group* G_K of K. When K is a *finite extension of* $\mathbb{Q}$ *or* $\mathbb{Q}_p$, and one *holds* G_K *fixed*, then it is known (cf. [Tama], [Mzk6]) that one may *recover the curve* X_K *in a functorial fashion* from Π_{X_K}. This sort of result may be thought of as a *"relative result"* (i.e., over G_K).

In the present paper, we continue our study — begun in [Mzk7] — of "ABSOLUTE ANALOGUES" of such relative results. Since such absolute analogues are well understood in the case where K is a finite extension of $\mathbb{Q}$ (cf. the Introduction to [Mzk7]), we concentrate on the *p-adic case*. In the p-adic case, it is proven in [Mzk7] (cf. [Mzk7], Theorem 2.7) — by applying the work of [Tama] and the techniques of [Mzk5]— that (if X_K has *stable reduction*, then) the "LOGARITHMIC SPECIAL FIBER" OF X_K — i.e., the special fiber, equipped with its natural "log structure" (cf. [Kato]), of the "stable model" of X_K over the ring of integers $\mathcal{O}_K$ — *may be recovered solely from the abstract profinite group* Π_{X_K}. This result prompts the question (cf. [Mzk7], Remark 2.7.3):

What other information — e.g., the ISOMORPHISM CLASS OF X_K ITSELF — *can be recovered from the profinite group* Π_{X_K}*?*

In this present paper, we give *three partial answers* to this question (cf. [Mzk7], Remark 2.7.3), all of which revolve around the *central theme* that:

When X_K *is, in some sense,* "CANONICAL", *there is a tendency for substantial information concerning* X_K *— e.g., its isomorphism class — to be recoverable from* Π_{X_K}.

Perhaps this "tendency" should not be surprising, in light of the fact that in some sense, a *"canonical"* curve is a curve which is *"rigid"*, i.e., has no moduli, hence should be "determined" by its special fiber (cf. Remark 3.6.3).

Our three partial answers are the following:

(a) The property that the *Jacobian* of the X_K be a *Serre-Tate canonical lifting* is determined by Π_{X_K} (Proposition 1.1).

(b) The theory of *correspondences* of X_K — in particular, whether or not X_K is *"arithmetic"* (cf. [Mzk3]) — is determined by Π_{X_K} (cf. Theorem 2.4, Corollary 2.5).

(c) The property that X_K be a *canonical lifting in the sense of the theory of [Mzk1] (cf. also [Mzk2])* is determined by Π_{X_K}; moreover, in this case, the *isomorphism class* of X_K is also determined by Π_{X_K} (cf. Theorem 3.6).

At a technical level, (a) is entirely elementary; (b) is a formal consequence of the *"p-adic version of the Grothendieck Conjecture" proven in [Mzk6], Theorem A*; and (c) is derived as a consequence of the theory of [Mzk1], together with [Mzk7], Theorem 2.7.

Finally, as a consequence of (c), we conclude (cf. Corollary 3.8) that the *set of points arising from curves over finite extensions of $\mathbb{Q}_p$ whose isomorphism classes are completely determined by Π_{X_K} forms a* ZARISKI DENSE *subset of the moduli stack over $\mathbb{Q}_p$*. This result (cf. Remark 3.6.2) constitutes the first *application* of the "p-adic Teichmüller theory" of [Mzk1], [Mzk2], to prove a *hitherto unknown result* that can be *stated* without using the terminology, concepts, or results of the theory of [Mzk1], [Mzk2]. Also, it shows that — unlike (a), (b) which only yield "useful information" concerning X_K in *"very rare cases"* — (c) may be applied to a *"much larger class of X_K"* (cf. Remarks 1.1.1, 2.5.1, 3.6.1).

Acknowledgements: I would like to thank *A. Tamagawa* for useful comments concerning earlier versions of this manuscript.

Section 0: Notations and Conventions

We will denote by $\mathbb{N}$ the set of *natural numbers*, by which we mean the set of integers $n \geq 0$. A *number field* is defined to be a finite extension of the field of rational numbers $\mathbb{Q}$.

Suppose that $g \geq 0$ is an *integer*. Then a *family of curves of genus g*

$$X \to S$$

is defined to be a smooth, proper, geometrically connected morphism $X \to S$ whose geometric fibers are curves of genus g.

Suppose that $g, r \geq 0$ are *integers* such that $2g-2+r > 0$. We shall denote the *moduli stack of r-pointed stable curves of genus g* (where we assume the points to be *unordered*) by $\overline{\mathcal{M}}_{g,r}$ (cf. [DM], [Knud] for an exposition of the theory of such curves; strictly speaking, [Knud] treats the finite étale covering of $\overline{\mathcal{M}}_{g,r}$ determined by *ordering* the marked points). The open substack $\mathcal{M}_{g,r} \subseteq \overline{\mathcal{M}}_{g,r}$ of smooth curves will be referred to as the *moduli stack of smooth r-pointed* *stable curves of genus* g or, alternatively, as the *moduli stack of hyperbolic curves of type* (g, r).

A *family of hyperbolic curves of type* (g, r)

$$X \to S$$

is defined to be a morphism which factors $X \hookrightarrow Y \to S$ as the composite of an open immersion $X \hookrightarrow Y$ onto the complement $Y \backslash D$ of a relative divisor $D \subseteq Y$ which is finite étale over S of relative degree r, and a family $Y \to S$ of curves of genus g. One checks easily that, if S is *normal*, then the pair (Y, D) is *unique up to canonical isomorphism*. (Indeed, when S is the spectrum of a field, this fact is well-known from the elementary theory of algebraic curves. Next, we consider an arbitrary *connected normal* S on which a prime l is *invertible* (which, by Zariski localization, we may assume without loss of generality). Denote by $S' \to S$ the finite étale covering parametrizing *orderings of the marked points* and *trivializations of the* l*-torsion points of the Jacobian of* Y. Note that $S' \to S$ is *independent* of the choice of (Y, D), since (by the normality of S) S' may be constructed as the *normalization* of S in the function field of S' (which is independent of the choice of (Y, D) since the restriction of (Y, D) to the generic point of S has already been shown to be unique). Thus, the uniqueness of (Y, D) follows by considering the classifying morphism (associated to (Y, D)) from S' to the finite étale covering of $(\mathcal{M}_{g,r})_{\mathbb{Z}[\frac{1}{l}]}$ parametrizing orderings of the marked points and trivializations of the l-torsion points of the Jacobian [since this covering is well-known to be a scheme, for l sufficiently large].)

We shall refer to Y (respectively, D; D; D) as the *compactification* (respectively, *divisor at infinity*; *divisor of cusps*; *divisor of marked points*) of X. A *family of hyperbolic curves* $X \to S$ is defined to be a morphism $X \to S$ such that the restriction of this morphism to each connected component of S is a *family of hyperbolic curves of type* (g, r) for some integers (g, r) as above.

Section 1: Serre-Tate Canonical Liftings

In this §, we observe (cf. Proposition 1.1 below) that the issue of whether or not the Jacobian of a p-adic hyperbolic curve is a *Serre-Tate canonical lifting* is completely determined by the abstract profinite group structure of its *arithmetic profinite group*.

Let p be a prime number. For $i = 1, 2$, let K_i be a finite extension of $\mathbb{Q}_p$, and $(X_i)_{K_i}$ a *proper hyperbolic curve* over K_i whose associated stable curve has stable reduction over $\mathcal{O}_{K_i}$. Denote the resulting *"stable model"* of $(X_i)_{K_i}$ over $\mathcal{O}_{K_i}$ by $(\mathcal{X}_i)_{\mathcal{O}_{K_i}}$.

Assume that we have chosen basepoints of the $(X_i)_{K_i}$ (which thus induce basepoints of the K_i) and suppose that we are given an *isomorphism of profinite groups* $\Pi_{(X_1)_{K_1}} \xrightarrow{\sim} \Pi_{(X_2)_{K_2}}$, which (by [Mzk7], Lemmas 1.1.4, 1.1.5) induces a *commutative diagram*:

$$\begin{array}{ccc} \Pi_{(X_1)_{K_1}} & \xrightarrow{\sim} & \Pi_{(X_2)_{K_2}} \\ \downarrow & & \downarrow \\ G_{K_1} & \xrightarrow{\sim} & G_{K_2} \end{array}$$

Proposition 1.1. (Group-Theoreticity of Serre-Tate Canonical Liftings) *The Jacobian of $(X_1)_{K_1}$ is Serre-Tate canonical if and only if the same is true of the Jacobian of $(X_2)_{K_2}$.*

Proof. Indeed, this follows from the fact that the Jacobian of $(X_i)_{K_i}$ is a Serre-Tate canonical lifting if and only if its p-adic Tate module *splits* (as a G_{K_i}-module) into a direct sum of an unramified G_{K_i}-module and the Cartier dual of an unramified G_{K_i}-module (cf. [Mess], Chapter V: proof of Theorem 3.3, Theorem 2.3.6; [Mess], Appendix: Corollary 2.3, Proposition 2.5). ○

Remark 1.1.1. As is shown in [DO] (cf. also [OS]), for $p > 2$, $g \geq 4$, the Serre-Tate canonical lifting of the Jacobian of a general proper curve of genus g in characteristic p is *not* a Jacobian. Thus, in some sense, one expects that:

There are not so many curves to which Proposition 1.1 may be applied.

From another point of view, if there exist infinitely many Jacobians of a given genus g over finite extensions of $\mathbb{Q}_p$ which are Serre-Tate canonical liftings, then one expects — cf. the *"André-Oort Conjecture"* ([Edix], Conjecture 1.3) — that every irreducible component of the Zariski closure of the resulting set of points in the moduli stack of principally polarized abelian varieties should be a "subvariety of Hodge type". Moreover, one expects that the intersection of such a subvariety with the Torelli locus (i.e., locus of Jacobians) in the moduli stack of principally polarized abelian varieties should typically be *"rather small"*. Thus, from this point of view as well, one expects that Proposition 1.1 should *not be applicable* to the "overwhelming majority" of curves of genus $g \geq 2$.

Section 2: Arithmetic Hyperbolic Curves

In this §, we show (cf. Theorem 2.4 below) that the theory of *correspondences* (cf. [Mzk3]) of a p-adic hyperbolic curve is completely determined by the abstract profinite group structure of its *arithmetic profinite group*. We begin by reviewing and extending the *theory of [Mzk3]*, as it will be needed in the discussion of the present §.

Let X be a *normal connected algebraic stack* which is *generically "scheme-like"* (i.e., admits an open dense algebraic substack isomorphic to a scheme). Then we shall denote by

$$\mathrm{Loc}(X)$$

the *category* whose *objects* are (necessarily generically scheme-like) algebraic stacks Y that admit a finite étale morphism to X, and whose *morphisms* are finite étale morphisms of stacks $Y_1 \to Y_2$ (that do not necessarily lie over X!). Note that since these stacks are *generically scheme-like*, it makes sense to speak of the *(1-)category* of such objects (so long as our morphisms are finite étale), i.e., there is no need to work with 2-categories.

