Compositio Mathematica **109:** 135–194, 1997.

The Grothendieck conjecture for affine curves

AKIO TAMAGAWA
Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-01, Japan
e-mail: tamagawa@kurims.kyoto-u.ac.jp

Received: 15 April 1996; accepted in final form 7 May 1996

Abstract. We prove that the isomorphism class of an affine hyperbolic curve defined over a field finitely generated over $\mathbb{Q}$ is completely determined by its arithmetic fundamental group. We also prove a similar result for an affine curve defined over a finite field.

Introduction

Let k be a field, and Y a k-scheme, geometrically connected and of finite type over k. Then we have the following exact sequence of profinite groups:

$$1 \to \pi_1\left(Y \bigotimes_k k^{\mathrm{sep}}, *\right) \to \pi_1(Y, *) \xrightarrow{\mathrm{pr}_Y} G_k \to 1. \tag{0-1}$$

Here, G_k is the absolute Galois group $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ of the field k, $*$ is a suitable geometric point, and π_1 means the étale fundamental group ([SGA]). The exact sequence above yields the following outer Galois representation

$$\rho_Y \colon G_k \to \mathrm{Out}\left(\pi_1\left(Y \bigotimes_k k^{\mathrm{sep}}, *\right)\right), \tag{0-2}$$

where, for a topological group G, $\mathrm{Out}(G)$ means the group $\mathrm{Aut}(G)$ of continuous group automorphisms of G divided by the group $\mathrm{Inn}(G)$ of inner automorphisms of G.

Recall that, if k is of characteristic 0 and an inclusion $\bar{k} \hookrightarrow \mathbb{C}$ is given, then $\pi_1(Y \otimes_k \bar{k}, *)$ is isomorphic to the profinite completion of the topological fundamental group of the complex analytic space $Y(\mathbb{C})$, hence it is determined by the homotopy type of $Y(\mathbb{C})$. For example, if Y is a proper, smooth, geometrically connected curve over such k, the profinite group $\pi_1(Y \otimes_k \bar{k}, *)$ is completely determined (up to isomorphism) by the genus of Y. Thus, in order to get more information on the k-scheme Y, we need to look at the relation between $\pi_1(Y \otimes_k \bar{k}, *)$ and the Galois group G_k, i.e. the exact sequence (0–1) or the outer Galois representation (0-2).

When k is finitely generated over $\mathbb{Q}$, A. Grothendieck proposed the following philosophy ([Grothendieck 1], [Grothendieck 2]):

If Y is anabelian, then the group-theoretical data $(\pi_1(Y,*), \mathrm{pr}_Y)$ (or $(\pi_1(Y \otimes_k k^{\mathrm{sep}}, *), \rho_Y)$) functorially determines the isomorphism class of the k-scheme Y.

Although we do not have any general definition of the term 'anabelian', hyperbolic curves have been regarded as typical examples of anabelian schemes. Here, a smooth, geometrically connected curve U over k is called hyperbolic, if it satisfies $\chi(U) \stackrel{\mathrm{def}}{=} 2-2g-n < 0$, where $g = g_U$ is the genus of the smooth compactification X of U, and $n = n_U$ is the cardinality of $S(\bar{k})$, where $S = X - U$. Thus, in this case, the philosophy above gives the following:

CONJECTURE (0.1). *Let k be a field finitely generated over $\mathbb{Q}$. Let U_1 and U_2 be hyperbolic curves over k. Then:*

(i) (*Weak form.*) *If there exists an isomorphism $\mathcal{F}$: $\pi_1(U_1,*) \to \pi_1(U_2,*)$ with $\mathrm{pr}_{U_1} = \mathrm{pr}_{U_2} \circ \mathcal{F}$, then U_1 is isomorphic to U_2 over k.*

(ii) (*Strong form.*) *The natural map*

$$\mathrm{Isom}_{(\mathrm{Schemes}/k)}(U_1, U_2) \to \mathrm{Isom}_{G_k}(\pi_1(U_1,*), \pi_1(U_2,*))/\mathrm{Inn}\left(\pi_1\left(U_2 \bigotimes_k \bar{k}, *\right)\right)$$

is bijective, where

$$\mathrm{Isom}_{G_k}(\pi_1(U_1,*), \pi_1(U_2,*)) \stackrel{\mathrm{def}}{=} \{\mathcal{F} \in \mathrm{Isom}(\pi_1(U_1,*), \pi_1(U_2,*)) \mid \mathrm{pr}_{U_1} = \mathrm{pr}_{U_2} \circ \mathcal{F}\}.$$

In terms of the outer Galois representations, the formulation of this conjecture is as follows:

CONJECTURE (0.2). *Notations and assumptions as in Conjecture* (0.1)*, then:*

(i) (*Weak form.*) *If there exists an isomorphism $\bar{\mathcal{F}}$: $\pi_1(U_1 \otimes_k \bar{k}, *) \to \pi_1(U_2 \otimes_k \bar{k}, *)$ with* $\mathrm{Out}(\bar{\mathcal{F}}) \circ \rho_{U_1} = \rho_{U_2}$*, then U_1 is isomorphic to U_2 over k.* (*Here,* $\mathrm{Out}(\bar{\mathcal{F}})$ *denotes the isomorphism* $\mathrm{Out}(\pi_1(U_1 \otimes_k \bar{k}, *)) \to \mathrm{Out}(\pi_1(U_2 \otimes_k \bar{k}, *))$ *induced by $\bar{\mathcal{F}}$.*)

(ii) (*Strong form.*) *The natural map*

$$\mathrm{Isom}_{(\mathrm{Schemes}/k)}(U_1, U_2) \to \mathrm{Isom}^{\mathrm{Out}}_{G_k}\left(\pi_1\left(U_1 \bigotimes_k \bar{k}, *\right), \pi_1\left(U_2 \bigotimes_k \bar{k}, *\right)\right) \Big/ \mathrm{Inn}\left(\pi_1\left(U_2 \bigotimes_k \bar{k}, *\right)\right)$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

is bijective, where

$$\begin{aligned}
&\mathrm{Isom}^{\mathrm{Out}}_{G_k}\left(\pi_1\left(U_1 \bigotimes_k \bar{k}, *\right), \pi_1\left(U_2 \bigotimes_k \bar{k}, *\right)\right) \\
&\quad \stackrel{\mathrm{def}}{=} \left\{ \bar{\mathcal{F}} \in \mathrm{Isom}\left(\pi_1\left(U_1 \bigotimes_k \bar{k}, *\right), \pi_1\left(U_2 \bigotimes_k \bar{k}, *\right)\right) \right. \\
&\qquad \left. \Big| \ \mathrm{Out}(\bar{\mathcal{F}}) \circ \rho_{U_1} = \rho_{U_2} \right\}.
\end{aligned}$$

In fact, Conjectures (0.1) and (0.2) are equivalent to each other. (See Section 7, A.)

The following is one of the main results of the present paper:

THEOREM (0.3). (cf. (6.3), (7.2).) *Conjecture* (0.1) $(=$ *hence* $(0.2))$ *is valid for affine* $(=$ *non-proper, i.e.* $n_{U_i} > 0)$ *hyperbolic curves* U_1, U_2 *over* k.

Partial results (weak form for genus 0 and 1) on Conjecture (0.1) have been obtained by H. Nakamura ([Nakamura 1], [Nakamura 2], [Nakamura 5]). (See also [Voevodskiĭ].) We also have the following Theorem of F. Pop ([Pop 1], [Pop 2]), which is regarded as a function field version of Conjecture (0.1).

THEOREM (Pop). *Let* k *be a field finitely generated over* $\mathbb{Q}$. *Let* X_1 *and* X_2 *be proper, smooth curves over* k. *Then the natural map*

$$\begin{aligned}
&\mathrm{Isom}_{(\mathrm{Schemes}/k)}(\mathrm{Spec}(k(X_1)), \mathrm{Spec}(k(X_2))) \\
&\quad \to \mathrm{Isom}_{G_k}(G_{k(X_1)}, G_{k(X_2)})/\mathrm{Inn}(G_{\bar{k}(X_2)})
\end{aligned}$$

is bijective.

Recently ([Pop 3]), he generalized this result to higher-dimensional varieties. Combining Theorem (0.3) with the main result of [Pop 3], we also obtain the following absolute version of Theorem (0.3).

THEOREM (0.4). (cf. (6.1).) *For each* $i = 1, 2$, *let* k_i *be a field finitely generated over* $\mathbb{Q}$ *and* U_i *an affine hyperbolic curve over* k_i. *Then the natural map*

$$\mathrm{Isom}_{(\mathrm{Schemes})}(U_1, U_2) \to \mathrm{Isom}(\pi_1(U_1, *), \pi_1(U_2, *))/\mathrm{Inn}(\pi_1(U_2, *))$$

is bijective. In particular, if $\pi_1(U_1, *)$ *is isomorphic to* $\pi_1(U_2, *)$, *then* U_1 *is isomorphic to* U_2.

We derive Theorem (0.3) from the following finite field version, which is another main result of the present paper:

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

THEOREM (0.5). (cf. (4.3).) *For each $i = 1, 2$, let k_i be a finite field and U_i an affine hyperbolic curve over k_i. Then the natural map*

$$\begin{aligned}&\mathrm{Isom}_{(\mathrm{Schemes})}(U_1, U_2)\\ &\quad\to \mathrm{Isom}(\pi_1^{\mathrm{tame}}(U_1, *), \pi_1^{\mathrm{tame}}(U_2, *))/\mathrm{Inn}(\pi_1^{\mathrm{tame}}(U_2, *))\end{aligned}$$

is bijective. In particular, if $\pi_1^{\mathrm{tame}}(U_1, *)$ is isomorphic to $\pi_1^{\mathrm{tame}}(U_2, *)$, then U_1 is isomorphic to U_2.

Here, π_1^{tame} means the tame fundamental group ([SGA, Exp. XIII], [GM]).

Simultaneously with Theorem (0.5), we also prove the following (which is not related to Theorem (0.3)):

THEOREM (0.6). (cf. (4.3).) *For each $i = 1, 2$, let k_i be a finite field and U_i an affine (not necessarily hyperbolic) curve over k_i. Then the natural map*

$$\mathrm{Isom}_{(\mathrm{Schemes})}(U_1, U_2) \to \mathrm{Isom}(\pi_1(U_1, *), \pi_1(U_2, *))/\mathrm{Inn}(\pi_1(U_2, *))$$

is bijective. In particular, if $\pi_1(U_1, *)$ is isomorphic to $\pi_1(U_2, *)$, then U_1 is isomorphic to U_2.

This is an affirmative answer to a slight modification of [Harbater, Question 1.12]. (Strictly speaking, the answer to the original question is negative in general. See (6.4) and (7.3)(ii).)

Roughly speaking, the proof of Theorems (0.5) and (0.6) is a modification of K. Uchida's proof of the following function field version of Theorem (0.6) ([Uchida]):

THEOREM (Uchida). *For each $i = 1, 2$, let k_i be a finite field and X_i a proper, smooth, geometrically connected curve over k_i. Then the natural map*

$$\begin{aligned}&\mathrm{Isom}_{(\mathrm{Schemes})}(\mathrm{Spec}(k_1(X_1)), \mathrm{Spec}(k_2(X_2)))\\ &\quad\to \mathrm{Isom}(G_{k_1(X_1)}, G_{k_2(X_2)})/\mathrm{Inn}(G_{k_2(X_2)})\end{aligned}$$

is bijective.

Starting from the profinite group $G_{k(X)}$, where k is a finite field and X is a proper, smooth, geometrically connected curve over k, Uchida (1) characterized the decomposition groups D_v (v: a closed point of X) in $G_{k(X)}$; (2) recovered the multiplicative group $k(X)^\times$; and (3) recovered the additive structure on $k(X) = k(X)^\times \cup \{0\}$.

In Step (1), he used a method concerning Brauer groups, after Neukirch. In the present case, the group $H^2(D_v, \mathbb{Q}/\mathbb{Z}(1)')$, where $'$ means the prime-to-char(k) part, vanishes for all closed points v of U, since $I_v = \{1\}$ and $D_v \simeq \widehat{\mathbb{Z}}$ for such v. So, instead, we exploit a completely different method, concerning Galois sections

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

and rational points. The main idea of our method is described in the following simplest case:

PROPOSITION (0.7). (cf. (2.10), (3.8).) *Let k be a finite field and X a proper hyperbolic curve over k. Let $s : G_k \to \pi_1(X, *)$ be a continuous group-theoretical section of* pr_X. *Then, $s(G_k)$ is the decomposition group (determined up to conjugacy) of some k-rational (closed) point of X if and only if $X_{\mathcal{H}}(k) \neq \emptyset$ for each open subgroup $\mathcal{H}$ of $\pi_1(X, *)$ containing $s(G_k)$, where $X_{\mathcal{H}}$ denotes the finite étale covering of X corresponding to $\mathcal{H}$. Moreover, the condition $X_{\mathcal{H}}(k) \neq \emptyset$ is equivalent to the following group-theoretical condition:*

$$\sum_{j=0}^{2} (-1)^j \mathrm{tr}_{\mathbb{Z}_l}(\varphi_k^{-1} \mid H^j_{\mathrm{cont}}(\mathcal{H} \cap \mathrm{Ker}(\mathrm{pr}_X), \mathbb{Z}_l)) > 0,$$

where φ_k is the $\sharp(k)$-th power Frobenius element in G_k, and l is an arbitrary prime number distinct from $\mathrm{char}(k)$.

In Step (2), Uchida resorted to class field theory for the function field $k(X)$. His proof goes well also in the present case, if we assume that U is affine. In his function field case, not only the multiplicative group of the function field but also the valuation and the reduction at each closed point of X were recovered. In our case, the valuation is recovered at each closed point of X, but the reduction is recovered only at each closed point of $S = X - U$.

In Step (3), he used infinitely many reductions freely, to prove the additivity of the multiplicative isomorphism $k_1(X_1) \simeq k_2(X_2)$ recovered from a given (topological) group isomorphism $G_{k_1(X_1)} \simeq G_{k_2(X_2)}$. In the present case, only finitely many reductions are at our disposal. Here is one of the main difficulties in our proof, which we overcome, roughly speaking, by constructing sufficiently many good elements in the function field.

We shall review the contents of the present paper in more detail. In Section 1, we collect generalities on the fundamental groups of curves. In Section 2, we show the formalism of our Galois section method of characterizing the decomposition groups group-theoretically, which is applied to not only finite fields but also more general fields, like p-adic local fields and fields finitely generated over $\mathbb{Q}$. In Section 3, we show how to recover various invariants of a curve from its fundamental group. In the finite field case, the contents of Section 2 and Section 3 give the complete characterization of the decomposition groups. In the other cases, we have no method (like the Lefschetz trace formula) of detecting whether at least one rational point exists or not, so the formalism in Section 2 remains to be a mere formalism, for the present. (See the end of Section 2.) In Section 4, we give the proof of Theorems (0.5) and (0.6), whose outline we have already described. In Section 5, we study the fundamental groups of curves over discrete valuation fields. Given a good family of hyperbolic curves over the spectrum of a discrete valuation ring, we

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

show how to recover the tame fundamental group of the special fiber from the (tame) fundamental group of the generic fiber. The main ingredient of our solution of this problem is the following criterion for good reduction of a hyperbolic curve over a discrete valuation field in terms of the monodromy on the pro-l fundamental group of the curve, which might be of interest, independently of the Grothendieck conjecture.

THEOREM (0.8). (cf. (5.3).) *Let S be the spectrum of a discrete valuation ring, and η (resp. s) its generic (resp. closed) point. Let X be a proper, smooth, geometrically connected curve over η, and D a relatively étale divisor in X/η. Put $U = X - D$ and assume that U is hyperbolic. Then the following conditions are equivalent:*

(i) *(X, D) has good reduction at s, i.e. there exist a proper, smooth S-scheme $\mathfrak{X}$ and a relatively étale divisor $\mathfrak{D}$ in $\mathfrak{X}/S$, whose generic fiber $(\mathfrak{X}_\eta, \mathfrak{D}_\eta)$ is isomorphic to (X, D) over η.*

(ii) *The image of the inertia group of η in $\mathrm{Out}(\pi_1(U_{\eta^{\mathrm{sep}}}, *)^l)$ is trivial for some (or all) prime number $l \neq \mathrm{char}(\kappa(s))$, where G^l means the maximal pro-l quotient of a given profinite group G.*

For D empty, this theorem is due to Oda ([Oda 1], [Oda 2]). In Section 6, we prove Theorem (0.3), using the results in Section 4 and Section 5, together with some global arguments. In Section 7, we give three complementary remarks – the relation between Conjectures (0.1) and (0.2), an application of Theorem (0.3) to profinite group theory, and an alternative proof of Pop's theorem above as a corollary of Theorem (0.3).

Remark (0.9). (i) Although we did not fix the geometric points $*$ in this section, we will fix them and exclude ambiguity of the inner automorphisms in the text.

(ii) In the text, we will also prove certain pro-$\mathcal{C}$ versions of the theorems above, where $\mathcal{C}$ is a full class of finite groups containing all finite abelian groups.

1. Generalities on the fundamental groups of curves

In this section, we fix the notations used in the text, and recall some general facts on the étale fundamental groups of algebraic curves.

Let k be a field of characteristic $p \geqslant 0$. Let U be a smooth, geometrically connected curve over k, and X the smooth compactification of U, which is a proper, smooth, geometrically connected curve over k. Put $S = X - U$, and regard it as a (possibly empty) reduced closed subscheme of X. Define non-negative integers $g = g_U = g_X$ and $n = n_U$ to be the genus of X over k and the cardinality of $S(\bar{k})$, respectively. Let ξ be the generic point of U, and put $K = \kappa(\xi)$, the function field of U.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Fix a separable closure k^{sep}, and define $\bar{U}$, $\bar{X}$, $\bar{S}$, and $\bar{\xi}$ to be $U \otimes_k k^{\mathrm{sep}}$, $X \otimes_k k^{\mathrm{sep}}$, $S \otimes_k k^{\mathrm{sep}}$, and $\xi \otimes_k k^{\mathrm{sep}}$, respectively. Note that $\bar{\xi}$ is identified with the generic point of $\bar{U}$.

Take a geometric point $\overline{\bar{\xi}}$ of $\bar{U}$ above the generic point $\bar{\xi}$. Note that $\overline{\bar{\xi}}$ also defines a geometric point of U above ξ. Let the symbol $\cdot$ denote either (unrestricted) or tame. Then we have the following exact sequence of profinite groups:

$$1 \to \pi_1^{\cdot}(\bar{U}, \overline{\bar{\xi}}) \to \pi_1^{\cdot}(U, \overline{\bar{\xi}}) \xrightarrow{\mathrm{pr}} G_k \to 1, \tag{1-1}$$

where $\pi_1^{\mathrm{tame}}(U, \overline{\bar{\xi}})$ (resp. $\pi_1^{\mathrm{tame}}(\bar{U}, \overline{\bar{\xi}})$) means the tame fundamental group of X (resp. $\bar{X}$) with respect to S (resp. $\bar{S}$). (See [SGA, Exp. XIII], [GM].)

We shall introduce a variant of (1-1) above. Let $\mathcal{C}$ be a *full* class of finite groups, i.e. $\mathcal{C}$ is closed under taking subgroups, quotients, finite products, and extensions. For a profinite group Π, $\Pi^{\mathcal{C}}$ denotes the maximal pro-$\mathcal{C}$ quotient of Π. When $\mathcal{C}$ is the class of l-groups (resp. l'-groups, i.e. finite groups of order prime to l), where l is a prime number or 0, write Π^{l} (resp. $\Pi^{l'}$) instead of $\Pi^{\mathcal{C}}$. Here we mean by 0-group (resp. 0′-group) trivial group (resp. finite group). Given a profinite group Π and its (closed) normal subgroup $\overline{\Pi}$, we denote $\Pi/\mathrm{Ker}(\overline{\Pi} \to \overline{\Pi}^{\mathcal{C}})$ by $\Pi^{(\mathcal{C})}$. Observe that $\Pi^{(\mathcal{C})}$ coincides with $\Pi^{\mathcal{C}}$ if and only if $G \overset{\mathrm{def}}{=} \Pi/\overline{\Pi}$ is a pro-$\mathcal{C}$ group. By definition, we have the following:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \overline{\Pi} & \longrightarrow & \Pi & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \overline{\Pi}^{\mathcal{C}} & \longrightarrow & \Pi^{(\mathcal{C})} & \longrightarrow & G & \longrightarrow & 1,
\end{array}$$

where the rows are exact and the columns are surjective. Applying this to (1-1), we obtain:

$$1 \to \pi_1^{\cdot}(\bar{U}, \overline{\bar{\xi}})^{\mathcal{C}} \to \pi_1^{\cdot}(U, \overline{\bar{\xi}})^{(\mathcal{C})} \xrightarrow{\mathrm{pr}} G_k \to 1. \tag{1-2}$$

Observe that (1-2) yields the outer Galois representation

$$G_k \to \mathrm{Out}(\pi_1^{\cdot}(\bar{U}, \overline{\bar{\xi}})^{\mathcal{C}}).$$

The Galois-theoretical interpretation of the exact sequence (1-2) is as follows. Define $\tilde{K} = \tilde{K}^{\cdot,\mathcal{C}}$ to be the maximal pro-$\mathcal{C}$ Galois extension of Kk^{sep} in $\kappa(\overline{\bar{\xi}})/Kk^{\mathrm{sep}}$, unramified on U, and, if $\cdot$ = tame, (at most) tamely ramified on S. Then the sequence (1-2) is canonically identified with the following:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(\tilde{K}/Kk^{\mathrm{sep}}) & \longrightarrow & \mathrm{Gal}(\tilde{K}/K) & \longrightarrow & \mathrm{Gal}(Kk^{\mathrm{sep}}/K) & \longrightarrow & 1. \\
 & & & & & & \| & & \\
 & & & & & & G_k & &
\end{array}$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Note that $\mathrm{Gal}(\tilde{K}/K)$ (resp. $\mathrm{Gal}(\tilde{K}/Kk^{\mathrm{sep}})$) coincides with $\mathrm{Aut}(\tilde{U}/U)$ (resp. $\mathrm{Aut}(\tilde{U}/\bar{U})$), where we define $\tilde{U} = \tilde{U}^{\cdot,\mathcal{C}}$ to be the integral closure of U in $\tilde{K}$.

For a closed subgroup $\mathcal{H} \subset \pi_1^{\cdot}(U, \overline{\overline{\xi}})^{(\mathcal{C})}$, denote by $U_{\mathcal{H}}$ the sub-covering in $\tilde{U}/U$ corresponding to $\mathcal{H}$, and define $k_{\mathcal{H}}$ to be the integral closure of k in $U_{\mathcal{H}}$, which is a separable extension in k^{sep}/k. If $\mathcal{H}$ is open, then $k_{\mathcal{H}}$ is finite over k, and $U_{\mathcal{H}}$ is a smooth, geometrically connected curve over $k_{\mathcal{H}}$. We denote invariants of $U_{\mathcal{H}}/k_{\mathcal{H}}$ by the corresponding symbols for U/k with subscript $\mathcal{H}$, like $X_{\mathcal{H}}$, $S_{\mathcal{H}}$, $g_{\mathcal{H}}$, $n_{\mathcal{H}}$, $K_{\mathcal{H}}$, etc. Putting $\bar{\mathcal{H}} = \mathcal{H} \cap \pi_1^{\cdot}(\bar{U}, \overline{\overline{\xi}})^{\mathcal{C}}$, we have the following exact sequence:

$$1 \to \bar{\mathcal{H}} \to \mathcal{H} \to \mathrm{pr}(\mathcal{H}) \to 1,$$

which is canonically identified with

$$1 \to \pi_1^{\cdot}(\overline{U_{\mathcal{H}}}, \overline{\overline{\xi}})^{\mathcal{C}} \to \pi_1^{\cdot}(U_{\mathcal{H}}, \overline{\overline{\xi}})^{(\mathcal{C})} \to G_{k_{\mathcal{H}}} \to 1,$$

or

$$1 \to \mathrm{Gal}(\tilde{K}/K_{\mathcal{H}}k^{\mathrm{sep}}) \to \mathrm{Gal}(\tilde{K}/K_{\mathcal{H}}) \to \mathrm{Gal}(K_{\mathcal{H}}k^{\mathrm{sep}}/K_{\mathcal{H}}) \to 1.$$

In our approach to the Grothendieck conjecture, it is important to observe not only U itself but also all the coverings $U_{\mathcal{H}}$.

Next, we recall some properties of the profinite group $\overline{\Pi} \stackrel{\mathrm{def}}{=} \pi_1^{\cdot}(\bar{U}, \overline{\overline{\xi}})$.

For a (discrete) group Γ, denote by $\widehat{\Gamma}^{\mathcal{C}}$ the pro-$\mathcal{C}$ completion of Γ, and, when $\mathcal{C}$ is the class of all finite groups (resp. l-groups, resp. l'-groups), denote it also by $\widehat{\Gamma}$ (resp. $\widehat{\Gamma}^{l}$, resp. $\widehat{\Gamma}^{l'}$). Define a discrete group $\Pi_{g,n}$ for non-negative integers g and n by:

$$\begin{aligned}\Pi_{g,n} \;=\; &\langle \alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g, \gamma_1, \ldots, \gamma_n \\ &\mid \alpha_1\beta_1\alpha_1^{-1}\beta_1^{-1} \ldots \alpha_g\beta_g\alpha_g^{-1}\beta_g^{-1}\gamma_1 \ldots \gamma_n = 1\rangle,\end{aligned}$$

which is known to be isomorphic to the topological fundamental group of a compact Riemann surface of genus g minus n points. Note that $\Pi_{g,n}$ is isomorphic to F_{2g+n-1} if $n > 0$, where F_r denotes the free group of rank r.

The following is well-known. (See [SGA], except for the description of $\overline{\Pi}^p$.)

PROPOSITION (1.1). (i) *If* $\mathrm{char}(k) = 0$, *then* $\overline{\Pi} \simeq \widehat{\Pi}_{g,n}$.