Given an object Y of $\mathrm{Loc}(X)$, let us denote by

$$\mathrm{Loc}(X)_Y$$

the *category* whose *objects* are morphisms $Z \to Y$ in $\mathrm{Loc}(X)$, and whose morphisms, from an object $Z_1 \to Y$ to an object $Z_2 \to Y$, are the morphisms $Z_1 \to Z_2$ over Y in $\mathrm{Loc}(X)$. Thus, by considering *maximal nontrivial decompositions* of the terminal object of $\mathrm{Loc}(X)_Y$ into a coproduct of nonempty objects of $\mathrm{Loc}(X)_Y$, we conclude that the *set of connected components of* Y may be recovered — *functorially!* — from the *category structure* of $\mathrm{Loc}(Y)$. Finally, let us observe that $\mathrm{Loc}(X)_Y$ may be identified with the category

$$\acute{\mathrm{E}}\mathrm{t}(Y)$$

of *finite étale coverings of* Y (and Y-morphisms).

We would also like to consider the *category*

$$\overline{\mathrm{Loc}}(X)$$

whose *objects* are generically scheme-like algebraic stacks which arise as *finite étale quotients* (in the sense of stacks!) of objects in $\mathrm{Loc}(X)$, and whose *morphisms* are finite étale morphisms of algebraic stacks. Note that $\overline{\mathrm{Loc}}(X)$ may be constructed *entirely category-theoretically* from $\mathrm{Loc}(X)$ by considering the *"category of objects of* $\mathrm{Loc}(X)$ *equipped with a (finite étale) equivalence relation"*. (We leave it to the reader to write out the routine details.)

Definition 2.1.

(i) X will be called *arithmetic* if $\overline{\mathrm{Loc}}(X)$ does not admit a terminal object.

(ii) X will be called a(n) *(absolute) core* if X is a terminal object in $\mathrm{Loc}(X)$.

(ii) X will be said to *admit a(n) (absolute) core* if there exists a terminal object Z in $\overline{\mathrm{Loc}}(X)$. In this case, $\overline{\mathrm{Loc}}(X) = \overline{\mathrm{Loc}}(Z)$, so we shall say that Z is a *core.*

Remark 2.1.1. Let k be a *field.* If X is a *geometrically normal, geometrically connected algebraic stack of finite type over* k, then we shall write

$$\mathrm{Loc}_k(X); \quad \overline{\mathrm{Loc}}_k(X)$$

for the categories obtained as above, except that we assume all the morphisms to be *k-morphisms.* Also, we shall say that X is *k-arithmetic*, or *arithmetic over k* (respectively, a *k-core*, or *core over k*), if $\overline{\mathrm{Loc}}_k(X)$ does not admit a terminal object (respectively, X is a terminal object in $\mathrm{Loc}_k(X)$). On the other hand, when k is *fixed*, and the entire discussion "takes place over k", then we shall often *omit* the "k-" from this terminology.

Remark 2.1.2. Thus, when $k = \mathbb{C}$, a hyperbolic curve X is k-arithmetic if and only if it is arithmetic in the sense of [Mzk3], §2. (Indeed, if X is *non-arithmetic* in the sense of [Mzk3], §2, then a terminal object in $\overline{\mathrm{Loc}}_k(X)$ — i.e., a *"(hyperbolic) core"* — is constructed in [Mzk3], §3, so X is non-k-arithmetic. Conversely, if X is *arithmetic* in the sense of [Mzk3], §2, then (cf. [Mzk3], Definition 2.1, Theorem 2.5) it corresponds to a *fuchsian group* $\Gamma \subseteq SL_2(\mathbb{R})/\{\pm 1\}$ which has *infinite index* in its commensurator $C_{SL_2(\mathbb{R})/\{\pm 1\}}(\Gamma)$ — a fact which precludes the existence of a *k-core.*) Moreover, issues over an *arbitrary algebraically closed k of characteristic zero* may always be *resolved over* $\mathbb{C}$, by Proposition 2.3, (ii), below.

Remark 2.1.3. If we *arbitrarily choose* a finite étale structure morphism to X for every object of $\mathrm{Loc}(X)$, then one verifies easily that every morphism of $\mathrm{Loc}(X)$ *factors* as the composite of an *isomorphism* (not necessarily over X!) with a *(finite étale) morphism over* X (i.e., relative to these arbtirary choices). A similar statement holds for $\mathrm{Loc}_k(X)$.

Definition 2.2. Let X be a smooth, geometrically connected, generically scheme-like algebraic stack of finite type over a field k of *characteristic zero.*

(i) We shall say that X is an *orbicurve* if it is of dimension 1.

(ii) We shall say that X is a *hyperbolic orbicurve* if it is an orbicurve which admits a compactification $X \hookrightarrow \overline{X}$ (necessarily unique!) by a *proper orbicurve* $\overline{X}$ over k such that if we denote the reduced divisor $\overline{X} \backslash X$ by $D \subseteq \overline{X}$, then

$\overline{X}$ is *scheme-like* near D, and, moreover, the line bundle $\omega_{\overline{X}/k}(D)$ on $\overline{X}$ has *positive degree*.

Proposition 2.3. (Independence of the Base Field)

(i) Let k^{sep} be a separable closure of k; X a geometrically normal, geometrically connected algebraic stack of finite type over k. Then X is a k-core (respectively, k-arithmetic) if and only if $X_{k^{\mathrm{sep}}} \stackrel{\mathrm{def}}{=} X \times_k k^{\mathrm{sep}}$ is a k^{sep}-core (respectively, k^{sep}-arithmetic). Moreover, if $X_{k^{\mathrm{sep}}}$ admits a finite étale morphism $X_{k^{\mathrm{sep}}} \to Z_{k^{\mathrm{sep}}}$ to a k^{sep}-core $Z_{k^{\mathrm{sep}}}$, then $Z_{k^{\mathrm{sep}}}$ descends uniquely to a k-core Z of X.

(ii) Suppose that k is algebraically closed of characteristic 0, and that X is a hyperbolic orbicurve. *Next, let k' be an algebraically closed field containing k. Then the natural functors*

$$\mathrm{Loc}_k(X) \to \mathrm{Loc}_{k'}(X \otimes_k k'); \quad \overline{\mathrm{Loc}}_k(X) \to \overline{\mathrm{Loc}}_{k'}(X \otimes_k k')$$

(given by tensoring over k with k') are equivalences *of categories. In particular, X is a k-core (respectively, k-arithmetic) if and only if $X \otimes_k k'$ is a k'-core (respectively, k'-arithmetic).*

Proof. First, we observe that (i) is a formal consequence of the definitions. As for (ii), let us observe first that it suffices to verify the asserted *equivalences of categories*. These equivalences, in turn, are formal consequences of the following *two assertions* (cf. Remark 2.1.3):

(a) The natural functor $\acute{\mathrm{E}}\mathrm{t}(X) \to \acute{\mathrm{E}}\mathrm{t}(X \otimes_k k')$ is an equivalence of categories.

(b) If Y_1, Y_2 are finite étale over X, then

$$\mathrm{Isom}_k(Y_1, Y_2) \to \mathrm{Isom}_{k'}(Y_1 \otimes_k k', Y_2 \otimes_k k')$$

is bijective.

The proofs of these two assertions is an exercise in elementary algebraic geometry, involving the following well-known techniques:

(1) *descending* the necessary diagrams of finite étale morphisms over k' to a subfield $K \subseteq k'$ which is finitely generated over k;

(2) *extending* orbicurves over K to orbicurves over some k-variety V with function field K;

(3) *specializing* orbicurves over V to closed (i.e., k-valued) points v of V;

(4) *base-changing* orbicurves over V to formal completions $\widehat{V}_v$ of V at closed points v;

(5) *deforming* (log) étale morphisms of orbicurves over v to morphisms over the completions $\widehat{V}_v$;

(6) *algebrizing* such deformed morphisms (when the orbicurves involved are proper).

This "elementary exercise" is carried out (for assertion (a) above) in the case when X itself is *proper* in [SGA1], Exposé X, Theorem 3.8. When X is an arbitrary orbicurve as in the statement of (ii), the *same arguments* — centering around the *rigidity* of (log) étale morphisms under infinitesimal deformations — may be used, by considering *compactifications* $(\overline{X}, D)$ of X as in Definition 2.2, (ii), and replacing "étale" by *"étale away from D"*. Note that we use the assumption that k is of characteristic zero here to ensure that *all ramification is tame.*

Finally, assertion (b) may be deduced by similar arguments — by applying, in (5) above, the *fact* (cf. Definition 2.2, (ii)) that, if $\overline{Y} \to \overline{X}$ is any finite morphism of orbicurves over k, then

$$H^0(\overline{Y}, \omega^{\vee}_{\overline{X}/k}(-D)|_{\overline{Y}}) = 0$$

(where "$\vee$" denotes the $\mathcal{O}_{\overline{X}}$*-dual*) in place of the *rigidity* of (log) étale morphisms used to prove assertion (a). $\bigcirc$

Next, for $i = 1, 2$, let K_i be a *finite extension of* $\mathbb{Q}_p$ (where p is a prime number); let $(X_i)_{K_i}$ be a *hyperbolic curve* over K_i. Assume that we have chosen basepoints of the $(X_i)_{K_i}$, which thus induce basepoints/algebraic closures $\overline{K}_i$ of the K_i and determine *fundamental groups* $\Pi_{(X_i)_{K_i}} \stackrel{\mathrm{def}}{=} \pi_1((X_i)_{K_i})$ and *Galois groups* $G_{K_i} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{K}_i/K_i)$. Thus, for $i = 1, 2$, we have an *exact sequence*:

$$1 \to \Delta_{X_i} \to \Pi_{(X_i)_{K_i}} \to G_{K_i} \to 1$$

(where $\Delta_{X_i} \subseteq \Pi_{(X_i)_{K_i}}$ is defined so as to make the sequence exact). Here, we shall think of G_{K_i} as a *quotient* of $\Pi_{(X_i)_{K_i}}$ (i.e., not as an independent group to which $\Pi_{(X_i)_{K_i}}$ happens to surject). By [Mzk7], Lemmas 1.1.4, 1.1.5, this quotient is *characteristic*, i.e., it is *completely determined by the structure of* $\Pi_{(X_i)_{K_i}}$ *as a profinite group.*

THEOREM 2.4. (GROUP-THEORETICITY OF CORRESPONDENCES) *Any isomorphism* $\alpha : \Pi_{(X_1)_{K_1}} \xrightarrow{\sim} \Pi_{(X_2)_{K_2}}$ *induces equivalences of categories:*

$$\mathrm{Loc}_{\overline{K}_1}((X_1)_{\overline{K}_1}) \xrightarrow{\sim} \mathrm{Loc}_{\overline{K}_2}((X_2)_{\overline{K}_2}); \quad \overline{\mathrm{Loc}}_{\overline{K}_1}((X_1)_{\overline{K}_1}) \xrightarrow{\sim} \overline{\mathrm{Loc}}_{\overline{K}_2}((X_2)_{\overline{K}_2})$$

in a fashion that is FUNCTORIAL *in* α.

Proof. Since $\overline{\mathrm{Loc}}_{\overline{K}_i}((X_i)_{\overline{K}_i})$ may be *reconstructed "category-theoretically"* from $\mathrm{Loc}_{\overline{K}_i}((X_i)_{\overline{K}_i})$ (cf. the discussion at the beginning of the present §), in order to prove Theorem 2.4, it thus suffices to show that the isomorphism α induces an equivalence between the categories $\mathrm{Loc}_{\overline{K}_i}((X_i)_{\overline{K}_i})$.