(ii) *Assume* $\mathrm{char}(k) = p > 0$. *Then* $\overline{\Pi}^{p'} \simeq \widehat{\Pi}^{p'}_{g,n}$. *For* $\cdot =$ *tame or* $n = 0$, $\overline{\Pi}$ *is a quotient of* $\widehat{\Pi}_{g,n}$, *hence is* (*topologically*) *finitely generated, and* $\overline{\Pi}^p$ *is isomorphic to the free pro-*p *group* $\widehat{F}_r^p$ *of* rank r, *where* r *is the* p-rank *of the Jacobian variety of* X *over* k (*hence* $0 \leqslant r \leqslant g$). *For* $\cdot =$ (*unrestricted*) *and* $n > 0$, $\overline{\Pi}$ *is not finitely generated, and* $\overline{\Pi}^p$ *is a free pro-*p *group of infinite rank* $|\bar{k}|$. □

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Put

$$\varepsilon \overset{\text{def}}{=} \begin{cases} 0, & \text{for } n = 0, \\ 1, & \text{for } n > 0. \end{cases}$$

COROLLARY (1.2).

$$\overline{\Pi}^{\text{ab}} \simeq \begin{cases} \widehat{\mathbb{Z}}^{\oplus 2g+n-\varepsilon}, & \text{char}(k) = 0, \\ (\widehat{\mathbb{Z}}^{p'})^{\oplus 2g+n-\varepsilon} \times \mathbb{Z}_p^{\oplus r}, & \text{char}(k) = p > 0; n = 0 \\ & \quad \textit{or } \cdot = \textit{tame}, \\ (\widehat{\mathbb{Z}}^{p'})^{\oplus 2g+n-\varepsilon} \times \prod_{i \in I} \mathbb{Z}_p, \ \sharp(I) = |\bar{k}|, & \text{char}(k) = p > 0; n > 0 \\ & \quad \textit{and } \cdot = (\textit{unrestricted}). \ \square \end{cases}$$

Remark (1.3). We have the following information on the G_k-module structure of $\overline{\Pi}^{\text{ab}}$. If $n = 0$, i.e. $U = X$, then we have a canonical isomorphism:

$$\overline{\Pi}^{\text{ab}} \simeq T(J_X), \tag{1-3}$$

where J_X means the jacobian variety of X and

$$T(A) \overset{\text{def}}{=} \varprojlim_m \text{Ker}(m \cdot \text{id}\colon A \to A)(\bar{k}),$$

is the Tate module of an abelian variety A over k. If $n > 0$ and $\cdot =$ tame, then we have the following exact sequence:

$$0 \to \widehat{\mathbb{Z}}^{p'}(1) \to \mathbb{Z}[S(\bar{k})] \bigotimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{p'}(1) \to \overline{\Pi}^{\text{ab}} \to T(J_X) \to 0, \tag{1-4}$$

where $\mathbb{Z}[S(\bar{k})]$ denotes the free $\mathbb{Z}$-module with basis $S(\bar{k})$, to which the G_k-action on $S(\bar{k})$ is extended, and

$$\widehat{\mathbb{Z}}^{p'}(1) = \varprojlim_{p \nmid m} \text{Ker}(m \cdot \text{id}\colon \mathbb{G}_m \to \mathbb{G}_m)(\bar{k})$$

$$= \varprojlim_m \text{Ker}(m \cdot \text{id}\colon \mathbb{G}_m \to \mathbb{G}_m)(\bar{k}),$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

where $\mathbb{G}_m$ is the multiplicative group scheme over k. (We usually write $\widehat{\mathbb{Z}}(1)$ instead of $\widehat{\mathbb{Z}}^{0'}(1)$.) In general, if $n > 0$, we have the following exact sequence at least:

$$0 \to \widehat{\mathbb{Z}}^{p'}(1) \to \mathbb{Z}[S(\bar{k})] \bigotimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{p'}(1) \to (\overline{\Pi}^{\mathrm{ab}})^{p'} \to T(J_X)^{p'} \to 0. \tag{1-5}$$

COROLLARY (1.4). (i) *Assume either* $\mathrm{char}(k) = 0$ *or* $\cdot =$ *tame. Then* $\overline{\Pi}$ *is trivial if and only if* $2 - 2g - n > 0$, *i.e.* $(g, n) = (0, 0)$ *or* $(0, 1)$, *and* $\overline{\Pi}$ *is abelian if and only if* $2 - 2g - n \geqslant 0$, *i.e.* $(g, n) = (0, 0), (0, 1)$, *or* $(1, 0)$.

(ii) *Assume* $\mathrm{char}(k) > 0$ *and* $\cdot =$ (*unrestricted*). *Then* $\overline{\Pi}$ *is trivial if and only if* $(g, n) = (0, 0)$, *and* $\overline{\Pi}$ *is abelian if and only if* $(g, n) = (0, 0)$ *or* $(1, 0)$. □

We shall investigate two important properties of $\overline{\Pi}$, namely, torsion-freeness and center-freeness. Here, we say that a profinite group is torsion-free (resp. center-free), if it has no non-trivial elements of finite order (resp. if its center is trivial).

LEMMA (1.5). *Let G be a profinite group. If H^{ab} is torsion-free for each open subgroup H of G, then G is torsion-free.*

Proof. For a projective system $\{G_\lambda\}$ of profinite groups, we can easily check the equality $(\varprojlim G_\lambda)^{\mathrm{ab}} = \varprojlim (G_\lambda)^{\mathrm{ab}}$. Since any closed subgroup of G is the intersection of open subgroups of G, it follows that H^{ab} is torsion-free for each *closed* subgroup H. This completes the proof, since any finite subgroup of G is closed. □

PROPOSITION (1.6). $\overline{\Pi}^{\mathcal{C}}$ *is torsion-free.*

Proof. By (1.5), it suffices to check that H^{ab} is torsion-free for each open subgroup H of $\overline{\Pi}^{\mathcal{C}}$. Let $\widetilde{H}$ be the inverse image of H in $\overline{\Pi}$. Then H is identified with $\widetilde{H}^{\mathcal{C}}$. (Note that $\overline{\Pi}/\widetilde{H} = \overline{\Pi}^{\mathcal{C}}/H$ is a finite group in $\mathcal{C}$ and that $\mathcal{C}$ is full.) Now $H^{\mathrm{ab}} = (\widetilde{H}^{\mathcal{C}})^{\mathrm{ab}} = (\widetilde{H}^{\mathrm{ab}})^{\mathcal{C}}$ is torsion-free by (1.2). (Apply it to U_H.) This completes the proof. □

Remark (1.7). In fact, we can prove more: the cohomological dimension of the profinite group $\overline{\Pi}^{\mathcal{C}}$ is $\leqslant 2 < \infty$. We omit the proof of this fact.

LEMMA (1.8). *Let G be a profinite group.*

(i) *If H^l is center-free for all open subgroups H of G and all prime numbers l, then G is center-free.*

(ii) *Assume that G is torsion-free. If G admits a center-free open subgroup, then G is also center-free.*

Proof. (i) For a projective system $\{G_\lambda\}$ of profinite groups, we can easily check the equality $(\varprojlim G_\lambda)^l = \varprojlim (G_\lambda)^l$. Since any closed subgroup Z of G is the intersection of open subgroups of G, it follows that, if Z^l is nontrivial, then there exists an open subgroup H of G containing Z such that the image of Z^l in H^l is

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

nontrivial. Now let Z be the center of G. Suppose that Z is nontrivial, then Z^l is nontrivial for some prime number l, since Z is abelian. But then the image of Z^l in H^l, which is contained in the center of H^l, is nontrivial for some open subgroup H of G containing Z. This is contradictory to the assumption.

(ii) Let Z be the center of G, and H a center-free open subgroup of G. Then $Z \cap H$, contained in the center of H, is trivial. This implies Z is finite, hence trivial since G is torsion-free. □

LEMMA (1.9). *Assume $p > 0$ and $g \geqslant 2$. Let l be any prime number $\neq p$. If an integer $m \geqslant 0$ satisfies*

$$l^m > \frac{l^{2g} - l^{2g-1}}{l^{2g} - 1}(p-1)g,$$

then there exists a connected étale Galois covering Y of $\bar{X}$ with Galois group $\mathbb{Z}/l^m\mathbb{Z}$, such that the abelian variety $J_Y/\mathrm{Im}(J_{Y'})$ is ordinary, where $Y'/\bar{X}$ is the sub-covering of $Y/\bar{X}$ corresponding to the subgroup $l^{m-1}\mathbb{Z}/l^m\mathbb{Z}$ in $\mathbb{Z}/l^m\mathbb{Z}$.

In particular, for a given integer $r_0 \geqslant 0$, there exist $m \geqslant 0$ and a connected étale Galois covering Y of $\bar{X}$ with Galois group $\mathbb{Z}/l^m\mathbb{Z}$, such that the p-rank r of J_Y satisfies $r \geqslant r_0$.

Proof. The first statement is a slight modification of [Raynaud, Théorème 4.3.1], and the proof is similar. (Use the following generalization of [Raynaud, Lemme 4.3.5]:

Let k be an algebraically closed field, A an abelian variety over k of dimension $g \geqslant 2$, D an effective divisor on A, and C a proper, smooth, connected curve on A. Then, for any prime number $l \neq \mathrm{char}(k)$ and any integer $m \geqslant 0$ with $(C.D) \leqslant l^m(l^{2g}-1)/(l^{2g}-l^{2g-1})$, there exists a cyclic subgroup G of A of order l^m, such that $D \cap G \subset lG$.)

The second statement follows from the first, since the p-rank (= dimension) of $J_Y/\mathrm{Im}(J_{Y'})$ is $(l^m - l^{m-1})(g-1)$, which goes to infinity if m goes to infinity. □

LEMMA (1.10). *Assume that $\overline{\Pi}$ is not abelian* (cf. (1.4)). *Let l be a prime number $\neq p$. Let g_0 and n_0 be given integers $\geqslant 0$.*

(i) *If $2 - 2g - n < 0$* (resp. *$p > 0$, $\cdot = (\textit{unrestricted})$, and $n > 0$*), *then there exists an open normal subgroup H of $\overline{\Pi}$ with $\overline{\Pi}/H$ l-group* (resp. *p-group*), *such that $g_H \geqslant g_0$.*

(ii) *Assume $n > 0$. If $2 - 2g - n < 0$* (resp. *$p > 0$, $\cdot = (\textit{unrestricted})$, $n > 0$, and $(g, n) \neq (0, 1)$*), *then there exists an open normal subgroup H of $\overline{\Pi}$ with $\overline{\Pi}/H$ an l-group* (resp. *a p-group*), *such that $g_H \geqslant g_0$ and $n_H \geqslant n_0$. In general, there exists an open normal subgroup H of $\overline{\Pi}$ with $\overline{\Pi}/H$ an extension of a p-group by an l-group, such that $g_H \geqslant g_0$ and $n_H \geqslant n_0$.*

Proof. Easy exercise. (Use abelian or meta-abelian coverings.) □

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

PROPOSITION (1.11). *Assume that* $\overline{\Pi}$ *is not abelian* (cf. (1.4)). *Let* l *be a prime number* $\neq p$, *and assume* $\mathbb{Z}/l\mathbb{Z} \in \mathcal{C}$. *Assume, moreover,* $\mathbb{Z}/p\mathbb{Z} \in \mathcal{C}$, *if* $2-2g-n > 0$. (*This occurs only if* $p > 0$, $\cdot =$ (*unrestricted*), *and* $n > 0$.) *Then* $\overline{\Pi}^{\mathcal{C}}$ *is center-free.*

Proof. If $p = 0$ or $p > 0$ but $\mathcal{C}$ does not contain $\mathbb{Z}/p\mathbb{Z}$, this follows from (1.1) and [Nakamura 3, Corollary (1.3.4)]. (See also [Anderson], [LV].) So, we may assume $p > 0$ and that $\mathcal{C}$ contains $\mathbb{Z}/p\mathbb{Z}$. By (1.6), (1.8)(ii), and (1.10)(i), we may assume $g \geqslant 2$. Then, by (1.9), we may also assume the p-rank r of X is greater than 1. Now (1.1) implies that $\overline{\Pi}$ satisfies the condition of (1.8)(i). (Note $g_H \geqslant g$, $n_H \geqslant n$, and $r_H \geqslant r$.) This completes the proof. □

2. Characterization of decomposition groups

In this section, we treat the problem of characterizing decomposition groups in $\pi_1^{\cdot}(U, \overline{\overline{\xi}})^{(\mathcal{C})}$. A similar problem in the case of Galois groups has been related to the method concerning Brauer groups, after Neukirch. Here we take another way, using the method of Galois sections and rational points. Although the Brauer group method may be applied to the points on S, it does not seem to be applied to the points on U. On the other hand, our method is efficient only for k finite, for the present, although its formalism is stated for more general k. (See the end of this section.)

We follow the notations of Section 1, and denote $\pi_1^{\cdot}(U, \overline{\overline{\xi}})^{(\mathcal{C})}$ and $\pi_1^{\cdot}(\bar{U}, \overline{\overline{\xi}})^{\mathcal{C}}$ by Π and $\overline{\Pi}$ for simplicity. In this section, we always *assume* that the base field k is perfect and that the class $\mathcal{C}$ contains $\mathbb{Z}/l\mathbb{Z}$ for *all* prime numbers l (hence it contains all finite solvable groups).

Remark (2.1). The assumption on $\mathcal{C}$ implies that $\overline{\Pi} = \pi_1^{\cdot}(\bar{U}, \overline{\overline{\xi}})^{\mathcal{C}}$ is trivial (resp. abelian) if and only if so is $\pi_1^{\cdot}(\bar{U}, \overline{\overline{\xi}})$. See (1.1) and its corollary (1.4).

For a scheme T, denote by Σ_T the set of closed points of T. For each $\tilde{v} \in \Sigma_{\tilde{X}}$, where $\tilde{X}$ denotes the integral closure of X in $\tilde{K}$, we define the decomposition group $D_{\tilde{v}}$ and the inertia group $I_{\tilde{v}}$ by

$$D_{\tilde{v}} = \{\gamma \in \Pi \mid \gamma(\tilde{v}) = \tilde{v}\},$$

$$I_{\tilde{v}} = \{\gamma \in D_{\tilde{v}} \mid \gamma \text{ acts trivially on } \kappa(\tilde{v})\}.$$

Then we have a canonical isomorphism $D_{\tilde{v}}/I_{\tilde{v}} \simeq \mathrm{Gal}(\kappa(\tilde{v})/\kappa(v))$, where v is the image of $\tilde{v}$ in X. Observe that $\kappa(\tilde{v})$ is naturally identified with $\bar{k}$ and that $I_{\tilde{v}}$ coincides with $D_{\tilde{v}} \cap \overline{\Pi}$. If $\tilde{v}$ is on $\tilde{U}$, then we have $I_{\tilde{v}} = \{1\}$.

Let $\tilde{v}$ be a closed point of $\tilde{X}$, and define $\tilde{v}_{\mathcal{H}}$ to be the image of $\tilde{v}$ in $X_{\mathcal{H}}$ for each closed subgroup $\mathcal{H}$ of Π. Define

$$\tilde{K}_{\tilde{v}} \overset{\text{def}}{=} \bigcup_{\substack{\mathcal{H} \subset \Pi \\ \text{open}}} (K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}},$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

where $(K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}$ means the $\tilde{v}_{\mathcal{H}}$-adic completion of the field $K_{\mathcal{H}}$. Note $D_{\tilde{v}} = \mathrm{Gal}(\bar{K}_{\tilde{v}}/K_v)$, where $v \overset{\text{def}}{=} \tilde{v}_{\Pi}$. Denote by K_v^{ur} (resp. K_v^{tame}) the maximal unramified extension (resp. the maximal tamely ramified extension) of K_v in a fixed algebraic closure of $\bar{K}_{\tilde{v}}$. Then:

LEMMA (2.2). *$\tilde{K}_{\tilde{v}}$ coincides with K_v^{ur} if and only if either $\tilde{v} \in \tilde{U}$, or $\tilde{v} \notin \tilde{U}$, $\mathrm{char}(k) = 0$ or $\cdot = \mathrm{tame}$, and $(g, n) = (0, 1)$. Otherwise, i.e. if $\tilde{v} \notin \tilde{U}$ and $(g, n) \neq (0, 1)$ for $\mathrm{char}(k) = 0$ or $\cdot = \mathrm{tame}$, then*

$$\tilde{K}_{\tilde{v}} = \begin{cases} K_v^{\mathrm{tame}} = K_v^{\mathrm{sep}} = \overline{K_v} & \text{if } \mathrm{char}(k) = 0, \\ K_v^{\mathrm{tame}} & \text{if } \mathrm{char}(k) > 0 \text{ and } \cdot = \text{tame}, \\ K_v^{\mathrm{sep}} & \text{if } \mathrm{char}(k) > 0 \\ & \quad \text{and } \cdot = (\text{unrestricted}). \end{cases}$$

Proof. If $\tilde{v} \in \tilde{U}$, then we have $K_v\bar{k} \subset \tilde{K}_{\tilde{v}} \subset K_v^{\mathrm{ur}} = K_v\bar{k}$. This also holds for $\tilde{v} \notin \tilde{U}$, $\mathrm{char}(k) = 0$ or $\cdot = \mathrm{tame}$, and $(g, n) = (0, 1)$, by (1.4).

Otherwise, the inclusion $\tilde{K}_{\tilde{v}} \subset K_v^*$ is clear, where $*$ is tame $=$ sep (resp. tame, resp. sep) if $\mathrm{char}(k) = 0$ (resp. $\mathrm{char}(k) > 0$ and $\cdot = \mathrm{tame}$, resp. $\mathrm{char}(k) > 0$ and $\cdot = (\mathrm{unrestricted})$). We shall prove $K_v^* \subset \tilde{K}_{\tilde{v}}$. Note that we have $K_v^{\mathrm{ur}} = K_v\bar{k} \subset \tilde{K}_{\tilde{v}}$ at least. Since $n > 0$ and $(g, n) \neq (0, 1)$ for $\mathrm{char}(k) = 0$ or $\cdot = \mathrm{tame}$, there exists an open subgroup $\mathcal{H}$ with $n_{\mathcal{H}} \geqslant 2$ by (1.10)(ii). Since $K_v^* \subset (K_{\mathcal{H}})^*_{\tilde{v}_{\mathcal{H}}}$, we may assume $n_{\mathcal{H}} \geqslant 2$. Then, applying (1.2) to $\bar{U}$ and $\bar{U} \cup \{\tilde{v}_{\overline{\Pi}}\}$, we see $K_v^{\mathrm{tame}} \subset \tilde{K}_{\tilde{v}}$ at least. In fact, $\mathrm{Gal}(K_v^{\mathrm{tame}}/K_v^{\mathrm{ur}})$ is isomorphic to $\widehat{\mathbb{Z}}^{p'}$, and, for any exact sequence $\mathbb{Z}_l \to \mathbb{Z}_l^{\oplus m} \to \mathbb{Z}_l^{\oplus m-1} \to 0$, the left arrow $\mathbb{Z}_l \to \mathbb{Z}_l^{\oplus m}$ is injective.

Now the case where $\mathrm{char}(k) = p > 0$ and $\cdot = (\mathrm{unrestricted})$ remains. From the preceding argument, we have $K_v^{\mathrm{tame}} \subset \tilde{K}_{\tilde{v}} \subset K_v^{\mathrm{sep}}$ at least. Since $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v^{\mathrm{tame}})$ is a pro-p group, it suffices to prove that $\tilde{K}_{\tilde{v}}$ has no $\mathbb{Z}/p\mathbb{Z}$-extensions. Suppose the contrary, then $\tilde{K}_{\tilde{v}}$ has a $\mathbb{Z}/p\mathbb{Z}$-extension, which comes from a $\mathbb{Z}/p\mathbb{Z}$-extension L of $(K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}$ for some open subgroup $\mathcal{H}$. Replacing $\mathcal{H}$ by a suitable smaller subgroup if necessary, we may assume that $\sharp(S_{\mathcal{H}}) \geqslant 2$. By the Artin-Schreier theory, $L = (K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}(\alpha)$, where $\alpha^p - \alpha = a \in (K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}$. By the assumption $\sharp(S_{\mathcal{H}}) \geqslant 2$ and by Riemann-Roch theorem, $A_{\mathcal{H}} = \Gamma(U_{\mathcal{H}}, \mathcal{O}_{X_{\mathcal{H}}})$ is dense in $(K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}$, so there exists $a_0 \in A_{\mathcal{H}}$ such that $a - a_0$ belongs to the valuation ring $O_{(K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}}$ of $(K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}$. Let α_0 be a root (in K_v^{sep}) of the equation $X^p - X = a_0$, and put $\epsilon = \alpha - \alpha_0$. Observe $\epsilon^p - \epsilon = a - a_0$. Then we have

$$L = (K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}(\alpha) \subset (K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}(\alpha_0)(K_{\mathcal{H}})_{\tilde{v}_{\mathcal{H}}}(\epsilon) \subset \tilde{K}_{\tilde{v}}(K_{\mathcal{H}})^{\mathrm{ur}}_{\tilde{v}_{\mathcal{H}}} = \tilde{K}_{\tilde{v}},$$

which is absurd since $L\tilde{K}_{\tilde{v}}/\tilde{K}_{\tilde{v}}$ is a $\mathbb{Z}/p\mathbb{Z}$-extension. □

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Next, we fix some notations about Galois sections. Recall that we have the following exact sequence (1-2):

$$1 \to \overline{\Pi} \to \Pi \stackrel{\mathrm{pr}}{\to} G_k \to 1.$$

DEFINITION (2.3). Let G be an open subgroup of G_k, and denote by ι the natural inclusion $G \to G_k$. Let $\mathcal{H}$ be an open subgroup of Π.

(i) We define

$$\mathcal{S}(G) \stackrel{\mathrm{def}}{=} \{s \in \mathrm{Hom}_{\mathrm{cont}}(G, \Pi) \mid \mathrm{pr} \circ s = \iota\},$$

and

$$\mathcal{S}_{\mathcal{H}}(G) \stackrel{\mathrm{def}}{=} \{s \in \mathcal{S}(G) \mid s(G) \subset \mathcal{H}\}.$$

(Note that $\mathcal{S}_{\mathcal{H}}(G)$ is empty unless $\mathrm{pr}(\mathcal{H})$ contains G.) We refer an element of $\mathcal{S}(G)$ as *section*.

(ii) We say that a section $s \in \mathcal{S}_{\mathcal{H}}(G)$ is *geometric*, if its image $s(G)$ is contained in $D_{\tilde{v}}$ for some $\tilde{v} \in \Sigma_{\tilde{X}}$, and denote by $\mathcal{S}_{\mathcal{H}}(G)^{\mathrm{geom}}$ the set of geometric sections in $\mathcal{S}_{\mathcal{H}}(G)$. We write $\mathcal{S}(G)^{\mathrm{geom}}$ instead of $\mathcal{S}_{\Pi}(G)^{\mathrm{geom}}$.

(iii) We define

$$\mathcal{Q}_{\mathcal{H}} \stackrel{\mathrm{def}}{=} \varinjlim_{G \subset G_k : \mathrm{open}} \mathcal{S}_{\mathcal{H}}(G),$$

and write $\mathcal{Q}$ instead of $\mathcal{Q}_{\Pi}$. We refer an element of $\mathcal{Q}$ as *quasi-section*. We define the set $\mathcal{Q}_{\mathcal{H}}^{\mathrm{geom}}$ of *geometric quasi-sections* by

$$\mathcal{Q}_{\mathcal{H}}^{\mathrm{geom}} \stackrel{\mathrm{def}}{=} \varinjlim_{G \subset G_k : \mathrm{open}} \mathcal{S}_{\mathcal{H}}(G)^{\mathrm{geom}},$$

and write $\mathcal{Q}^{\mathrm{geom}}$ instead of $\mathcal{Q}_{\Pi}^{\mathrm{geom}}$.

Remark (2.4). (i) The natural map $\mathcal{Q}_{\mathcal{H}} \to \mathcal{Q}$ is bijective, since $\mathcal{H}$ is an open subgroup of Π. If we identify $\mathcal{Q}_{\mathcal{H}}$ with $\mathcal{Q}$ by this bijection, $\mathcal{Q}_{\mathcal{H}}^{\mathrm{geom}}$ is identified with $\mathcal{Q}^{\mathrm{geom}}$.

(ii) Since any section s: $G \to \Pi$ is determined by its image $s(G)$, we can identify $\mathcal{S}(G)$ with the set of closed subgroups of Π which are isomorphically mapped onto G by pr. Thus the conjugation of $\gamma \in \Pi$ defines a bijection $\mathcal{S}(G) \simeq \mathcal{S}(\gamma(G))$, where $\gamma(G) = \mathrm{pr}(\gamma) G \mathrm{pr}(\gamma)^{-1}$, which maps $\mathcal{S}(G)^{\mathrm{geom}}$ onto $\mathcal{S}(\gamma(G))^{\mathrm{geom}}$. This bijection induces a bijection $\mathcal{S}_{\mathcal{H}}(G) \simeq \mathcal{S}_{\gamma(\mathcal{H})}(\gamma(G))$, where $\gamma(\mathcal{H}) = \gamma \mathcal{H} \gamma^{-1}$,

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

which maps $\mathcal{S}_{\mathcal{H}}(G)^{\text{geom}}$ onto $\mathcal{S}_{\gamma(\mathcal{H})}(\gamma(G))^{\text{geom}}$. Taking the inductive limit, Π acts on $\mathcal{Q}$ and $\mathcal{Q}^{\text{geom}}$.

Next, we shall define important maps from the sets of pairs of Galois sections to certain cohomology groups.