Clearly, the class of *objects* of $\mathrm{Loc}_{\overline{K}_i}((X_i)_{\overline{K}_i})$ may be reconstructed as the class of objects of the category of finite sets with continuous Δ_{X_i}-action. To reconstruct the *morphisms*, it suffices (cf. Remark 2.1.3) to show that given any two *open subgroups* $H_1, J_1 \subseteq \Pi_{(X_1)_{K_1}}$ — which we may assume, without loss of generality, to *surject* onto G_{K_1} — and an isomorphism

$$H_1 \xrightarrow{\sim} J_1$$

that *arises "K_1-geometrically"* (i.e., from a K_1-scheme-theoretic isomorphism between the curves corresponding to H_1, J_1), it is necessarily the case that the corresponding isomorphism

$$H_2 \xrightarrow{\sim} J_2$$

between open subgroups $H_2, J_2 \subseteq \Pi_{(X_2)_{K_2}}$ *arises K_2-geometrically.*

But this *follows formally from the "p-adic version of the Grothendieck Conjecture" proven in [Mzk6], Theorem A*: Indeed, $H_1 \xrightarrow{\sim} J_1$ necessarily lies over an *inner automorphism* $\gamma_1 : G_{K_1} \xrightarrow{\sim} G_{K_1}$. In particular, $H_2 \xrightarrow{\sim} J_2$ lies over an isomorphism $\gamma_2 : G_{K_2} \xrightarrow{\sim} G_{K_2}$, which is obtained by conjugating γ_1 by *some fixed isomorphism* (not necessarily geometric!) arising from α between the *characteristic quotients* $G_{K_1} \xrightarrow{\sim} G_{K_2}$. Since the property of "being an inner automorphism" is *manifestly intrinsic*, we thus conclude that γ_2 is *also an inner automorphism.* This allows us to apply [Mzk6], Theorem A, which implies that $H_2 \xrightarrow{\sim} J_2$ arises K_2-geometrically, as desired. ◯

COROLLARY 2.5. (CONSEQUENCES FOR CORES AND ARITHMETICITY) *Let*

$$\alpha : \Pi_{(X_1)_{K_1}} \xrightarrow{\sim} \Pi_{(X_2)_{K_2}}$$

be an isomorphism. Then:

(i) $(X_1)_{\overline{K}_1}$ *is* $\overline{K}_1$- ARITHMETIC *(respectively, a* $\overline{K}_1$- CORE*) if and only if* $(X_2)_{\overline{K}_2}$ *is* $\overline{K}_2$- ARITHMETIC *(respectively, a* $\overline{K}_2$- CORE*).*

(ii) Suppose that, for $i = 1, 2$, *we are given a finite étale morphism* $(X_i)_{K_i} \to (Z_i)_{K_i}$ *to a* K_i*-core* $(Z_i)_{K_i}$. *Then the isomorphism* α EXTENDS UNIQUELY *to an isomorphism* $\Pi_{(Z_1)_{K_1}} \xrightarrow{\sim} \Pi_{(Z_2)_{K_2}}$.

Proof. Assertion (i) is a formal consequence of Theorem 2.4 and Definition 2.1 (cf. also Remark 2.1.1). In light of Proposition 2.3, (i), assertion (ii) is a formal consequence of Theorem 2.4, at least over *some* corresponding finite Galois extensions K_1', K_2' of K_1, K_2. That the resulting extension $\Pi_{(Z_1)_{K_1'}} \xrightarrow{\sim} \Pi_{(Z_2)_{K_2'}}$ of α is *unique* is a formal consequence of the fact that every open subgroup of $\Pi_{(X_i)_{K_i}}$ has *trivial centralizer* in $\Pi_{(Z_i)_{K_i}}$ (cf. [Mzk7], Lemma 1.3.1, Corollary 1.3.3). Moreover, it follows formally from this triviality of centralizers that, by choosing corresponding normal open subgroups $H_i \subseteq \Pi_{(Z_i)_{K_i}}$ such that $H_i \subseteq \Pi_{X_{K_i'}}$, we may think of $\Pi_{(Z_i)_{K_i}}$ (and its various open subgroups) as *subgroups of* $\mathrm{Aut}(H_i)$, in a fashion which is *compatible* with α and its various (unique) extensions. Thus, since $\Pi_{(Z_i)_{K_i}}$ is *generated* by $\Pi_{(Z_i)_{K_i'}}$ and $\Pi_{(X_i)_{K_i}}$, we conclude that this extension $\Pi_{(Z_i)_{K_1'}} \xrightarrow{\sim} \Pi_{(Z_i)_{K_2'}}$ over the K_i' descends to some $\Pi_{(Z_1)_{K_1}} \xrightarrow{\sim} \Pi_{(Z_2)_{K_2}}$, as desired. ○

Remark 2.5.1. Recall from the theory of [Mzk3] (cf. Remark 2.1.2; Proposition 2.3, (ii), of the discussion above) that $(X_i)_{\overline{K}_i}$ is *arithmetic* if and only if it admits a finite étale cover which is a finite étale cover of a *Shimura curve*, i.e., (equivalently) if there exists a Shimura curve in $\overline{\mathrm{Loc}}_{\overline{K}_i}((X_i)_{\overline{K}_i})$. As is discussed in [Mzk3], Theorem 2.6, a theorem of Takeuchi states that for a given (g,r), there are only *finitely many* isomorphism classes of hyperbolic curves of type (g,r) (over a given algebraically closed field of characteristic zero) which are *arithmetic*. Moreover, a general hyperbolic curve of type (g,r) is not only non-arithmetic; it is, in fact, *equal to its own hyperbolic core* (cf. [Mzk3], Theorem 5.3). Thus, for general curves of a given type (g,r), the structure of the category $\overline{\mathrm{Loc}}((X_i)_{\overline{K}_i})$ is *not* sufficient to determine the isomorphism class of the curve. It is not clear to the author at the time of writing whether or not, in the case when $(X_i)_{K_i}$ is *arithmetic*, the structure of the category $\overline{\mathrm{Loc}}((X_i)_{\overline{K}_i})$ is sufficient to determine the isomorphism class of $(X_i)_{K_i}$. At any rate, just as was the case with Proposition 1.1 (cf. Remark 1.1.1), *Theorem 2.4 does not allow one to recover the isomorphism class of* $(X_i)_{K_i}$ *for "most"* $(X_i)_{K_i}$ — where here we take "most" to mean that (at least for (g,r) sufficiently large) the set of points determined by the curves for which it *is* possible to recover the isomorphism class of $(X_i)_{K_i}$ from the profinite group $(X_i)_{K_i}$ via the method in question *fails to be Zariski dense in the moduli stack of hyperbolic curves of type* (g,r) (cf. Corollary 3.8 below).

Finally, to give the reader a feel for the abstract theory — and, in particular, the state of affairs discussed in Remark 2.5.1 above — we consider the case of *punctured hemi-elliptic orbicurves*, in which the situation is understood somewhat explicitly:

Definition 2.6. Let X be an *orbicurve* (cf. Definition 2.2, (i)) over a field of characteristic zero k.

(i) We shall say that X is a *hemi-elliptic orbicurve* if it is obtained by forming the quotient — in the *sense of stacks* — of an elliptic curve by the action of ± 1.

(ii) We shall say that X is a *punctured hemi-elliptic orbicurve* if it is obtained by forming the quotient — in the *sense of stacks* — of a once-punctured elliptic curve (i.e., the open subscheme given by the complement of the origin in an elliptic curve) by the action of ± 1.

PROPOSITION 2.7. (PUNCTURED HEMI-ELLIPTIC CORES) *Let k be an algebraically closed field of characteristic 0; let X be a* PUNCTURED HEMI-ELLIPTIC ORBICURVE *over k. Then if X is non-k-arithmetic, then X is a k-core. In particular, if X admits nontrivial automorphisms (over k), then X is k-arithmetic. Finally, there exist precisely 4 isomorphism classes of k-arithmetic X, which are described explicitly in [Take2], Theorem 4.1, (i).*

Proof. In the following discussion, we *omit* the "k-". Suppose that X is *non-arithmetic*. Write

$$Y \to X$$

for the unique *double (étale) covering by a punctured elliptic curve* Y, and

$$Y \to Z$$

for the unique morphism to the *core* (i.e., the terminal object in $\overline{\mathrm{Loc}}_k(X) = \overline{\mathrm{Loc}}_k(Y)$). Thus, the induced morphism

$$\overline{Y} = \overline{Y}^{\mathrm{crs}} \to \overline{Z}^{\mathrm{crs}}$$

on the *"coarse moduli spaces"* (cf. [FC], Chapter I, Theorem 4.10) associated to the *canonical compactifications* $\overline{Y}$, $\overline{Z}$ of the orbicurves Y, Z is a *finite ramified covering morphism* — whose degree we denote by d — from an elliptic curve $\overline{Y}$ to a copy of $\mathbb{P}^1_k \cong \overline{Z}^{\mathrm{crs}}$. Note that since $\overline{Y}$ has only *one* "cusp" y_∞ (i.e. point $\in \overline{Y} \backslash Y$), and a point of $\overline{Y}$ is a cusp if and only if its image is a cusp in $\overline{Z}$, it follows that $\overline{Z}$ also has a *unique cusp* z_∞, and that y_∞ is the unique point of $\overline{Y}$ lying over z_∞. Moreover, because $\overline{Y} \to \overline{Z}^{\mathrm{crs}}$ arises from a *finite étale* morphism $Y \to Z$, it follows that the ramification index of $\overline{Y} \to \overline{Z}^{\mathrm{crs}}$ is the *same* at all points of $\overline{Y}$ lying over a given point of $\overline{Z}^{\mathrm{crs}}$. Thus, applying the Riemann-Hurwitz formula yields:

$$0 = -2d + \sum_i \frac{d}{e_i}(e_i - 1)$$

where the e_i are the ramification indices over the points of $\overline{Z}^{\mathrm{crs}}$ at which the covering morphism ramifies. Thus, we conclude that $2 = \sum_i \frac{1}{e_i}(e_i - 1)$. Since all of the e_i are *integers*, one verifies immediately that the only possibilities for the set of e_i's are the following:

$$(2,2,2,2);\ (2,3,6);\ (2,4,4);\ (3,3,3)$$

Note that it follows from the fact that y_∞ is the unique point of $\overline{Y}$ lying over z_∞ that d, as well as the ramification index at z_∞, is *necessarily equal to the largest* e_i. In the case of $(2,2,2,2)$, we thus conclude that $X = Z$, so X is a *core*, as asserted. In the other three cases, we conclude that Y is a *finite étale covering of the orbicurve determined by a "triangle group"* (cf. [Take1]) of one of the following types:

$$(2,3,\infty);\ (2,4,\infty);\ (3,3,\infty)$$

By [Take1], Theorem 3, (ii), such a triangle group is *arithmetic*, so X itself is *arithmetic*, thus contradicting our hypotheses. This completes the proof of the *first assertion* of Proposition 2.7.

The *second (respectively, third) assertion* of Proposition 2.7 is a formal consequence of the first assertion of Proposition 2.7 (respectively, [Take2], Theorem 4.1, (i)). ○

Section 3: Hyperbolically Ordinary Canonical Liftings

In this §, we would like to work over a *finite, unramified extension K of* $\mathbb{Q}_p$, where p is a *prime number* ≥ 5. We denote the ring of integers (respectively, residue field) of K by A (respectively, k). Since $A \cong W(k)$ (the ring of Witt vectors with coefficients in k), we have a natural *Frobenius morphism*

$$\Phi_A : A \to A$$

which lifts the Frobenius morphism $\Phi_k : k \to k$ on k. In the following discussion, the result of base-changing over A (respectively, A; A; $\mathbb{Z}_p$) with k (respectively, K; with A, via Φ_A; $\mathbb{Z}/p^n\mathbb{Z}$, for an integer $n \geq 1$) will be denoted by a *subscript k* (respectively, *subscript K*; *superscript F*; *subscript $\mathbb{Z}/p^n\mathbb{Z}$*).