Let $\mathcal{H}$ be an open subgroup of Π. We define a closed subgroup $I(\mathcal{H})$ of $\mathcal{H}$ to be the kernel of

$$\mathcal{H} = \pi_1(U_{\mathcal{H}}, \bar{\bar{\xi}})^{(\mathcal{C})} \to \pi_1(X_{\mathcal{H}}, \bar{\bar{\xi}})^{(\mathcal{C})},$$

which coincides with the kernel of

$$\bar{\mathcal{H}} = \pi_1(\overline{U_{\mathcal{H}}}, \bar{\bar{\xi}})^{\mathcal{C}} \to \pi_1(\overline{X_{\mathcal{H}}}, \bar{\bar{\xi}})^{\mathcal{C}}.$$

By definition, we have

$$\mathcal{H}/I(\mathcal{H}) = \pi_1(X_{\mathcal{H}}, \bar{\bar{\xi}})^{(\mathcal{C})}, \bar{\mathcal{H}}/I(\mathcal{H}) = \pi_1(\overline{X_{\mathcal{H}}}, \bar{\bar{\xi}})^{\mathcal{C}},$$

and

$$(\bar{\mathcal{H}}/I(\mathcal{H}))^{\text{ab}} = \pi_1(\overline{X_{\mathcal{H}}}, \bar{\bar{\xi}})^{\text{ab}} = T(J_{X_{\mathcal{H}}}).$$

(Recall that $\mathcal{C}$ contains all finite abelian groups.) Observe that $(\bar{\mathcal{H}}/I(\mathcal{H}))^{\text{ab}} = T(J_{X_{\mathcal{H}}})$ becomes a $G_{k_{\mathcal{H}}}(= \text{pr}(\mathcal{H}))$-module.

DEFINITION (2.5). (i) For each open subgroup G of $G_{k_{\mathcal{H}}}$, define the map

$$j_{\mathcal{H}}(G)\colon \mathcal{S}_{\mathcal{H}}(G) \times \mathcal{S}_{\mathcal{H}}(G) \to H^1_{\text{cont}}(G, T(J_{X_{\mathcal{H}}})) \overset{\text{def}}{=} \varprojlim_m H^1(G, T(J_{X_{\mathcal{H}}})/mT(J_{X_{\mathcal{H}}}))$$

to send a pair $(s_1, s_2) \in \mathcal{S}_{\mathcal{H}}(G) \times \mathcal{S}_{\mathcal{H}}(G)$ to the cohomology class of the (continuous) 1-cocycle: $G \to (\bar{\mathcal{H}}/I(\mathcal{H}))^{\text{ab}} = T(J_{X_{\mathcal{H}}})$, $\sigma \mapsto$ the image of $s_1(\sigma)s_2(\sigma)^{-1}$.

(ii) Define

$$j_{\mathcal{H}}\colon \mathcal{Q}_{\mathcal{H}} \times \mathcal{Q}_{\mathcal{H}} \to \varinjlim_{G \subset G_{k_{\mathcal{H}}}\text{: open}} H^1_{\text{cont}}(G, T(J_{X_{\mathcal{H}}}))$$

as $\varinjlim j_{\mathcal{H}}(G)$. (Note that we define $j_{\mathcal{H}}(G)$ only when G is contained in $G_{k_{\mathcal{H}}}$. However, $\mathcal{S}_{\mathcal{H}}(G)$ is empty, otherwise.)

LEMMA (2.6). *Let s_i be an element of $\mathcal{S}_{\mathcal{H}}(G)^{\text{geom}}$ for $i = 1, 2$, and take $\tilde{v}_i \in \Sigma_{\tilde{X}}$ satisfying $s_i(G) \subset D_{\tilde{v}_i}$. Denote by v_i the image of $\tilde{v}_i$ in $X_{\mathcal{H}\cap \text{pr}^{-1}(G)} = X_{\mathcal{H}} \otimes_{k_{\mathcal{H}}} L$, where $L = \bar{k}^G$.*

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Then v_i is a L-rational point for $i = 1, 2$, and $j_{\mathcal{H}}(G)(s_1, s_2)$ coincides with the image of the divisor $v_1 - v_2$ of degree 0 on $X_{\mathcal{H}} \otimes_{k_{\mathcal{H}}} L$ by

$$\mathrm{Div}^0\left(X_{\mathcal{H}} \bigotimes_{k_{\mathcal{H}}} L\right) \to J_{X_{\mathcal{H}}}(L) \to \varprojlim J_{X_{\mathcal{H}}}(L)/mJ_{X_{\mathcal{H}}}(L)$$
$$\overset{\text{Kummer sequence}}{\longrightarrow} H^1_{\mathrm{cont}}(G, T(J_{X_{\mathcal{H}}})).$$

Proof. Since $D_{\tilde{v}_i} \cap \mathcal{H}$ contains $s_i(G)$, its image $\mathrm{pr}(D_{\tilde{v}_i} \cap \mathcal{H})$ in G_k contains G, which also implies that $\mathrm{pr}(D_{\tilde{v}_i} \cap \mathcal{H} \cap \mathrm{pr}^{-1}(G))$ coincides with G. This means v_i is L-rational.

As for the second statement, see [NT, Lemma (4.14)], [Nakamura2, 2.2. Claim]. □

Recall (2.4)(i) that $\mathcal{Q}_{\mathcal{H}}$ is naturally identified with $\mathcal{Q}$.

DEFINITION (2.7). Let s_i be an element of $\mathcal{Q}$ for $i = 1, 2$.

(i) Let $\mathcal{H}$ be an open subgroup of Π. Then we define:

$$s_1 \underset{\mathcal{H}}{\sim} s_2 \overset{\text{def}}{\Longleftrightarrow} j_{\mathcal{H}}(s_1, s_2) = 0.$$

(ii) We define

$$s_1 \sim s_2 \overset{\text{def}}{\Longleftrightarrow} s_1 \underset{\mathcal{H}}{\sim} s_2 \quad \text{for all open subgroups } \mathcal{H} \text{ in } \Pi.$$

(Observe that $\underset{\mathcal{H}}{\sim}$ and $\sim$ are equivalence relations on $\mathcal{Q}$.)

Our approach to the problem of characterizing decomposition groups depends on properties of the base field k. Consider the following conditions for the (perfect) field k:

(A_k) For any abelian variety A over k, we have

$$\bigcap_{m \geqslant 1} mA(k) = \{0\}.$$

(B_k) The profinite group $\mathrm{Gal}(k((T))^{\mathrm{sep}}/k((T)))$ is topologically generated by (the images of) continuous group-theoretical sections of the surjective homomorphism

$$\mathrm{Gal}(k((T))^{\mathrm{sep}}/k((T))) \to \mathrm{Gal}(\bar{k} \cdot k((T))/k((T))) = G_k.$$

(C_k) (resp. (C'_k)) k admits a structure of Hausdorff topological field, so that $Y(k)$ becomes compact for any proper, smooth, geometrically connected curve Y (resp. proper, smooth, geometrically connected curve Y of genus $\geqslant 2$) over k.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

We define the conditions (A), (B), (C) and (C′) for the field k by:

$$(\cdot) \iff (\cdot_L) \quad \text{for any finite extension } L \text{ over } k.$$

Examples of fields satisfying (A) are: finite fields, fields finitely generated over $\mathbb{Q}$, and p-adic local fields, i.e. finite extensions of $\mathbb{Q}_p$. When $\mathrm{char}(k) = 0$, the condition (B_k) holds if and only if $k^\times/k^{\times m} \neq 1$ for all natural numbers $m > 1$. In particular, fields of characteristic 0 admitting a discrete valuation (e.g. fields finitely generated over $\mathbb{Q}$ and p-adic local fields) satisfy (B). Other cases where (B) holds are when G_k is a free profinite group of rank > 0. In particular, finite fields satisfy (B). Examples of fields satisfying (C) are finite fields (for discrete topology) and p-adic local fields (for p-adic topology). Examples of fields satisfying (C′) are fields finitely generated over $\mathbb{Q}$ (for discrete topology). (Mordell conjecture! ([Faltings], [FW]))

The following is a key proposition of our method of characterizing decomposition groups.

PROPOSITION (2.8). (i) *Assume that k satisfies* (A). *Assume $(g, n) \neq (0, 0)$, and assume also $(g, n) \neq (0, 1), (0, 2)$ when either* $\mathrm{char}(k) = 0$ *or* $\cdot =$ tame. *Let $\tilde{v}$ be a closed point of $\tilde{X}$, and $H_{\tilde{v}}$ a closed subgroup of $D_{\tilde{v}}$ whose image in $D_{\tilde{v}}/I_{\tilde{v}}$ is open. Then, for each closed point $\tilde{v}' \neq \tilde{v}$ of $\tilde{X}$, $D_{\tilde{v}'}$ does not contain $H_{\tilde{v}}$. In particular, $D_{\tilde{v}'}$ does not contain $D_{\tilde{v}}$.*

Moreover, the map $\Sigma_{\tilde{X}} \to \{$ closed subgroups of $\Pi\}$, $\tilde{v} \mapsto D_{\tilde{v}}$ is injective.

(ii) *Put the same assumptions as in* (i). *Then, for each open subgroup G of G_k, there exists a unique map $\varphi(G)$: $\mathcal{S}(G)^{\mathrm{geom}} \to \Sigma_{\tilde{X}}$ satisfying $s(G) \subset D_{\varphi(G)(s)}$ for each $s \in \mathcal{S}(G)$. Taking the inductive limit of $\varphi(G)$, we obtain*

$$\varphi\colon \mathcal{Q}^{\mathrm{geom}} \to \Sigma_{\tilde{X}},$$

which is compatible with the actions of Π.

The map φ induces a bijection $\bar{\varphi}$: $(\mathcal{Q}^{\mathrm{geom}}/\sim) \to \Sigma_{\tilde{X}}$, which induces a bijection $\bar{\varphi}_{\mathcal{H}}\colon \mathcal{H}\backslash(\mathcal{Q}^{\mathrm{geom}}/\sim) \to \mathcal{H}\backslash\Sigma_{\tilde{X}} = \Sigma_{X_{\mathcal{H}}}$ for each closed subgroup $\mathcal{H}$ of Π:

$$\begin{array}{ccc}
\mathcal{Q}^{\mathrm{geom}} & \xrightarrow{\varphi} & \Sigma_{\tilde{X}} \\
\downarrow & & \| \\
\mathcal{Q}^{\mathrm{geom}}/\sim & \xrightarrow{\bar{\varphi}} & \Sigma_{\tilde{X}} \\
\downarrow & & \downarrow \\
\mathcal{H}\backslash(\mathcal{Q}^{\mathrm{geom}}/\sim) & \xrightarrow{\bar{\varphi}_{\mathcal{H}}} & \mathcal{H}\backslash\Sigma_{\tilde{X}} \\
 & & \| \\
 & & \Sigma_{X_{\mathcal{H}}}.
\end{array}$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

When $\mathcal{H}$ is open and $g_{\mathcal{H}} > 0$, φ also induces a bijection

$$\varphi_{\mathcal{H}}\colon (\mathcal{Q}^{\mathrm{geom}}/\underset{\mathcal{H}}{\sim}) \to \Sigma_{X_{\bar{\mathcal{H}}}} = X_{\mathcal{H}}(\bar{k}) \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\mathrm{Spec}(k_{\mathcal{H}})}(\mathrm{Spec}(\bar{k}), X_{\mathcal{H}}),$$

which is compatible with the actions of $\mathrm{pr}(\mathcal{H}) = \mathcal{H}/\bar{\mathcal{H}}$.

(iii) *Put the same assumptions as in* (i)*, and further assume that k satisfies* (B). *Let* **s** *be an element of $\mathcal{Q}^{\mathrm{geom}}/\sim$. Then $D_{\bar{\varphi}(\mathbf{s})}$ is the closed subgroup (topologically) generated by $s(G)$ for all open subgroups G of G_k and all $s \in \mathcal{S}(G)^{\mathrm{geom}}$ with $s \bmod \sim = \mathbf{s}$. The open subgroup $G_{\mathbf{s}} \stackrel{\mathrm{def}}{=} \mathrm{pr}(D_{\bar{\varphi}(\mathbf{s})})$ is characterized as the maximal open subgroup G of G_k with $\{s \in \mathcal{S}(G)^{\mathrm{geom}} \mid s \bmod \sim = \mathbf{s}\} \neq \emptyset$, and $D_{\bar{\varphi}(\mathbf{s})}$ is characterized also as the closed subgroup (topologically) generated by $s(G_{\mathbf{s}})$ for all $s \in \mathcal{S}(G_{\mathbf{s}})^{\mathrm{geom}}$ with $s \bmod \sim = \mathbf{s}$.*

Moreover, $\bar{\varphi}(\mathbf{s}) \in \tilde{\mathrm{U}}$ if and only if $\{s \in \mathcal{S}(G_{\mathbf{s}})^{\mathrm{geom}} \mid s \bmod \sim = \mathbf{s}\}$ is a one-element set. If this is the case, the unique element s of this set satisfies $D_{\bar{\varphi}(\mathbf{s})} = s(G_{\mathbf{s}})$.

(iv) *Assume either that k satisfies* (C) *or that k satisfies* (C′) *and $\overline{\Pi}$ is not abelian.* (*cf.* (1.4) *and* (2.1).) *Let G be an open subgroup of G_k, and put $L = \bar{k}^G$. Let s be an element of $\mathcal{S}(G)$. Then s belongs to $\mathcal{S}(G)^{\mathrm{geom}}$ if and only if $X_{\mathcal{H}}(L) \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\mathrm{Spec}(k_{\mathcal{H}})}(\mathrm{Spec}(L), X_{\mathcal{H}})$ is non-empty for all open subgroup $\mathcal{H}$ of Π containing $s(G)$.*

Proof. First note that, for each closed subgroup $\mathcal{K}$ of Π and each sub-extension M/k in $\bar{k}/k$, we have:

$$\Sigma_{X_{\mathcal{K}}} = \varprojlim_{\substack{\mathcal{K} \subset \mathcal{H} \subset \Pi \\ \text{open}}} \Sigma_{X_{\mathcal{H}}},$$

and

$$X_{\mathcal{K}}(M) = \varprojlim_{\substack{\mathcal{K} \subset \mathcal{H} \subset \Pi \\ \text{open}}} X_{\mathcal{H}}(M).$$

Denote the image of $v \in \Sigma_{X_{\mathcal{K}}}$ (resp. $P \in X_{\mathcal{K}}(M)$) in $\Sigma_{X_{\mathcal{H}}}$ (resp. $X_{\mathcal{H}}(M)$) by $v_{\mathcal{H}}$ (resp. $P_{\mathcal{H}}$).

(i) The assumption on (g, n) means that there exists an open subgroup $\mathcal{H}_0$ of Π with $g_{\mathcal{H}_0} > 0$. Since $\tilde{v}' \neq \tilde{v}$, there exists an open subgroup $\mathcal{H}$ of Π with $\tilde{v}'_{\mathcal{H}} \neq \tilde{v}_{\mathcal{H}}$. Taking the intersection with $\mathcal{H}_0$ if necessary, we may assume $g_{\mathcal{H}} > 0$. Moreover, we may assume that $\mathrm{pr}(H_{\tilde{v}} \cap \mathcal{H}) = \mathrm{pr}(D_{\tilde{v}'} \cap \mathcal{H}) = \mathrm{pr}(\mathcal{H})$. In fact, put $G = \mathrm{pr}(H_{\tilde{v}} \cap \mathcal{H}) \cap \mathrm{pr}(D_{\tilde{v}'} \cap \mathcal{H})$, which is an open subgroup of G_k, and replace $\mathcal{H}$ by $\mathcal{H} \cap \mathrm{pr}^{-1}(G)$.

Now, suppose $H_{\tilde{v}} \subset D_{\tilde{v}'}$, hence $H_{\tilde{v}} \cap \mathcal{H} \subset D_{\tilde{v}'} \cap \mathcal{H}$. Then the image of $H_{\tilde{v}} \cap \mathcal{H}$ in $\mathcal{H}/I(\mathcal{H})$ coincides with that of $D_{\tilde{v}'} \cap \mathcal{H}$. In fact, these are injectively mapped

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

into G_k by pr, and both of their (injective) images coincides with $\mathrm{pr}(\mathcal{H})$. These images are identified with sections s and s' of $\mathcal{H}/I(\mathcal{H}) \twoheadrightarrow \mathrm{pr}(\mathcal{H})$. Applying (2.6) to $X_{\mathcal{H}}$, we see that $\tilde{v}_{\mathcal{H}} = \tilde{v}'_{\mathcal{H}}$, since $g_{\mathcal{H}} > 0$ and k satisfies (A). This is absurd.

Putting $H_{\tilde{v}} = D_{\tilde{v}}$, we get the second statement. The third statement follows from the second.

(ii) By definition, for each $s \in \mathcal{S}(G)^{\mathrm{geom}}$, there exists a $\tilde{v} \in \Sigma_{\tilde{X}}$ with $D_{\tilde{v}} \supset s(G)$. By (i), such $\tilde{v}$ is unique. This shows the existence and uniqueness of $\varphi(G)$. Since $\varphi(G)$ is compatible with the restriction of the open subgroup G of G_k, we can define φ as

$$\varinjlim_{G \subset G_k : \text{open}} \varphi(G),$$

which is compatible with the Π-actions by definitions.

First we prove that φ is surjective. Take any $\tilde{v} \in \Sigma_{\tilde{X}}$ and put $v = \tilde{v}_{\Pi}$. Put $G = \mathrm{pr}(D_{\tilde{v}})$, which is identified with $D_{\tilde{v}}/I_{\tilde{v}} = \mathrm{Gal}(\bar{k}/\kappa(v))$. Now it suffices to show that the surjection $D_{\tilde{v}} \to G$ admits a (continuous group-theoretical) section. Since $D_{\tilde{v}}$ is a quotient of the absolute Galois group of the fractional field of the completion of $\mathcal{O}_{X,v}$, the following lemma settles the problem.

LEMMA (2.9). *Let K be the fractional field of a henselian discrete valuation ring, and I_K the inertia group in the absolute Galois group G_K of K. Then the surjection $G_K \to G_K/I_K$ admits a continuous group-theoretical section.*

Proof. Let p be the characteristic of the residue field of the henselian valuation. Let P_K be the p-Sylow subgroup of I_K if $p > 0$, and $\{1\}$ if $p = 0$. Choosing a compatible system of power roots of a prime element, we can construct a section of $G_K/P_K \to G_K/I_K$. On the other hand, $G_K \to G_K/P_K$ admits a section by [KPR]. Composing them, we obtain a section of $G_K \to G_K/I_K$. □

Next, let $\mathcal{H}$ be an open subgroup of Π, and G a closed subgroup of G_k. Let s_1 and s_2 be elements of $\mathcal{S}_{\mathcal{H}}(G)^{\mathrm{geom}}$, which define elements of $\mathcal{Q} = \mathcal{Q}_{\mathcal{H}}$. Then, by (2.6), $\varphi(s_i)_{\mathcal{H}\cap \mathrm{pr}^{-1}(G)}$ is an L-rational point of $X_{\mathcal{H}\cap \mathrm{pr}^{-1}(G)} = X_{\mathcal{H}} \otimes_{k_{\mathcal{H}}} L$ for each $i = 1, 2$, where $L = \bar{k}^G$. Since $J_{X_{\mathcal{H}}}(L) \to J_{X_{\mathcal{H}}}(L')$ is injective for each finite subextension L'/L of $\bar{k}/L$, $j_{\mathcal{H}}(s_1, s_2) = 0$ is equivalent to $j_{\mathcal{H}}(G)(s_1, s_2) = 0$, and, moreover, this occurs if and only if either $g_{\mathcal{H}} = 0$ or $g_{\mathcal{H}} > 0$ and $\varphi(s_1)_{\mathcal{H}\cap \mathrm{pr}^{-1}(G)} = \varphi(s_2)_{\mathcal{H}\cap \mathrm{pr}^{-1}(G)}$. (Use (2.6).) Since $X_{\mathcal{H}}(L) \to X_{\mathcal{H}}(\bar{k})$ is injective, we have:

$$s_1 \underset{\mathcal{H}}{\sim} s_2 \iff \text{either } g_{\mathcal{H}} = 0 \text{ or } g_{\mathcal{H}} > 0, \varphi(s_1)_{\bar{\mathcal{H}}} = \varphi(s_2)_{\bar{\mathcal{H}}}.$$

Thus we obtain the bijection $\varphi_{\mathcal{H}}\colon (\mathcal{Q}^{\mathrm{geom}}/\underset{\mathcal{H}}{\sim}) \to \Sigma_{X_{\bar{\mathcal{H}}}}$ if $g_{\mathcal{H}} > 0$, and the bijection $\bar{\varphi}\colon (\mathcal{Q}^{\mathrm{geom}}/\sim) \to \Sigma_{\tilde{X}}$. (For the latter, note that for each open subgroup $\mathcal{H}$ of Π there exists an open subgroup $\mathcal{H}'$ of $\mathcal{H}$ with $g_{\mathcal{H}'} > 0$, by our assumption.) By definition, φ is compatible with the Π-actions, hence so is the bijection $\bar{\varphi}$. Therefore

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

$\bar{\varphi}$ induces the bijection $\bar{\varphi}_{\mathcal{H}}$ for any closed subgroup $\mathcal{H}$ of Π. Since φ is compatible with the $\mathcal{H}$-actions for each open subgroup $\mathcal{H}$ of Π, $\varphi_{\mathcal{H}}$ is also compatible with the $\mathcal{H}$-actions.

(iii) For $s \in \mathcal{S}(G)^{\text{geom}}$, $s \bmod \sim = \mathbf{s} \Longleftrightarrow \varphi(s) = \bar{\varphi}(\mathbf{s}) \Longleftrightarrow s(G) \subset D_{\bar{\varphi}(\mathbf{s})}$, by (ii). From this and the condition (B), all the statements are clear, except for the statements on $\tilde{U}$. Note that we exclude $(g, n) = (0, 0)$ and $(g, n) = (0, 1)$ for $\text{char}(k) = 0$ or $\cdot =$ tame. Hence, by (2.2), $\tilde{v} \in \Sigma_{\tilde{X}}$ belongs to $\tilde{U}$ if and only if $I_{\tilde{v}} = \{1\}$, or, equivalently, $D_{\tilde{v}} \overset{\text{pr}}{\to} G_k$ is injective. Since $D_{\bar{\varphi}(\mathbf{s})}$ is generated by $s(G_{\mathbf{s}})$ for $s \in \mathcal{S}(G_{\mathbf{s}})^{\text{geom}}$ with $s \bmod \sim = \mathbf{s}$, $\bar{\varphi}(\mathbf{s})$ belongs to $\tilde{U}$ if and only if $\{s \in \mathcal{S}(G_{\mathbf{s}})^{\text{geom}} \mid s \bmod \sim = \mathbf{s}\}$ is a one-element set. The last statement is clear.

(iv) First assume $s \in \mathcal{S}(G)^{\text{geom}}$, and let $\mathcal{H}$ be any open subgroup of Π containing $s(G)$. Put $\tilde{v} = \varphi(s)$. Then $\text{Gal}(\bar{k}/\kappa(\tilde{v}_{\mathcal{H}})) \subset G_k$ coincides with $\text{pr}(D_{\tilde{v}} \cap \mathcal{H})$, which contains $\text{pr}(s(G)) = G$. Hence L contains $\kappa(\tilde{v}_{\mathcal{H}})$ (in $\bar{k}$). In particular, $X_{\mathcal{H}}(L)$ is non-empty.

Next, let s be an element of $\mathcal{S}(G)$, and assume $X_{\mathcal{H}}(L) \neq \emptyset$ for all open subgroups $\mathcal{H}$ of Π containing $s(G)$. Since

$$X_{s(G)}(L) = \varprojlim_{\substack{s(G) \subset \mathcal{H} \subset \Pi \\ \text{open}}} X_{\mathcal{H}}(L),$$

$X_{s(G)}(L)$ is also non-empty by the condition (C) and Tikhonov's theorem. Here, when we assume that $\overline{\Pi}$ is not abelian, observe that there exists an $\mathcal{H}$ containing $s(G)$ with $g_{\mathcal{H}} \geqslant 2$. In fact, there exists an open subgroup H of $\overline{\Pi}$ with $g_H \geqslant 2$ by (1.10), and since

$$\bigcap_{\substack{s(G) \subset \mathcal{H} \subset \Pi \\ \text{open}}} (\mathcal{H} \cap \overline{\Pi}) = s(G) \cap \overline{\Pi} = \{1\} \subset H,$$

the compactness argument assures the existence of $\mathcal{H}$ with $\mathcal{H} \cap \overline{\Pi} \subset H$. Then $g_{\mathcal{H}} \geqslant g_H \geqslant 2$.

Take any L-rational point P of $X_{s(G)}$. (Note $k_{s(G)} = \bar{k}^{\text{pr}(s(G))} = \bar{k}^G = L$.) Define $v \in \Sigma_{X_{s(G)}}$ to be the image of P, and choose any $\tilde{v} \in \Sigma_{\tilde{X}}$ above v. As v is L-rational, $\text{pr}(D_{\tilde{v}} \cap s(G)) = G = \text{pr}(s(G))$. Since $s(G) \overset{\text{pr}}{\to} G_k$ is injective, this implies $D_{\tilde{v}} \cap s(G) = s(G)$, i.e. $s(G) \subset D_{\tilde{v}}$. In particular, $s \in \mathcal{S}(G)^{\text{geom}}$. □

COROLLARY (2.10). (Summary of (2.8).) *Assume either* (a)*: k satisfies* (A), (B), (C) (*e.g. k: a finite field or a p-adic local field*), $(g, n) \neq (0, 0)$, *and* $(g, n) \neq (0, 1), (0, 2)$ *if* $\text{char}(k) = 0$ *or* $\cdot =$ tame*; or* (b) *k satisfies* (A), (B), (C′) (*e.g. k: finitely generated over $\mathbb{Q}$*), *and* $\overline{\Pi}$ *is not abelian. Then the map* $\Sigma_{\tilde{X}} \to \{$*closed*

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

subgroups of $\Pi\}$, $\tilde{v} \mapsto D_{\tilde{v}}$ *is injective. There exists a* Π*-equivariant bijection* $\bar{\varphi}\colon (\mathcal{Q}^{\mathrm{geom}}/\sim) \to \Sigma_{\tilde{X}}$, *which is characterized by:*

$$D_{\bar{\varphi}(\mathbf{s})} = \langle s(G) \mid G \subset G_k\text{: open}, s \in \mathcal{S}(G)^{\mathrm{geom}}, s \bmod \sim = \mathbf{s}\rangle.$$

Moreover, for each open subgroup G *of* G_k, *the subset* $\mathcal{S}(G)^{\mathrm{geom}}$ *in* $\mathcal{S}(G)$ *is characterized by:*

$$s \in \mathcal{S}(G)^{\mathrm{geom}} \iff X_{\mathcal{H}}(L) \neq \emptyset \quad \text{for all open subgroups } \mathcal{H} \text{ of } \Pi \text{ containing } s(G),$$

where $L = \bar{k}^G$. □

Remark (2.11). Put the same assumptions as in (2.8)(i). Let $G' \subset G$ be open subgroups of G_k. If $s \in \mathcal{S}(G)$ satisfies $s(G') \subset D_{\tilde{v}}$ for some $\tilde{v} \in \Sigma_{\tilde{X}}$, then $s(G) \subset D_{\tilde{v}}$. Moreover, the inverse image of $\mathcal{Q}^{\mathrm{geom}}$ by $\mathcal{S}(G) \to \mathcal{Q}$ coincides with $\mathcal{S}(G)^{\mathrm{geom}}$.