Let

$$(X \to S \stackrel{\mathrm{def}}{=} \mathrm{Spec}(A),\ D \subseteq X)$$

be a *smooth, pointed curve of type* (g, r) (for which D is the divisor of marked points), where $2g-2+r > 0$ — cf. §0. In the following discussion, we would like to consider the extent to which (X, D) is a *canonical lifting* of (X_k, D_k), in the sense of [Mzk1], Chapter III, §3; Chapter IV. We refer also to the Introduction of [Mzk2] for a *survey of "p-adic Teichmüller theory"* (including the theory of [Mzk1]).

LEMMA 3.1. (CANONICALITY MODULO $\boldsymbol{p}^2$) *Suppose that*

$$Y_K \to X_K$$

is a finite ramified morphism of smooth, proper, geometrically connected curves over K which is unramified away from D_K. Denote the reduced induced subscheme associated to the inverse image in Y_K of D_K by $E_K \subseteq Y_K$. Suppose further that the reduction

$$Y_k \to X_k$$

modulo p of the normalization $Y \to X$ of X in Y_K has the following form:

(i) Y_k is reduced;

(ii) Y_k is smooth over k, except for a total of precisely $\frac{1}{2}(p-1)(2g-2+r)$ (≥ 2) nodes. Moreover, the "order" of the deformation of each node determined by Y is equal to 1 (equivalently: Y is REGULAR *at the nodes), and the special fiber $E_k \subseteq Y_k$ of the closure $E \subseteq Y$ of E_K in Y is a reduced divisor (equivalently: a divisor which is* ÉTALE *over k) at which Y_k is smooth.*

(iii) Y_k has precisely two irreducible components C_V, C_F. Here, the morphism $C_V \to X_k$ (respectively, $C_F \to X_k$) is an isomorphism (respectively, k-isomorphic to the relative Frobenius morphism $\Phi_{X_k/k} : X_k^F \to X_k$ of X_k).

(iv) (X_k, D_k) admits a nilpotent ordinary indigenous bundle (cf. [Mzk1], Chapter II, Definitions 2.4, 3.1) whose supersingular divisor (cf. [Mzk1], Chapter II, Proposition 2.6, (3)) is equal to the image of the nodes of Y_k in X_k.

Then (X, D) is isomorphic modulo p^2 to the CANONICAL LIFTING *(cf. [Mzk1], Chapter III, §3; Chapter IV) determined by the nilpotent indigenous bundle of (iv).*

REMARK 3.1.1. In the context of Lemma 3.1, we shall refer to the points of X_k which are the image of nodes of Y_k as *supersingular points* and to points which are not supersingular as *ordinary*. Moreover, the open subscheme of ordinary points will be denoted by

$$X_k^{\text{ord}} \subseteq X_k$$

and the corresponding *p-adic formal open subscheme* of $\widehat{X}$ (the p-adic completion of X) by $\widehat{X}^{\mathrm{ord}}$. Also, we shall consider X (respectively, Y) to be equipped with the *log structure* (cf. [Kato] for an introduction to the theory of log structures) determined by the monoid of regular functions invertible on $X_K \backslash D_K$ (respectively, $Y_K \backslash E_K$) and denote the resulting *log scheme* by $X^{\log}$ (respectively, $Y^{\log}$). Thus, the morphism of schemes $Y \to X$ extends uniquely to a morphism of log schemes $Y^{\log} \to X^{\log}$.

Proof. First, let us observe that

$$(Y^{\log})^{\mathrm{ord}}_k \cong \{(X^{\log})^{\mathrm{ord}}_k\}^F \bigcup (X^{\log})^{\mathrm{ord}}_k$$

where the isomorphism is the *unique* isomorphism lying over $X^{\log}_k$. Since $(X^{\log})^{\mathrm{ord}}$, $(Y^{\log})^{\mathrm{ord}}$ are *log smooth* over A, it follows that the inclusion $\{(X^{\log})^{\mathrm{ord}}_k\}^F \hookrightarrow (Y^{\log})^{\mathrm{ord}}_k$ lifts to a (not necessarily unique!) inclusion

$$\{(X^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}}\}^F \hookrightarrow (Y^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}}$$

whose *composite*

$$\Psi^{\log} : \{(X^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}}\}^F \to (X^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}}$$

with the natural morphism $(Y^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}} \to (X^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}}$ *is* nevertheless *independent of the choice of lifting of the inclusion*. Indeed, this is formal consequence of the fact that $\Psi^{\log}$ is a *lifting of the Frobenius morphism* on $(X^{\log})^{\mathrm{ord}}_k$ (cf., e.g., the discussion of [Mzk1], Chapter II, the discussion preceding Proposition 1.2, as well as Remark 3.1.2 below).

Of course, $\Psi^{\log}$ might not be regular at the supersingular points, but we may estimate the *order of the poles of* $\Psi^{\log}$ at the supersingular points as follows: Since Y is assumed to be *regular*, it follows that the completion of $Y_{\mathbb{Z}/p^2\mathbb{Z}}$ at a supersingular point ν is given by the formal spectrum Spf of a complete local ring isomorphic to:

$$R_Y \stackrel{\mathrm{def}}{=} (A/p^2 \cdot A)[[s,t]]/(st - p)$$

(where s, t are indeterminates). Thus, modulo p, this completion is a *node*, with the property that *precisely one* branch — i.e., irreducible component — of this node lies on C_F (respectively, C_V). (Indeed, this follows from the fact that both C_F and C_V are *smooth* over k.) Suppose that the irreducible component lying on C_F is defined locally (modulo p) by the equation $t = 0$. Thus, the ring of regular functions on the ordinary locus of C_F restricted to this formal neighborhood of a supersingular point is given by $k[[s]][s^{-1}]$. The connected component of $(Y^{\log})^{\mathrm{ord}}_{\mathbb{Z}/p^2\mathbb{Z}}$ determined by C_F may be thought of as the *open subscheme* "$s \neq 0$". Here, we recall that the parameter s in this discussion is uniquely determined *up to multiplication by an element of* $R_Y^\times$ — cf. [Mzk4], §3.7.

Next, let us write:

$$R'_X \stackrel{\mathrm{def}}{=} \mathrm{Im}(R_Y) \subseteq R_Y[s^{-1}]$$

for the image of R_Y in $R_Y[s^{-1}]$. Then since

$$t = s^{-1} \cdot p \in R_Y[s^{-1}] = (A/p^2 \cdot A)[[s]][s^{-1}]$$

it follows that $R'_X = (A/p^2 \cdot A)[[s]][s^{-1} \cdot p]$. In particular, if we think of

$$R_X \stackrel{\mathrm{def}}{=} (A/p^2 \cdot A)[[s]] \subseteq R'_X$$

— so $R_X[s^{-1}] = R'_X[s^{-1}] = R_Y[s^{-1}]$ — as a local *smooth lifting* of C_F at ν, we thus conclude that *arbitrary regular functions on Spf*(R_Y) *restrict to meromorphic functions on Spf*(R_X) *with poles of order* ≤ 1 *at* ν. Thus, since $\Psi^{\log}$ arises from an *everywhere regular* morphism $Y^{\log} \to X^{\log}$, we conclude that:

$\Psi^{\log}$ *has poles of order* ≤ 1 *at the supersingular points.*

But then the conclusion of Lemma 3.1 follows formally from [Mzk1], Chapter II, Proposition 2.6, (4); Chapter IV, Propositions 4.8, 4.10, Corollary 4.9. ○

Remark 3.1.2. The fact — cf. the end of the first paragraph of the proof of Lemma 3.1 — that the order of a pole of a Frobenius lifting is *independent* of the choice of smooth lifting of the domain of the Frobenius lifting may be understood more *explicitly* in terms of the coordinates used in the latter portion of the proof of Lemma 3.1 as follows: Any *"coordinate transformation"*

$$s \mapsto s + p \cdot g(s)$$

(where $g(s) \in k[[s]][s^{-1}]$) *fixes* — since we are working *modulo* p^2 — functions of the form $s^p + p \cdot f(s)$ (where $f(s) \in k[[s]][s^{-1}]$). This shows that the order of the pole of $f(s)$ does not depend on the choice of parameter s.

In the situation of Lemma 3.1, let us denote the *natural morphism of fundamental groups* (induced by $(\widehat{X}^{\log})^{\mathrm{ord}} \to X^{\log}$) by

$$\Pi_{(\widehat{X}^{\log})^{\mathrm{ord}}} \stackrel{\mathrm{def}}{=} \pi_1((\widehat{X}^{\log})^{\mathrm{ord}}_K) \;\;\rightarrow\;\; \Pi_{X^{\log}} \stackrel{\mathrm{def}}{=} \pi_1(X^{\log}_K) = \pi_1(X_K \backslash D_K)$$

(for some fixed choice of basepoints). Here, we observe that (by the main theorem of [Vala]) $(\widehat{X}^{\log})^{\mathrm{ord}}$ is *excellent*, so the *normalization* of $(\widehat{X}^{\log})^{\mathrm{ord}}$ in a finite étale covering of $(\widehat{X}^{\log})^{\mathrm{ord}}_K$ is *finite* over $(\widehat{X}^{\log})^{\mathrm{ord}}$. Thus, $(\widehat{X}^{\log})^{\mathrm{ord}}_K$ has a "well-behaved theory" of finite étale coverings which is *compatible with étale localization on* $(\widehat{X}^{\log})^{\mathrm{ord}}$. Also, before proceeding, we observe that $\Pi_{X^{\log}}$ fits into an exact sequence:

$$1 \rightarrow \Delta_{X^{\log}} \rightarrow \Pi_{X^{\log}} \rightarrow G_K \rightarrow 1$$

(where $\Delta_{X^{\log}}$ is defined so as to make the sequence exact).

Lemma 3.2. (The Ordinary Locus Modulo $\boldsymbol{p}^2$) *Let $V_{\mathbb{F}_p}$ be a 2-dimensional $\mathbb{F}_p$-vector space equipped with a continuous action of $\Pi_{X^{\log}}$ up to ± 1 — i.e., a representation*

$$\Pi_{X^{\log}} \rightarrow GL_2^{\pm}(V_{\mathbb{F}_p}) \stackrel{\mathrm{def}}{=} GL_2(V_{\mathbb{F}_p})/\{\pm 1\}$$

— such that:

(i) The determinant of $V_{\mathbb{F}_p}$ is isomorphic (as a $\Pi_{X^{\log}}$-module) to $\mathbb{F}_p(1)$.

(ii) There exists a finite log étale Galois covering (i.e., we assume tame ramification over D)

$$X^{\log}_{\pm} \rightarrow X^{\log}$$

such that the action of $\Pi_{X^{\log}}$ up to ± 1 on $V_{\mathbb{F}_p}$ lifts to a (usual) action (i.e., without sign ambiguities) of $\Pi_{X^{\log}_{\pm}} \subseteq \Pi_{X^{\log}}$ on $V_{\mathbb{F}_p}$. This action is uniquely determined up to tensor product with a character of $\Pi_{X^{\log}_{\pm}}$ of order 2.

(iii) The finite étale covering $Y^{\log}_K \rightarrow X^{\log}_K$ determined by the finite $\Pi_{X^{\log}}$-set of 1-dimensional $\mathbb{F}_p$-subspaces of $V_{\mathbb{F}_p}$ satisfies the hypotheses of Lemma 3.1.