In fact, we may assume that G' is normal in G, shrinking G' if necessary. Then, for each $\tau \in G$, $s(G') = s(\tau)s(G')s(\tau)^{-1}$ is contained in both $D_{\tilde{v}}$ and $s(\tau)D_{\tilde{v}}s(\tau)^{-1} = D_{s(\tau)\tilde{v}}$. By (2.8)(i), this implies $\tilde{v} = s(\tau)\tilde{v}$, i.e. $s(\tau) \in D_{\tilde{v}}$. The second statement directly follows from the first.

Assuming the conditions (A), (B), and (C) (or (C′)) for the field k and the minor conditions on (g, n), what remain for our group-theoretical characterization of the decomposition groups in $\Pi = \pi_1(U, \overline{\overline{\xi}})^{(\mathcal{C})}$?

First, we exploited the exact sequence

$$1 \to \overline{\Pi} \to \Pi \xrightarrow{\mathrm{pr}} G_k \to 1.$$

So, we have to characterize $\overline{\Pi}$ in Π or to start from $\Pi \xrightarrow{\mathrm{pr}} G_k$.

Second, to define the equivalence relation $\underset{\mathcal{H}}{\sim}$ for each open subgroup $\mathcal{H}$ of Π, we used the closed subgroup $I(\mathcal{H})$ of $\bar{\mathcal{H}}$. So, we have to characterize $I(\mathcal{H})$ for each such $\mathcal{H}$. (Of course, this problem is trivial if $n = 0$.)

Third, to characterize the subset $\mathcal{S}(G)^{\mathrm{geom}}$ in $\mathcal{S}(G)$ for each open subgroup G of G_k, we have to detect whether $X_{\mathcal{H}}(L)$ is empty or not for each open subgroup $\mathcal{H}$ of Π, where $L = \bar{k}^G$.

The first and the second problems are settled for k finite or k finitely generated over $\mathbb{Q}$. However, the third problem is most essential and still open for k finitely generated over $\mathbb{Q}$ (unless we use the Grothendieck conjecture over such k, of course.)

Remark (2.12). For k finitely generated, we might conjecture $\mathcal{S}(G) = \mathcal{S}(G)^{\mathrm{geom}}$.

Anyway, these three problems are main topics of the next section.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

3. Characterization of various invariants

We follow the notations of Sections 1 and 2. The aim of this section is to describe various invariants of the curve U in terms of the profinite group $\Pi = \pi_1^{\cdot}(U, \overline{\overline{\xi}})^{(\mathcal{C})}$. We *assume* that the class $\mathcal{C}$ contains $\mathbb{Z}/l\mathbb{Z}$ for all prime numbers l as in Section 2, and also *assume* that $\overline{\Pi} = \pi_1^{\cdot}(\bar{U}, \overline{\overline{\xi}})^{\mathcal{C}}$ is not trivial, i.e. *exclude* $(g, n) = (0, 0)$, and also (0,1) if $\mathrm{char}(k) = 0$ or $\cdot =$ tame. (cf. (1.4) and (2.1).) We mainly consider the case where k is finite and the case where k is finitely generated over $\mathbb{Q}$.

1. $\overline{\Pi}$ and $p = \mathrm{char}(k)$.

By our assumption that $\overline{\Pi}$ is not trivial and by (1.2), $p = \mathrm{char}(k)$ is recovered by $\overline{\Pi}$ as follows:

PROPOSITION (3.1). *If* $\overline{\Pi}^{\mathrm{ab}}$ *is free as a* $\widehat{\mathbb{Z}}$*-module, then* $\mathrm{char}(k)$ *is* 0. *Otherwise,* $\mathrm{char}(k)$ *is positive, and is the unique prime number* p *such that* $(\overline{\Pi}^{\mathrm{ab}})^{p'}$ *is free as a* $\widehat{\mathbb{Z}}^{p'}$*-module.* □

As is well-known (cf. [Nakamura 3, Lemma (1.6.2)], [Pop 2, Introduction]), when k is a field finitely generated over $\mathbb{Q}$, we can recover $\overline{\Pi}$ from Π as follows:

PROPOSITION (3.2). *Assume that* k *is a field finitely generated over* $\mathbb{Q}$. *Then* $\overline{\Pi}$ *is the maximal closed normal subgroup of* Π *which is* (*topologically*) *finitely generated.*

Proof. Immediate from [FJ, Theorem 15.10]. □

On the other hand, when k is finite, G_k is isomorphic to $\widehat{\mathbb{Z}}$, hence, in particular, is finitely generated. (Moreover, if $n > 0$ and $\cdot =$ (unrestricted), $\overline{\Pi}$ is not finitely generated. See (1.1).) So the preceding characterization of $\overline{\Pi}$ fails in this case. However, we have the following:

PROPOSITION (3.3). *Assume that* k *is a finite field.*

(i) *The following are all equivalent:*

(a) *either* $n = 0$ *or* $\cdot =$ *tame;*
(b) Π *is finitely generated;*
(b′) Π^{ab} *is finitely generated;*
(c) Π^p *is finitely generated;*
(c′) $(\Pi^{\mathrm{ab}})^p$ *is finitely generated.*

(*Note that the conditions* (b) *and* (b′) *do not involve* $p = \mathrm{char}(k)$.)

(ii) *If* $n = 0$ *or* $\cdot =$ *tame, then*

$$\overline{\Pi} = \mathrm{Ker}(\Pi \to \Pi^{\mathrm{ab}}/(\Pi^{\mathrm{ab}})_{\mathrm{tors}}).$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

(iii) *If* $n > 0$ *and* $\cdot = (\textit{unrestricted})$, *then* $\mathrm{char}(k)$ *is the unique prime number* p *such that* $(\Pi^{\mathrm{ab}})^p$ *is not finitely generated as a* $\mathbb{Z}_p$*-module.*

Put

$$N' = \mathrm{Ker}(\Pi \to (G_k)^{p'} \simeq \widehat{\mathbb{Z}}^{p'}),$$
$$N = \mathrm{Ker}(\Pi \to (G_k)^{p} \simeq \mathbb{Z}_p).$$

Then

$$N' = \mathrm{Ker}(\Pi \to (\Pi^{\mathrm{ab}})^{p'}/((\Pi^{\mathrm{ab}})^{p'})_{\mathrm{tors}}),$$

and N *is the unique closed subgroup of* Π *such that* (a) $\Pi/N \simeq \mathbb{Z}_p$*; and* (b) $\log(\sharp(((N_m^{\mathrm{ab}})^{p'})_{\mathrm{tors}})) = O(p^m)$ $(m \to +\infty)$, *where*

$$N_m \stackrel{\mathrm{def}}{=} \mathrm{Ker}(\Pi \to (\Pi/N)/p^m \simeq \mathbb{Z}/p^m\mathbb{Z}).$$

Moreover, $\overline{\Pi} = N' \cap N$.

Proof. If $n = 0$ or $\cdot =$ tame, then, by (1.1), $\overline{\Pi}$ is finitely generated, hence so is Π, since G_k is now finitely generated. If $n > 0$ and $\cdot = (\mathrm{unrestricted})$, then we see that $\mathrm{Hom}_{\mathrm{cont}}(\Pi, \mathbb{Z}/p\mathbb{Z})$ is infinite-dimensional as a $\mathbb{Z}/p\mathbb{Z}$-vector space, using the Artin–Schreier theory. Therefore $(\Pi^{\mathrm{ab}})^p$ is not finitely generated. These imply (i).

Next, we have the following exact sequence (written additively):

$$0 \to (\overline{\Pi}^{\mathrm{ab}})_{G_k} \to \Pi^{\mathrm{ab}} \to G_k \to 0,$$

where, for a topological G_k-module M, the G_k-coinvariant quotient M_{G_k} is defined by:

$$M_{G_k} \stackrel{\mathrm{def}}{=} M/\overline{\langle \sigma(m) - m \mid m \in M, \sigma \in G_k \rangle}.$$

Note that (when M is compact)

$$M_{G_k} = M/(\varphi_k - 1)M,$$

where φ_k is the $\sharp(k)$-th power Frobenius element in G_k.

Let P be the characteristic polynomial of the Frobenius element $\varphi_k \in G_k$ on the free $\widehat{\mathbb{Z}}^{p'}$-module $(\overline{\Pi}^{\mathrm{ab}})^{p'}$. (For the G_k-module structure of $\overline{\Pi}^{\mathrm{ab}}$, see (1.3).) The coefficients of P are in $\mathbb{Z}$, and the absolute values of the roots of P are either $\sharp(k)^{1/2}$ (for $2g$ roots) or $\sharp(k)$ (for $n - \varepsilon$ roots, where ε is 0 for $n = 0$ and is 1 for $n > 0$). In particular, $P(1)$ is a non-zero integer, hence $(\overline{\Pi}^{\mathrm{ab}})_{G_k}$ (resp. $((\overline{\Pi}^{\mathrm{ab}})^{p'})_{G_k}$) is finite in the case (ii) (resp. (iii)). (For the case (ii), observe that $P(\varphi_k)$ is 0 also on the pro-p part.) Now, all the statements except for N in the case (iii) are clear.

Next, check the conditions (a) and (b) for N. (a) immediately follows from the definition of N. For (b), let $\alpha_1, \ldots, \alpha_{2g+n-\varepsilon}$ be the roots of P. Since $((N_m^{\mathrm{ab}})^{p'})_{\mathrm{tors}} =$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

$(\overline{\Pi}^{\mathrm{ab}})^{p'}/(\varphi_k^{p^m}-1)(\overline{\Pi}^{\mathrm{ab}})^{p'}$ similarly as above, we have $\sharp(((N_m^{\mathrm{ab}})^{p'})_{\mathrm{tors}}) = P_m(1)'$, where

$$P_m(T) = \prod_{i=1}^{2g+n-\varepsilon} (T-\alpha_i^{p^m})$$

and a' means the maximal integer (>0) prime to p dividing a given integer $a \neq 0$. Thus

$$\begin{aligned}\sharp(((N_m^{\mathrm{ab}})^{p'})_{\mathrm{tors}}) &= P_m(1)' \leqslant |P_m(1)| \\ &= \textstyle\prod |1-\alpha_i^{p^m}| \leqslant \prod(1+|\alpha_i^{p^m}|) \\ &= (1+q^{p^m/2})^{2g}(1+q^{p^m})^{n-\varepsilon} \leqslant (2q^{p^m/2})^{2g}(2q^{p^m})^{n-\varepsilon} \\ &= 2^{2g+n-\varepsilon}q^{(g+n-\varepsilon)p^m},\end{aligned}$$

where $q = \sharp(k)$, and (b) follows from this.

Finally, let M be any closed subgroup $\neq N$ of Π satisfying $\Pi/M \simeq \mathbb{Z}_p$, and put $M_m = \mathrm{Ker}(\Pi \to (\Pi/M)/p^m)$ and $k_m = \bar{k}^{\mathrm{pr}(M_m)}$. Then

$$((M_m^{\mathrm{ab}})^{p'})_{\mathrm{tors}} = \frac{(\overline{M}_m{}^{\mathrm{ab}})^{p'}}{(\varphi_{k_m}-1)(\overline{M}_m{}^{\mathrm{ab}})^{p'}} \twoheadrightarrow \frac{T(J_{X_{M_m}})^{p'}}{(\varphi_{k_m}-1)T(J_{X_{M_m}})^{p'}}.$$

Observe that the sequence $k_1 \subset k_2 \subset \cdots \subset k_m \subset \cdots$ stabilizes, from the assumption $M \neq N$. Now, [GK, Theorem 1 and Theorem 2] implies that there exists $C > 0$ such that

$$\log(\sharp(((M_m^{\mathrm{ab}})^{p'})_{\mathrm{tors}})) \geqslant Cp^{2m},$$

for sufficiently large m. □

2. $q = \sharp(k)$ and the Frobenius element φ_k (for k finite).

By a recent theorem of Pop [Pop 3], for k finitely generated over $\mathbb{Q}$, the profinite group G_k determines the isomorphism class of the field k. Thus, in this case, Π also determines the isomorphism class of k by (3.2). Moreover, [Pop 3] also shows that any automorphism of G_k for such k comes from an automorphism of k or, more precisely, an automorphism of $\bar{k}$ mapping k onto itself.