(iv) Write

$$(Z^{\log}_{\pm})_K \rightarrow (X^{\log}_{\pm})_K$$

for the finite log étale covering (of degree $p^2 - 1$) corresponding to the nonzero portion of $V_{\mathbb{F}_p}$. Write

$$(Y^{\log}_{\pm})_K \rightarrow (X^{\log}_{\pm})_K$$

for the finite log étale covering of smooth curves which is the composite (i.e., normalization of the fiber product over $X^{\log}_K$) of the coverings $(Z^{\log}_{\pm})_K$, $Y^{\log}_K$

of $X_K^{\log}$. (Thus, $(Z_{\pm}^{\log})_K$ maps naturally to $(Y_{\pm}^{\log})_K$, hence also to $Y_K^{\log}$.) Let us refer to an irreducible component of the special fiber of a stable reduction of $(Y_{\pm}^{\log})_K$ (respectively, $(Z_{\pm}^{\log})_K$) over some finite extension of K that maps FINITELY *to the irreducible component "C_F" (cf. Lemma 3.1) as being* "OF C_F-TYPE" *and "associated to $(Y_{\pm}^{\log})_K$ (respectively, $(Z_{\pm}^{\log})_K$)". Then any irreducible component of C_F-type associated to $(Z_{\pm}^{\log})_K$ is* ÉTALE AND FREE OF NODES *over the* ORDINARY LOCUS *of any irreducible component of C_F-type associated to $(Y_{\pm}^{\log})_K$.*

Then (after possibly tensoring $V_{\mathbb{F}_p}$ with a character of $\Pi_{X_{\pm}^{\log}}$ of order 2) the étale local system $\mathcal{E}_{\mathbb{F}_p}^{\mathrm{ord}}$ on $(\widehat{X}_{\pm}^{\log})_K^{\mathrm{ord}}$ determined by the $\Pi_{(\widehat{X}_{\pm}^{\log})^{\mathrm{ord}}}$-module $V_{\mathbb{F}_p}$ arises from a (logarithmic) finite flat group scheme on $(\widehat{X}_{\pm}^{\log})^{\mathrm{ord}}$. Moreover, the $\Pi_{(\widehat{X}_{\pm}^{\log})^{\mathrm{ord}}}$-module $V_{\mathbb{F}_p}$ fits into an exact sequence:

$$0 \to (V_{\mathbb{F}_p}^{\mathrm{etl}})^{\vee}(1) \to V_{\mathbb{F}_p} \to V_{\mathbb{F}_p}^{\mathrm{etl}} \to 0$$

where $V_{\mathbb{F}_p}^{\mathrm{etl}}$ is a 1-dimensional $\mathbb{F}_p$-space "up to ± 1" whose $\Pi_{(\widehat{X}_{\pm}^{\log})^{\mathrm{ord}}}$-action arises from a finite étale local system on $(X_{\pm}^{\mathrm{ord}})_k \subseteq (X_{\pm})_k$, and the "$\vee$" denotes the $\mathbb{F}_p$-linear dual.

Proof. As was seen in the proof of Lemma 3.1, we have an *isomorphism*

$$(Y^{\log})_k^{\mathrm{ord}} \cong \{(X^{\log})_k^{\mathrm{ord}}\}^F \bigcup (X^{\log})_k^{\mathrm{ord}}$$

which thus determines a *decomposition of $(\widehat{Y}^{\log})^{\mathrm{ord}}$ into two connected components*. Moreover, the *second* connected component on the right-hand side corresponds to a *rank one quotient $V_{\mathbb{F}_p} \twoheadrightarrow Q_{\mathbb{F}_p}$* which is *stabilized* by the action of $\Pi_{(\widehat{X}^{\log})^{\mathrm{ord}}}$, while the *first* connected component on the right-hand side parametrizes *splittings* of this quotient $V_{\mathbb{F}_p} \twoheadrightarrow Q_{\mathbb{F}_p}$. Here, we observe that $Q_{\mathbb{F}_p}^{\otimes 2}$ admits a *natural $\Pi_{(\widehat{X}^{\log})^{\mathrm{ord}}}$-action* (i.e., without sign ambiguities).

Now *any choice of isomorphism* between $\{(\widehat{X}^{\log})^{\mathrm{ord}}\}^F$ and the *first* connected component of $(\widehat{Y}^{\log})^{\mathrm{ord}}$ determines a *lifting of Frobenius*

$$\Phi^{\log} : \{(\widehat{X}^{\log})^{\mathrm{ord}}\}^F \to (\widehat{X}^{\log})^{\mathrm{ord}}$$

which is *ordinary* (by the conclusion of Lemma 3.1 — cf. [Mzk1], Chapter IV, Proposition 4.10). Thus, by the *general theory of ordinary Frobenius liftings*, $\Phi^{\log}$ determines, in particular, a *(logarithmic) finite flat group scheme* annihilated by p which is an *extension* of the trivial finite flat group scheme

"$\mathbb{F}_p$" by the finite flat group scheme determined by the Cartier dual of some étale local system of one-dimensional $\mathbb{F}_p$-vector spaces on X_k^{ord} (cf. [Mzk1], Chapter III, Definition 1.6); denote the $\Pi_{(\widehat{X}^{\log})^{\mathrm{ord}}}$-module corresponding to this étale local system by $\Omega_{\mathbb{F}_p}$. Moreover, it is a formal consequence of this general theory that $\Phi_K^{\log}$ is precisely the covering of $(\widehat{X}^{\log})_K^{\mathrm{ord}}$ determined by considering *splittings of this extension*. Thus, since the Galois closure of this covering has Galois group given by the *semi-direct product* of a cyclic group of order p with a cyclic group of order $p-1$, we conclude (by the elementary group theory of such a semi-direct product) that we have an *isomorphism of* $\Pi_{(\widehat{X}^{\log})^{\mathrm{ord}}}$*-modules*: $(Q_{\mathbb{F}_p})^{\otimes -2}(1) \cong \Omega_{\mathbb{F}_p}(1)$, i.e.,

$$(Q_{\mathbb{F}_p})^{\otimes -2} \cong \Omega_{\mathbb{F}_p}$$

We thus conclude that the local system $\mathcal{E}_{\mathbb{F}_p}^{\Phi^{\log}}$ on $(\widehat{X}^{\log})_K^{\mathrm{ord}}$ determined by this (logarithmic) finite flat group scheme arising from the general theory satisfies:

$$\mathcal{E}_{\mathbb{F}_p}^{\Phi^{\log}}|_{(\widehat{X}_{\pm}^{\log})_K^{\mathrm{ord}}} \cong \mathcal{E}_{\mathbb{F}_p}^{\mathrm{ord}} \otimes_{\mathbb{F}_p} Q_{\mathbb{F}_p}^{\vee}$$

Next, let us write χ_Q for the *character* (valued in $\mathbb{F}_p{}^{\times}$) of $\Pi_{(\widehat{X}_{\pm}^{\log})^{\mathrm{ord}}}$ corresponding to $Q_{\mathbb{F}_p}$. Now it follows formally from condition (iv) of the statement of Lemma 3.2 that the *finite étale covering of* $(\widehat{X}_{\pm}^{\log})_K^{\mathrm{ord}}$ *determined by* $\mathrm{Ker}(\chi_Q)$

$$W_Q \to (\widehat{X}_{\pm}^{\log})_K^{\mathrm{ord}}$$

is *dominated* by the composite of some *finite étale covering of* $\widehat{X}_{\pm}^{\mathrm{ord}}$ and a *"constant covering"* (i.e., a covering arising from a finite extension L of K). Thus, the only *ramification* that may occur in the covering W_Q arises from ramification of the "constant covering", i.e., the finite extension L/K. Moreover, (since $(Q_{\mathbb{F}_p})^{\otimes -2} \cong \Omega_{\mathbb{F}_p}$) the covering determined by $\mathrm{Ker}(\chi_Q^2)$ is *unramified*, so, in fact, we may take L to be the extension $K(p^{\frac{1}{2}})$. This implies that we may write

$$\chi_Q = \chi_Q' \cdot \chi_Q''$$

where the covering determined by the kernel of χ_Q' (respectively, χ_Q'') is finite étale over $\widehat{X}_{\pm}^{\mathrm{ord}}$ (respectively, the covering arising from base-change from K to L). On the other hand, since χ_Q'' *extends naturally* to $\Pi_{X_{\pm}^{\log}}$, we may assume (without loss of generality — cf. condition (ii) of the statement of Lemma 3.2) that χ_Q'' is *trivial*, hence that $Q_{\mathbb{F}_p}$ *arises from an étale local system on* $(X_{\pm}^{\mathrm{ord}})_k$.

But this — together with the isomorphism $\mathcal{E}^{\Phi^{\log}}_{\mathbb{F}_p}|_{(\widehat{X}^{\log}_{\pm})^{\mathrm{ord}}_K} \cong \mathcal{E}^{\mathrm{ord}}_{\mathbb{F}_p} \otimes_{\mathbb{F}_p} Q^{\vee}_{\mathbb{F}_p}$ — implies the conclusion of Lemma 3.2. ◯

LEMMA 3.3. (GLOBAL LOGARITHMIC FINITE FLAT GROUP SCHEME) *Let $V_{\mathbb{F}_p}$ be a 2-dimensional $\mathbb{F}_p$-vector space equipped with a continuous action of $\Pi_{X^{\log}}$ up to ± 1 which satisfies the hypotheses of Lemma 3.2. Then the étale local system $\mathcal{E}_{\mathbb{F}_p}$ on $(X^{\log}_{\pm})_K$ determined by the $\Pi_{X^{\log}_{\pm}}$-module $V_{\mathbb{F}_p}$ arises from a (logarithmic) finite flat group scheme on $X^{\log}_{\pm}$.*

Proof. Write

$$Z \to X_{\pm}$$

for the *normalization* of $X_{\pm}$ in the finite étale covering of $(X^{\log}_{\pm})_K$ determined by the local system $\mathcal{E}_{\mathbb{F}_p}$. Since $X_{\pm}$ is *regular of dimension* 2, it thus follows that Z is *finite and flat* (by the "Auslander-Buchsbaum formula" and "Serre's criterion for normality" — cf. [Mtmu], p. 114, p. 125) over $X_{\pm}$. Moreover, since Z_K is already equipped with a structure of (logarithmic) finite flat group scheme, which, by the conclusion of Lemma 3.2, extends naturally over the generic point of the special fiber of X — since it extends (by the proof of Lemma 3.2) to a *regular*, hence normal, (logarithmic) finite flat group scheme over the ordinary locus — it thus suffices to verify that this finite flat group scheme structure *extends (uniquely) over the supersingular points of* $X_{\pm}$. But this follows formally from [Mtmu], p. 124, Theorem 38 — i.e., the fact (applied to $X_{\pm}$, not Z!) that a meromorphic function on a normal scheme is regular if and only if it is regular at the primes of height 1 — and the fact that Z (hence also $Z \times_{X_{\pm}} Z$) is *finite and flat* over $X_{\pm}$. ◯

LEMMA 3.4. (THE ASSOCIATED DIEUDONNÉ CRYSTAL MODULO $\boldsymbol{p}$) *Let $V_{\mathbb{F}_p}$ be a 2-dimensional $\mathbb{F}_p$-vector space equipped with a continuous action of $\Pi_{X^{\log}}$ up to ± 1 which satisfies the hypotheses of Lemma 3.2. Suppose, further, that the $\Pi_{X^{\log}}$-module (up to ± 1) $V_{\mathbb{F}_p}$ satisfies the following condition:*

($\dagger_M$) *The G_K-module*

$$M \stackrel{\mathrm{def}}{=} H^1(\Delta_{X^{\log}}, \mathrm{Ad}(V_{\mathbb{F}_p}))$$

(where $\mathrm{Ad}(V_{\mathbb{F}_p}) \subseteq \mathrm{End}(V_{\mathbb{F}_p})$ is the subspace of endomorphisms whose trace $= 0$) fits into an exact sequence:

$$0 \to \mathbb{G}^{-1}(M) \to M \to \mathbb{G}^2(M) \to 0$$

where $\mathbb{G}^2(M)$ (respectively, $\mathbb{G}^{-1}(M)$) is isomorphic to the result of tensoring an UNRAMIFIED *G_K-module whose dimension over $\mathbb{F}_p$ is equal to $3g - 3 + r$ with the Tate twist $\mathbb{F}_p(2)$ (respectively, $\mathbb{F}_p(-1)$).*

Then the "$\mathcal{MF}^{\nabla}$-object (up to ± 1)" (cf. [Falt], §2) determined by the $\Pi_{X^{\log}}$*-module (up to ± 1)* $V_{\mathbb{F}_p}$ *(cf. Lemma 3.3) arises from the (unique) nilpotent ordinary indigenous bundle of Lemma 3.1, (iv).*

Proof. First, we recall from the theory of [Falt], §2, that the conclusion of Lemma 3.3 implies that $V_{\mathbb{F}_p}$ arises from an *"$\mathcal{MF}^{\nabla}$-object (up to ± 1)"* on $X^{\log}$, as in the theory of [Falt], §2. Here, the reader uncomfortable with "$\mathcal{MF}^{\nabla}$-objects up to ± 1" may instead work with a usual $\mathcal{MF}^{\nabla}$-object over $X_{\pm}^{\log}$ equipped with an "action of $\mathrm{Gal}(X_{\pm}^{\log}/X^{\log})$ up to ± 1". Write $\mathcal{F}_k$ for the vector bundle on $(X_{\pm})_k$ underlying the $\mathcal{MF}^{\nabla}$-object on $X_{\pm}^{\log}$ determined by $\mathcal{E}_{\mathbb{F}_p}$.

Thus, $\mathcal{F}_k$ is a vector bundle of *rank* 2, whose Hodge filtration is given by a *subbundle* $F^1(\mathcal{F}_k) \subseteq \mathcal{F}_k$ *of rank* 1. Moreover, the *Kodaira-Spencer morphism* of this subbundle, as well as the *"Hasse invariant"*

$$\Phi_{X_{\pm}}^{*} F^1(\mathcal{F}_k)^{\vee} \hookrightarrow \mathcal{F}_k \twoheadrightarrow \mathcal{F}_k/F^1(\mathcal{F}_k) \cong F^1(\mathcal{F}_k)^{\vee}$$

(where $\Phi_{X_{\pm}}$ is the Frobenius morphism on $X_{\pm}$; and the injection is the morphism that arises from the Frobenius action on the $\mathcal{MF}^{\nabla}$-object in question), is *generically nonzero.* Indeed, these facts all follow immediately from our analysis of $\mathcal{E}_{\mathbb{F}_p}$ over the ordinary locus in the proof of Lemma 3.2.

Next, let us observe that *this Hasse invariant has at least one zero.* Indeed, if it were nonzero everywhere, it would follow formally from the general theory of $\mathcal{MF}^{\nabla}$-objects (cf. [Falt], §2) that the $\Pi_{X^{\log}}$-module (up to ± 1) $V_{\mathbb{F}_p}$ admits a $\Pi_{X^{\log}}$*-invariant subspace of* $\mathbb{F}_p$*-dimension* 1 — cf. the situation over the *ordinary locus* in the proof of Lemma 3.2, over which the Hasse invariant is, in fact, nonzero. On the other hand, this implies that $Y_K \to X_K$ admits a section, hence that Y is *not connected.* But this contradicts the fact (cf. the proof of Lemma 3.1) that the two irreducible components C_V, C_F of Y_k (cf. Lemma 3.1, (iii)) necessarily meet at the nodes of Y_k. (Here, we recall from Lemma 3.1, (ii), that there exists at least one node on Y_k.)

In particular, it follows from the fact that the Hasse invariant is generically nonzero, but not nonzero everywhere that *the degree of the line bundle* $F^1(\mathcal{F})$ *on* $(X_{\pm})_k$ *is positive.* Note that since $F^1(\mathcal{F})^{\otimes 2}$ descends naturally to a line bundle $\mathcal{L}$ on X_k, we thus obtain that

$$1 \leq \deg(\mathcal{L}) \leq 2g - 2 + r$$

(where the second inequality follows from the fact that the Kodaira-Spencer morphism in nonzero).

Now, we conclude — from the *p-adic Hodge theory* of [Falt], §2; [Falt], §5, Theorem 5.3 — that the condition $(\dagger_M)$ implies various consequences concerning the *Hodge filtration on the first de Rham cohomology module* of Ad of the $\mathcal{MF}^\nabla$-object determined by $V_{\mathbb{F}_p}$, which may be summarized by the inequality:

$$h^1(X_k, \mathcal{L}^{-1}) = h^0(X_k, \mathcal{L} \otimes_{\mathcal{O}_X} \omega_X) \geq 3g - 3 + r$$

(where "h^i" denotes the dimension over k of "H^i") — cf. [Mzk1], IV, Theorem 1.3 (and its proof), which, in essence, addresses the $\mathbb{Z}_p$ analogue of the present $\mathbb{F}_p$-vector space situation. (Note that here we make *essential use* of the hypothesis $p \geq 5$.) Thus, (cf. *loc. cit.*) we conclude that (since $\deg(\mathcal{L}) > 0$) the line bundle $\mathcal{L} \otimes_{\mathcal{O}_X} \omega_X$ on X_k is *nonspecial*, hence (by the above inequality) that:

$$\begin{aligned} \deg(\mathcal{L}) &= \deg(\mathcal{L} \otimes_{\mathcal{O}_X} \omega_X) - \deg(\omega_X) \\ &= h^0(X_k, \mathcal{L} \otimes_{\mathcal{O}_X} \omega_X) + (g-1) - 2(g-1) \\ &\geq 3g - 3 + r - (g-1) = 2g - 2 + r \end{aligned}$$

Combining this with the inequalities of the preceding paragraph, we thus obtain that $\deg(\mathcal{L}) = 2g - 2 + r$, so the $\mathcal{MF}^\nabla$-object in question is an *indigenous bundle*, which is necessarily equal to the indigenous bundle of Lemma 3.1, (iv), since the supersingular locus of the former is contained in the supersingular locus of the latter (cf. [Mzk1], Chapter II, Proposition 2.6, (4)). ○

Lemma 3.5. (Canonical Deformations Modulo Higher Powers of $\boldsymbol{p}$) *Let $V_{\mathbb{F}_p}$ be a 2-dimensional $\mathbb{F}_p$-vector space equipped with a continuous action of $\Pi_{X^{\log}}$ up to ± 1 which satisfies the hypotheses of Lemmas 3.2, 3.4. Suppose that, for some $n \geq 1$:*

(i) (X, D) is isomorphic modulo p^n to a canonical lifting *(as in [Mzk1], Chapter III, §3; Chapter IV).*

(ii) $V_{\mathbb{F}_p}$ is the reduction modulo p of a rank 2 free $\mathbb{Z}/p^n\mathbb{Z}$-module $V_{\mathbb{Z}/p^n\mathbb{Z}}$ with continuous $\Pi_{X^{\log}}$-action up to ± 1.

Then (X, D) is isomorphic modulo p^{n+1} to a canonical lifting*, and the $\Pi_{X^{\log}}$-set $\mathbb{P}(V_{\mathbb{Z}/p^n\mathbb{Z}})$ (of free, rank one $\mathbb{Z}/p^n\mathbb{Z}$-module quotients of $V_{\mathbb{Z}/p^n\mathbb{Z}}$) is isomorphic to the projectivization of the* canonical representation *modulo p^n (cf. [Mzk1], Chapter IV, Theorem 1.1) associated to (X, D). Finally, if the determinant of $V_{\mathbb{Z}/p^n\mathbb{Z}}$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})(1)$, then the $\Pi_{X^{\log}}$-module (up to ± 1) $V_{\mathbb{Z}/p^n\mathbb{Z}}$ is isomorphic to the canonical representation modulo p^n.*

Proof. First, we observe that the case $n = 1$ is a formal consequence of Lemmas 3.1, 3.4. The case of general n is then, in essence, a *formal consequence of the theory of [Mzk1], Chapter V, §1* — cf. especially, Theorem 1.7, and the discussion following it. We review the details as follows:

The *space of deformations* (of the projectivization) of the $\Pi_{X^{\log}}$-module "up to ± 1" $V_{\mathbb{F}_p}$ may be thought of as a *formal scheme*

$$\mathcal{R}$$

which is noncanonically isomorphic to $\mathrm{Spf}(\mathbb{Z}_p[[t_1, \dots, t_{2(3g-3+r)}]])$ (where the t_i's are indeterminates) — cf. the discussion preceding [Mzk1], Chapter V, Lemma 1.5. Write $\mathcal{R}^{\mathrm{PD}}$ for the *p-adic completion of the PD-envelope of* $\mathcal{R}$ at the $\mathbb{F}_p$-valued point defined by "$V_{\mathbb{F}_p}$". Note that $\mathcal{R}$ and $\mathcal{R}^{\mathrm{PD}}$ are equipped with a *natural* G_K*-action.* Then according to the theory of *loc. cit.*, there is a G_K*-equivariant closed immersion of formal schemes* (cf. Remark 3.5.1 below)

$$\kappa^{\mathrm{PD}} : \mathrm{Spf}(\widehat{\mathcal{D}}^{\mathrm{Gal}}) \hookrightarrow \mathcal{R}^{\mathrm{PD}}$$

where $\widehat{\mathcal{D}}^{\mathrm{Gal}}$ is noncanonically isomorphic to the p-adic completion of the PD-envelope at the closed point of a power series ring $\mathbb{Z}_p[[t_1, \dots, t_{3g-3+r}]]$ equipped with a natural G_K-action.

Now it follows from the theory of *loc. cit.*, the induction hypothesis on n, and the assumptions (i), (ii) of Lemma 3.5, that $V_{\mathbb{Z}/p^{n-1}\mathbb{Z}} \stackrel{\mathrm{def}}{=} V_{\mathbb{Z}/p^n\mathbb{Z}} \otimes \mathbb{Z}/p^{n-1}\mathbb{Z}$ corresponds (at least projectively) to the *canonical representation modulo* p^{n-1}, hence determines a G_K*-invariant rational point*

$$\sigma_{n-1} \in \mathcal{R}^{\mathrm{PD}}(\mathbb{Z}/p^{n-1}\mathbb{Z})$$

that *lies in the image* $\mathrm{Im}(\kappa^{\mathrm{PD}})$ *of* κ^{PD}. Thus, the point

$$\sigma_n \in \mathcal{R}^{\mathrm{PD}}(\mathbb{Z}/p^n\mathbb{Z})$$

determined by $V_{\mathbb{Z}/p^n\mathbb{Z}}$ may be regarded as a G_K*-invariant deformation* of σ_{n-1}. Note that the set of deformations of σ_{n-1} naturally forms a *torsor* $\mathcal{T}$ *over the* $\mathbb{F}_p$*-vector space* M of Lemma 3.4. Since $\sigma_{n-1} \in \mathrm{Im}(\kappa^{\mathrm{PD}})$, this torsor is equipped with a natural G_K*-stable subspace*

$$\mathcal{T}'' \subseteq \mathcal{T}$$

(consisting of the deformations that lie $\in \mathrm{Im}(\kappa^{\mathrm{PD}})$) which is (by the theory of *loc. cit.*) a *torsor over* $\mathbb{G}^{-1}(M)$. In particular, this subspace determines a G_K*-invariant trivialization* τ' of the $\mathbb{G}^2(M)$-torsor

$$(\mathcal{T} \twoheadrightarrow)\ \mathcal{T}'$$

given by the "change of structure group $M \twoheadrightarrow \mathbb{G}^2(M)$".

Now let us observe that by $(\dagger_M)$ and the fact that $p \geq 5$ — so the square of the cyclotomic character $G_K \to \mathbb{F}_p{}^\times$ is *nontrivial* — $\mathbb{G}^2(M)$ has no nontrivial Galois invariants, i.e.:

$$\mathbb{G}^2(M)^{G_K} = 0$$

Thus, we conclude that τ' is the *unique* G_K-invariant point of $\mathcal{T}'$, hence that the image in $\mathcal{T}'$ of the point $\tau_n \in \mathcal{T}$ determined by σ_n is necessarily equal to τ', i.e., $\tau_n \in \mathcal{T}''$ — or, in other words, $\sigma_n \in \mathrm{Im}(\kappa^{\mathrm{PD}})$.

On the other hand, if we interpret the *Galois-theoretic fact* that σ_{n-1} lifts to a *G_K-invariant* $\sigma_n \in \mathrm{Im}(\kappa^{\mathrm{PD}})$ in terms of the *original finite étale coverings* — combinatorial information concerning which the Galois theory is intended to encode — then we obtain the following conclusion: The *A-valued point*

$$\alpha \in \mathcal{N}(A)$$

of the $\mathbb{Z}_p$-smooth p-adic formal scheme $\mathcal{N} \stackrel{\mathrm{def}}{=} \mathcal{N}^{\mathrm{ord}}_{g,r}$ (cf. [Mzk1], Chapter III, §2) determined by (X, D) and the nilpotent ordinary indigenous bundle modulo p of Lemma 3.4 not only lies — by assumption (i) of the statement of Lemma 3.5 — in the image of $\mathcal{N}(A)$ under the $(n-1)$-st iterate $\Phi_{\mathcal{N}}^{n-1}$ of the *canonical Frobenius lifting*

$$\Phi_{\mathcal{N}} : \mathcal{N} \to \mathcal{N}$$

on (cf. [Mzk1], Chapter III, Theorem 2.8) but also in the image of $\mathcal{N}(A)$ under the *n-th iterate $\Phi_{\mathcal{N}}^n$ of* $\Phi_{\mathcal{N}}$. (Indeed, the restriction of the covering $\Phi_{\mathcal{N}}^{n-1}$ (respectively, $\Phi_{\mathcal{N}}^n$) to α *admits a section*, determined by the G_K-invariant rational point σ_{n-1} (respectively, σ_n).) Thus, we conclude that $X^{\log}$ is *canonical modulo* p^{n+1}. Finally, since

$$\mathbb{G}^{-1}(M)^{G_K} = 0$$

we conclude that σ_n is the *unique G_K-invariant lifting* of σ_{n-1} to $\mathbb{Z}/p^n\mathbb{Z}$, hence that $V_{\mathbb{Z}/p^n\mathbb{Z}}$ corresponds (projectively) to the *canonical representation modulo* p^n, as desired. ◯

Remark 3.5.1. In some sense, it is natural to think of $\mathrm{Im}(\kappa^{\mathrm{PD}})$ (cf. the proof of Lemma 3.5) as the *"crystalline locus"* in the space of "all" representations $\mathcal{R}^{\mathrm{PD}}$.

Theorem 3.6. (Group-Theoreticity of Canonical Liftings) *Let $p \geq 5$ be a prime number. For $i = 1, 2$, let K_i be an* unramified *finite extension of $\mathbb{Q}_p$, and (X_i, D_i) a* smooth pointed curve *of type (g_i, r_i) over $\mathcal{O}_{K_i}$, where $2g_i - 2 + r_i > 0$. Assume that we have chosen basepoints of the $(X_i)_{K_i} \backslash (D_i)_{K_i}$ (which thus induce basepoints of the K_i); denote the resulting fundamental group by $\Pi_{X_i^{\log}}$. Suppose that we have been given an* isomorphism of profinite groups*:*

$$\Pi_{X_1^{\log}} \xrightarrow{\sim} \Pi_{X_2^{\log}}$$

Then:

(i) (X_1, D_1) is a canonical lifting *(in the sense of [Mzk1], Chapter III, §3; Chapter IV) if and only if (X_2, D_2) is so.*

(ii) If at least one of the (X_i, D_i) is a canonical lifting, then the isomorphism on logarithmic special fibers of [Mzk7], Theorem 2.7, lifts *(uniquely) to an isomorphism $(X_1, D_1) \xrightarrow{\sim} (X_2, D_2)$ over $\mathcal{O}_{K_1} \cong W(k_1) \xrightarrow{\sim} W(k_2) \cong \mathcal{O}_{K_2}$.*

Proof. Let us verify (i). Since, by [Mzk7], Theorem 2.7 (and [Mzk7], Proposition 1.2.1, (vi)), the logarithmic special fibers of all stable reductions of all finite étale coverings of $(X_i)_{K_i} \backslash (D_i)_{K_i}$ are *"group-theoretic"*, it follows that the conditions (i), (ii), (iii), (iv) of Lemma 3.1, as well as the conditions (i), (ii), (iii), (iv) of Lemma 3.2, are all *group-theoretic* conditions which, moreover, (by the theory of [Mzk1], Chapter III, §3; Chapter IV) are satisfied by canonical liftings. (Here, relative to the assertion that canonical liftings satisfy Lemma 3.1, (ii), and Lemma 3.2, (iv), we remind the reader that:

(1) Since $p \geq 5$, the special fiber of the curve Y of Lemma 3.1 has ≥ 2 nodes (cf. Lemma 3.1, (ii)), which implies that the curve Y is *stable* (i.e., even without the marked points).

(2) The *smooth locus* of *any* model of a curve over a discrete valuation ring *necessarily* maps to the *stable model* (whenever it exists) of the curve — cf., e.g., [JO]— and, moreover, whenever this map is *quasi-finite*, necessarily embeds as an *open subscheme of the smooth locus* of the stable model.)

Moreover, (since the cyclotomic character and inertia subgroup are group-theoretic — cf. [Mzk7], Proposition 1.2.1, (ii), (vi) — it follows that) condition $(\dagger_M)$ of Lemma 3.4 is a *group-theoretic* condition which (by the theory of *loc. cit.*) is satisfied by canonical liftings. Thus, successive application of Lemma 3.5 for $n = 1, 2, \ldots$ implies assertion (i) of the statement of Theorem 3.6.

Next, let us observe that when one (hence both) of the (X_i, D_i) is a canonical lifting, it follows from Lemma 3.1 that the isomorphism of special fibers

$$(X_1, D_1)_{k_1} \xrightarrow{\sim} (X_2, D_2)_{k_2}$$

(lying over some isomorphism $k_1 \xrightarrow{\sim} k_2$) determined by [Mzk7], Theorem 2.7 is compatible with the nilpotent ordinary indigenous bundles on either side that give rise to the canonical liftings. On the other hand, by the theory of *loc. cit.*, the lifting of $(X_i, D_i)_{k_i}$ over $\mathcal{O}_{K_i} \cong W(k_i)$ is determined uniquely by the fact that this lifting is "canonical" (i.e., when it is indeed the case that it is canonical!). This completes the proof of assertion (ii) of the statement of Theorem 3.6. ◯

Remark 3.6.1. Thus, (cf. Remarks 1.1.1, 2.2.1) unlike the situation with Proposition 1.1, Theorem 2.2:

Theorem 3.6 provides, for each hyperbolic (g, r), *"lots of examples"* — in particular, an example lifting a general curve of type (g, r) in characteristic $p \geq 5$ — of (X_K, D_K) which are *group-theoretically determined solely by the profinite group* $\pi_1(X_K \backslash D_K)$.

In fact, the exact same arguments of the present §3 show that the *analogue of Theorem 3.6 also holds for "Lubin-Tate canonical curves (for various tones* ϖ*)"* — i.e., the curves defined by considering *canonical points* (cf. [Mzk2], Chapter VIII, §1.1) associated to the *canonical Frobenius lifting* of [Mzk2], Chapter VIII, Theorem 3.1, in the case of a "VF-pattern Π of pure tone ϖ".

One feature of the Lubin-Tate case that *differs* (cf. [Mzk7], Proposition 1.2.1, (vi)) from the "classical ordinary" case of [Mzk1] is that it is not immediately clear that the *"Lubin-Tate character"*

$$\chi : G_K \to W(\mathbb{F}_q)^\times$$

(where $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_p$) is *group-theoretic*. Note, however, that at least for the *"portion of* χ *modulo* p*"*

$$G_K \to {\mathbb{F}_q}^\times$$

group-theoreticity — at least after passing to a *finite unramified extension* of the original base field K (which does not present any problems, from the point of view of proving the Lubin-Tate analogue of Theorem 3.6) — is a consequence of the fact that the *field structure* on (the union of 0 and) the torsion in G_K^{ab} of order prime to p is group-theoretic (cf. [Mzk7], Lemma 2.6, Theorem 2.7). This much is *sufficient for the Lubin-Tate analogues* of Lemmas 3.1, 3.2, 3.3, 3.4, 3.5 (except for the last sentence of the statement of Lemma 3.5, which is, at any rate, not necessary to prove Theorem 3.6), and hence of Theorem 3.6. Finally, once one has proved that the curve in question is (Lubin-Tate) *canonical* and recovered its canonical representation $V_{\mathbb{Z}_p}$, at least *projectively*, then it follows, by considering the $W(\mathbb{F}_q)$-module analogue of the exact sequence of $\mathbb{F}_p$-vector spaces in the conclusion of Lemma 3.2, over the ordinary locus, that (even if one only knows $V_{\mathbb{Z}_p}$ "projectively") one may *recover the Lubin-Tate character* by forming

$$\begin{aligned}&\mathrm{Hom}(\text{third nonzero term of the exact sequence},\\ &\qquad\qquad \text{first nonzero term of the exact sequence})\end{aligned}$$

— at least *up to un "étale twist"*, i.e., up to multiplication by some *unramified* character $G_K \to W(\mathbb{F}_q)^\times$. (We leave the remaining routine technical details of the Lubin-Tate case to the enthusiastic reader.) At the time of writing, it is not clear to the author whether or not it is possible to eliminate this "étale twist". Since this étale twist corresponds to the *well-known dependence of the Lubin-Tate group on the choice of uniformizer*, this indeterminacy with respect to an étale twist may be thought of as being related to the fact that (at the present time) the author is unable to prove the *group-theoreticity of the natural uniformizer "p"* — cf. [Mzk7], Remark 2.7.2.

At any rate, the theory of the present §3 constitutes the case of "tone 0". Moreover, one checks easily — by considering the "FL-bundle" (as in [Mzk1], Chapter II, Proposition 1.2) determined by the lifting modulo p^2 — that canonical curves of distinct tones are never isomorphic. Thus, (at least when $r = 0$) the Lubin-Tate canonical curves give rise to (strictly) more examples of (proper) hyperbolic X_K which are group-theoretically determined solely by the profinite group $\pi_1(X_K)$. This prompts the following interesting question: Is this "list" complete? — i.e.:

Do there exist any other curves (X_K, D_K) that are group-theoretically determined solely by the profinite group $\pi_1(X_K \backslash D_K)$?

At the time of writing, the author does not even have a conjectural answer to this question.

REMARK 3.6.2. One interesting aspect of the theory of the present §3 is that, to the knowledge of the author:

It constitutes the first *application* of the "p-adic Teichmüller theory" of [Mzk1], [Mzk2], to prove a *hitherto unknown result* (cf. Corollary 3.8 below) that lies *outside* — i.e., can be *stated* without using the terminology, concepts, or results of — the theory of [Mzk1], [Mzk2].

Moreover, not only does this constitute the first application of "p-adic Teichmüller theory" to prove a *new* result (cf. the proof of the irreducibility of the moduli stack via p-adic Teichmüller theory in [Mzk2], Chapter III, §2.5

— an application, albeit to an *old* result), it is interesting relative to the *original philosophical motivation* for this theory, involving the analogy to *uniformization theory/Teichmüller theory over the complex numbers*, which was to construct a p-adic theory that would allow one to prove a *"p-adic version of the Grothendieck Conjecture"* as in [Mzk6] — cf. [Mzk2], Introduction, §0.10, for more on these ideas.

REMARK 3.6.3. One interesting point of view is the following:

For a hyperbolic curve X_K over a finite extension K of $\mathbb{Q}_p$, consideration of the profinite group Π_{X_K} should be thought of as the *arithmetic analogue* of considering a hyperbolic curve (which is given *a priori*) over $\mathbb{F}_p[[t]][t^{-1}]$ — where t is an indeterminate which, perhaps, should be thought of as the *symbol "p"* — "IN THE ABSOLUTE", i.e., "stripped of its structure morphism to a *specific* copy of $\mathbb{F}_p[[t]][t^{-1}]$", or, alternatively, "when we allow the indeterminate t to *vary freely* (in $\mathbb{F}_p[[t]]$)".

Thus, from this point of view, it is *natural* to expect that the hyperbolic curves X_K most likely to be recoverable from the absolute datum Π_{X_K} are those which are "defined over some (fictitious) ABSOLUTE FIELD OF CONSTANTS inside K" — hence which have moduli that are *invariant* with respect to changes of variable $t \mapsto t + t^2 + \dots$. In particular, since one expects *canonical curves* to be arithmetic analogues of "curves defined over the constant field" (cf. [Mzk2], Introduction, §2.3), it is perhaps not surprising that they should satisfy the property of Theorem 3.6.

Moreover, this point of view suggests that:

Perhaps it is natural to regard Theorem 3.6 as the proper analogue for hyperbolic canonical curves of the fact that Serre-Tate canonical liftings (of abelian varieties) are defined over number fields (cf. [Mzk2], Introduction, §2.1, Open Question (7)).

Indeed, one way of showing that Serre-Tate canonical liftings — or, indeed, arbitrary abelian varieties with lots of endomorphisms — are defined over number fields is by thinking of the algebraic extension $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ over which such abelian varieties are a priori defined *"in the absolute"*, i.e., as a *transcendental extension of* $\mathbb{Q}$ and considering what happens when one transports such abelian varieties via *arbitrary field automorphisms of* $\overline{\mathbb{Q}}_p$. Such field automorphisms are reminiscent of the *"changes of variable"* appearing in the approach to thinking about "recovering X_K from the absolute datum Π_{X_K}" described above.

REMARK 3.6.4. The *"rigidity"* of canonical curves — in the sense that they are determined by the existence of the *unique* G_K-invariant lifting "$V_{\mathbb{Z}_p}$" of the representation $V_{\mathbb{F}_p}$ (cf. Lemma 3.5 and its proof) — is reminiscent, at least at a technical level, of the theory of deformations of representations applied in *Wiles' famous proof of the "modularity conjecture"* (cf. [Wiles]). It would be interesting if this analogy could be pursued in more detail in the future.

Remark 3.6.5. Just as the Serre-Tate canonical coordinates are used in [Mzk5], §9, to prove a *weak p-adic Grothendieck Conjecture-type result* for hyperbolic curves over p-adic fields whose Jacobians have ordinary reduction, the techniques of the present § may be applied — by using the *canonical coordinates* of [Mzk1]— to prove a *similar (but in some sense even weaker) p-adic Grothendieck Conjecture-type result* for hyperbolic curves over absolutely unramified p-adic fields which are isomorphic to *canonical curves (as in [Mzk1]) modulo* p^2. Thus, the true significance of the theory of the present § lies in its *wide applicability in the canonical lifting case* (cf. Corollary 3.8 below), a feature which differs substantially from the theory in the case of ordinary Jacobians (cf. Remark 1.1.1).

Definition 3.7. Let Y_L be a hyperbolic curve over a finite extension L of $\mathbb{Q}_p$. Then we shall say that Y_L is *absolute* if for every other hyperbolic curve $Y'_{L'}$ over a finite extension L' of $\mathbb{Q}_p$,

$$\pi_1(Y_L) \cong \pi_1(Y'_{L'})$$

(as profinite groups) implies that $Y'_{L'}$ is isomorphic as a $\mathbb{Q}_p$-scheme to Y_L. Also, we shall refer to points in moduli stacks of hyperbolic curves over $\mathbb{Q}_p$ that are defined by absolute hyperbolic curves as *absolute*.

Corollary 3.8. (Application of $\boldsymbol{p}$-adic Teichmüller Theory)

(i) A general pointed smooth curve (X_k, D_k) of type (g, r), where $2g-2+r > 0$, over a finite field k of characteristic $p \geq 5$ may be lifted to a pointed smooth curve (X_K, D_K) over the quotient field K of the ring of Witt vectors $A = W(k)$ such that the hyperbolic curve $X_K \backslash D_K$ is absolute.

(ii) In particular, for each (g, r), $p \geq 5$, there exists a Zariski dense *— hence (at least when $3g - 3 + r \geq 1$) infinite — set of* absolute points*, valued in absolutely unramified finite extensions of $\mathbb{Q}_p$, of the moduli stack of hyperbolic curves of type (g, r) over $\mathbb{Q}_p$.*

Proof. Assertion (i) follows formally from Theorem 3.6; [Mzk7], Lemmas 1.1.4, 1.1.5; and [Mzk7], Proposition 1.2.1, (v). Assertion (ii) follows formally from assertion (i) and the following elementary argument: The scheme-theoretic closure of the points of assertion (i) in the (compactified) moduli stack over $\mathbb{Z}_p$ forms a $\mathbb{Z}_p$- *flat* proper algebraic stack Z with the property that $Z \otimes \mathbb{F}_p$ is equal to the entire moduli stack over $\mathbb{F}_p$, hence is smooth of dimension $3g-3+r$. But this implies — by $\mathbb{Z}_p$-*flatness* — that $Z \otimes \mathbb{Q}_p$ is also of dimension $3g-3+r$, hence equal to the entire moduli stack over $\mathbb{Q}_p$, as desired. $\bigcirc$

Bibliography

Unpublished RIMS preprints are available as .ps files at:

`http://www.kurims.kyoto-u.ac.jp/~kenkyubu/paper/all.html`

[DM] P. Deligne and D. Mumford, The Irreducibility of the Moduli Space of Curves of Given Genus, *IHES Publ. Math.* 36 (1969), pp. 75-109.

[DO] B. Dwork and A. Ogus, Canonical liftings of Jacobians, *Compositio Math.* 58 (1986), pp. 111-131.

[Edix] B. Edixhoven, On the André-Oort conjecture for Hilbert modular surfaces, *Moduli of abelian varieties (Texel Island, 1999)*, *Progr. Math.* 195, Birkhäuser (2001), pp. 133-155.

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

[FC] G. Faltings and C.-L. Chai, *Degenerations of Abelian Varieties*, Springer-Verlag (1990).

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

[JO] A. J. de Jong and F. Oort, On Extending Families of Curves, *Journal of Alg. Geom.* 6 (1997), pp. 545-562.

[Kato] K. Kato, Logarithmic Structures of Fontaine-Illusie, *Proceedings of the First JAMI Conference*, Johns Hopkins University Press (1990), pp. 191-224.

[Knud] F. F. Knudsen, The Projectivity of the Moduli Space of Stable Curves, II, *Math. Scand.* 52 (1983), 161-199.

[Mtmu] H. Matsumura, *Commutative Algebra (Second Edition)*, The Benjamin/Cummings Publishing Company (1980).

[Mess] W. Messing, *The Crystals Associated to Barsotti-Tate Groups; with Applications to Abelian Schemes*, *Lecture Notes in Mathematics* 264, Springer-Verlag (1972).

[Mzk1] S. Mochizuki, A Theory of Ordinary p-adic Curves, *Publ. of RIMS* 32 (1996), pp. 957-1151.

[Mzk2] S. Mochizuki, *Foundations of p-adic Teichmüller Theory*, AMS/IP Studies in Advanced Mathematics 11, American Mathematical Society/International Press (1999).

[Mzk3] S. Mochizuki, Correspondences on Hyperbolic Curves, *Journ. Pure Appl. Algebra* 131 (1998), pp. 227-244.

[Mzk4] S. Mochizuki, The Geometry of the Compactification of the Hurwitz Scheme, *Publ. of RIMS* 31 (1995), pp. 355-441.

[Mzk5] S. Mochizuki, The Profinite Grothendieck Conjecture for Closed Hyperbolic Curves over Number Fields, *J. Math. Sci., Univ. Tokyo* 3 (1996), pp. 571-627.

[Mzk6] S. Mochizuki, The Local Pro-p Anabelian Geometry of Curves, *Invent. Math.* 138 (1999), pp. 319-423.

[Mzk7] S. Mochizuki, *The Absolute Anabelian Geometry of Hyperbolic Curves*, RIMS Preprint No. 1363 (June 2002).

[NTM] H. Nakamura, A. Tamagawa, and S. Mochizuki, The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves, *Sugaku Expositions* 14 (2001), pp. 31-53.

[OS] F. Oort and T. Sekiguchi, The canonical lifting of an ordinary Jacobian variety need not be a Jacobian variety, *J. Math. Soc. Japan* 38 (1986), pp. 427-437.

[SGA1] *Revêtement étales et groupe fondamental*, Séminaire de Géometrie Algébrique du Bois Marie 1960-1961 (SGA1), dirigé par A. Grothendieck, augmenté de deux exposés de M. Raynaud, *Lecture Notes in Mathematics* 224, Springer-Verlag (1971).

[Take1] K. Takeuchi, Arithmetic Triangle Groups, *Journ. Math. Soc. Japan* 29 (1977), pp. 91-106.

[Take2] K. Takeuchi, Arithmetic Fuchsian Groups with Signature $(1;e)$, *Journ. Math. Soc. Japan* 35 (1983), pp. 381-407.

[Tama] A. Tamagawa, The Grothendieck Conjecture for Affine Curves, *Compositio Math.* 109 (1997), pp. 135-194.

[Vala] P. Valabrega, A Few Theorems on Completion of Excellent Rings, *Nagoya Math J.* 61 (1976), pp. 127-133.

[Wiles] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* 141 (1995), pp. 443-551.

Shinichi Mochizuki
Research Institute
for Mathematical Sciences
Kyoto University
Kyoto 606-8502, Japan
motizuki@kurims.kyoto-
u.ac.jp