On the other hand, for k finite, (the isomorphism class of) the profinite group $G_k \simeq \widehat{\mathbb{Z}}$ is independent of k and does not determine the isomorphism class of k (nor, equivalently, $\sharp(k)$). Moreover, for such k, *any* automorphism of $\bar{k}$, which preserves k automatically, defines the identity in $\mathrm{Aut}(G_k)$, while $\mathrm{Aut}(G_k) = \mathrm{Aut}(\widehat{\mathbb{Z}}) = \widehat{\mathbb{Z}}^{\times}$ is big.

However, the following proposition shows that Π determines $\sharp(k)$ and the Frobenius element $\varphi_k \in G_k = \Pi/\overline{\Pi}$ group-theoretically. (Recall (3.1)(3.3) that the prime number $p = \mathrm{char}(k)$ is determined by Π.)

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

PROPOSITION (3.4). *Assume that k is finite, and denote by φ_k the $\sharp(k)$-th power Frobenius element in G_k.*

(i) *The subgroup $\Phi \stackrel{\text{def}}{=} \varphi_k^{\mathbb{Z}}$ of G_k has the following properties:* (a) *G_k is topologically generated by Φ; and* (b) *for each open subgroup $\mathcal{H}$ of Π with $(\bar{\mathcal{H}}^{\text{ab}})^{p'} \neq 0$, the image of $\Phi \cap \text{pr}(\mathcal{H})$ by*

$$\text{pr}(\mathcal{H}) \to \text{Aut}\left(\bigwedge_{\widehat{\mathbb{Z}}^{p'}}^{\max} (\bar{\mathcal{H}}^{\text{ab}})^{p'}\right) = (\widehat{\mathbb{Z}}^{p'})^{\times}$$

is contained in $\pm p^{\mathbb{Z}}$.

The properties (a) *and* (b) *(for one such $\mathcal{H}$) characterize Φ.*

(ii) *The Frobenius element φ_k has the following properties:* (a) *Φ is generated by φ_k; and* (b) *for each open subgroup $\mathcal{H}$ of Π with $(\bar{\mathcal{H}}^{\text{ab}})^{p'} \neq 0$, the image of $\varphi_k^{[G_k:\text{pr}(\mathcal{H})]} \in \text{pr}(\mathcal{H})$ by*

$$\text{pr}(\mathcal{H}) \to \text{Aut}\left(\bigwedge_{\widehat{\mathbb{Z}}^{p'}}^{\max} (\bar{\mathcal{H}}^{\text{ab}})^{p'}\right) = (\widehat{\mathbb{Z}}^{p'})^{\times}$$

is contained in $\pm p^{\mathbb{Z}_{>0}}$.

These properties (a) *and* (b) *(for one such $\mathcal{H}$) characterize φ_k.*

(iii) *For each open subgroup $\mathcal{H}$ of Π, denote by $|\mathcal{A}_{\mathcal{H}}|$ the set of the absolute values of the eigenvalues of the action of $\varphi_{k_{\mathcal{H}}} = \varphi_k^{[G_k:\text{pr}(\mathcal{H})]}$ on the free $\widehat{\mathbb{Z}}^{p'}$-module $(\bar{\mathcal{H}}^{\text{ab}})^{p'}$.*

When $\overline{\Pi}$ is abelian, then the $\widehat{\mathbb{Z}}^{p'}$-rank i_0 of $\overline{\Pi}^{p'}$ is either 1 or 2, and is 1 if and only if $n > 0$. We have $|\mathcal{A}_{\mathcal{H}}| = \{\sharp(k)^{[G_k:\text{pr}(\mathcal{H})]/i_0}\}$ for any open subgroup $\mathcal{H}$ of Π. These characterize $\sharp(k)$ in this case.

When $\overline{\Pi}$ is not abelian, then

$$|\mathcal{A}_{\mathcal{H}}| \subset \{\sharp(k)^{[G_k:\text{pr}(\mathcal{H})]/i} \mid i = 1, 2\},$$

and $n > 0$ if and only if $\sharp(|\mathcal{A}_{\mathcal{H}}|) = 2$ for some open subgroup $\mathcal{H}$ of Π. If $n = 0$, then

$$|\mathcal{A}_{\mathcal{H}}| = \{\sharp(k)^{[G_k:\text{pr}(\mathcal{H})]/2}\}.$$

These characterize $\sharp(k)$ in this case.

Proof. (i) From the isomorphism (1-3) and the exact sequence (1-5) (for $U_{\mathcal{H}}$), we can compute the character

$$\rho_{\mathcal{H}}^{\text{det}}\colon \text{pr}(\mathcal{H}) \to \text{Aut}\left(\bigwedge_{\widehat{\mathbb{Z}}^{p'}}^{\max} (\bar{\mathcal{H}}^{\text{ab}})^{p'}\right) = (\widehat{\mathbb{Z}}^{p'})^{\times}$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

and obtain

$$\rho_{\mathcal{H}}^{\det} = {\lambda_{k_{\mathcal{H}}}}^{n_{\mathcal{H}}-n_{0,\mathcal{H}}}\chi^{g_{\mathcal{H}}+n_{\mathcal{H}}-\varepsilon},$$

where χ is the cyclotomic character $\mathrm{pr}(\mathcal{H}) \subset G_k \to (\widehat{\mathbb{Z}}^{p'})^{\times} = \mathrm{Aut}(\widehat{\mathbb{Z}}^{p'}(1))$, and $\lambda_{k_{\mathcal{H}}}$ is the character defined as

$$\mathrm{pr}(\mathcal{H}) \twoheadrightarrow \mathrm{pr}(\mathcal{H})/(\mathrm{pr}(\mathcal{H}))^2 \simeq \{\pm 1\} \hookrightarrow (\widehat{\mathbb{Z}}^{p'})^{\times},$$

and $n_{0,\mathcal{H}} \overset{\text{def}}{=} \sharp(S_{\mathcal{H}}) = \sharp(\Sigma_{S_{\mathcal{H}}})$. In particular,

$$\rho_{\mathcal{H}}^{\det}(\varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]}) = (-1)^{n_{\mathcal{H}}-n_{0,\mathcal{H}}}\sharp(k_{\mathcal{H}})^{g_{\mathcal{H}}+n_{\mathcal{H}}-\varepsilon},$$

which lies in $\pm p^{\mathbb{Z}}$. Since $\Phi \cap \mathrm{pr}(\mathcal{H}) = \varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]\mathbb{Z}}$, we have $\rho_{\mathcal{H}}^{\det}(\varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]\mathbb{Z}}) \subset \pm p^{\mathbb{Z}}$. So Φ satisfies (b), and also (a) clearly.

Now, assume $(\bar{\mathcal{H}}^{\mathrm{ab}})^{p'} \neq 0 (\Longleftrightarrow 2g_{\mathcal{H}}+n_{\mathcal{H}}-\varepsilon > 0 \Longleftrightarrow (g_{\mathcal{H}}, n_{\mathcal{H}}) \neq (0,1) \iff g_{\mathcal{H}} + n_{\mathcal{H}} - \varepsilon > 0)$, then

$$\mathrm{Ker}(\rho_{\mathcal{H}}^{\det}) \subset \mathrm{Ker}((\rho_{\mathcal{H}}^{\det})^2) = \mathrm{Ker}(\chi^{2(g_{\mathcal{H}}+n_{\mathcal{H}}-\varepsilon)}) = \{1\}.$$

If $\sigma \in \mathrm{pr}(\mathcal{H})$ satisfies $\rho_{\mathcal{H}}^{\det}(\sigma) \in \pm p^{\mathbb{Z}}$, then we have $\rho_{\mathcal{H}}^{\det}(\sigma)^s = \rho_{\mathcal{H}}^{\det}(\varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]})^r$ for some $s \in \mathbb{Z}_{>0}$ and $r \in \mathbb{Z}$. This implies $\sigma \in \varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]\mathbb{Z}}$, since $\mathrm{pr}(\mathcal{H}) = \varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]\widehat{\mathbb{Z}}} \simeq \widehat{\mathbb{Z}}$. This implies that Φ' with the condition (b) for $\mathcal{H}$ satisfies: $(\Phi')^{[G_k:\mathrm{pr}(\mathcal{H})]} (\subset \Phi' \cap \mathcal{H}) \subset \varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]\mathbb{Z}}$, which implies $\Phi' \subset \varphi_k^{\mathbb{Z}} = \Phi$. If, moreover, Φ' satisfies (a), then it must coincide with Φ.

(ii) Observe that, for $\sigma \in G_k$, $\Phi = \sigma^{\mathbb{Z}}$ if and only if $\sigma = \varphi_k$ or φ_k^{-1}, and that

$$\rho_{\mathcal{H}}^{\det}(\varphi_k^{[G_k:\mathrm{pr}(\mathcal{H})]}) = (-1)^{n_{\mathcal{H}}-n_{0,\mathcal{H}}}\sharp(k_{\mathcal{H}})^{g_{\mathcal{H}}+n_{\mathcal{H}}-\varepsilon} \in \pm p^{\mathbb{Z}_{>0}},$$

if $g_{\mathcal{H}} + n_{\mathcal{H}} - \varepsilon > 0$.

(iii) As has been explained in the proof of (3.3), the absolute values are $\sharp(k_{\mathcal{H}})^{1/2} = \sharp(k)^{[G_k:\mathrm{pr}(\mathcal{H})]/2}$ ($2g_{\mathcal{H}}$ times) and $\sharp(k_{\mathcal{H}}) = \sharp(k)^{[G_k:\mathrm{pr}(\mathcal{H})]}$ ($n_{\mathcal{H}} - \varepsilon$ times).

From our assumption that $\overline{\Pi}$ is non-trivial, $\overline{\Pi}$ is abelian if and only if either $(g,n) = (0,2)$ and $\cdot =$ tame, or $(g,n) = (1,0)$. In both cases, we have $(g_{\mathcal{H}}, n_{\mathcal{H}}) = (g,n)$ for any open subgroup $\mathcal{H}$ of Π. Since

$$i_0 = 2g + n - \varepsilon = \left\{ \begin{array}{ll} 1, & \text{for } (g,n) = (0,2), \cdot = \text{tame}, \\ 2, & \text{for } (g,n) = (1,0), \end{array} \right\}$$

the statements for the abelian case hold.

Assume that $\overline{\Pi}$ is not abelian. If $n = 0$, then $n_{\mathcal{H}} = 0$ for all open subgroup $\mathcal{H}$ of Π. If $n > 0$, then, by (1.10)(ii), there exists an open subgroup $\mathcal{H}$ such that $g_{\mathcal{H}} > 0$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

and $n_{\mathcal{H}} > 1$, hence $\sharp(|\mathcal{A}_{\mathcal{H}}|) = 2$. The statements for the non-abelian case follow from this. □

3. g and n.

We can recover (g, n), using the Frobenius weight.

PROPOSITION (3.5). *Assume that k is finite. Define P to be the characteristic polynomial of the $\sharp(k)$-th power Frobenius element $\varphi_k \in G_k$ on the free $\widehat{\mathbb{Z}}^{p'}$-module $(\overline{\Pi}^{\mathrm{ab}})^{p'}$, and $\mathcal{A}$ the set of roots of P.*

(i) *$n > 0$ if and only if $\overline{\Pi}^{p'}$ is a free pro-p' group.* (*cf.* (3.4) *for another criterion for $n > 0$.*)

(ii) *If $n = 0$, then*

$$g = \tfrac{1}{2}\mathrm{rank}_{\widehat{\mathbb{Z}}^{p'}}((\overline{\Pi}^{\mathrm{ab}})^{p'}) = \tfrac{1}{2}\sharp_m(\mathcal{A}).$$

If $n > 0$, then

$$g = \tfrac{1}{2}\sharp_m(\{\alpha \in \mathcal{A} \mid |\alpha| = \sharp(k)^{1/2}\}),$$
$$n = \sharp_m(\{\alpha \in \mathcal{A} \mid |\alpha| = \sharp(k)\}) + 1.$$

Here, for a subset $\mathcal{A}'$ of $\mathcal{A}$, we define

$$\sharp_m(\mathcal{A}') \stackrel{\text{def}}{=} \sum_{\alpha \in \mathcal{A}'} m_\alpha,$$

where m_α is defined by:

$$P(T) = \prod_{\alpha \in \mathcal{A}} (T - \alpha)^{m_\alpha}.$$

Proof. (i) follows from (1.1). (ii) follows from the isomorphism (1-3) and the exact sequence (1-5). □

Remark (3.6). (i) In the case where k is finitely generated over $\mathbb{Q}$, the recovery of (g, n) from Π can be reduced to the finite field case.

(ii) In fact, when $\mathrm{char}(k) > 0$ and $\cdot = (\text{unrestricted})$, $\overline{\Pi}$ (without G_k) determines g and n. We shall treat this in another paper.

4. The kernel $I(\Pi)$ of $\Pi (= \pi_1^{\cdot}(U, \overline{\overline{\xi}})^{(\mathcal{C})}) \to \pi_1(X, \overline{\overline{\xi}})^{(\mathcal{C})}$.

We can recover $I(\Pi)$, as follows.

PROPOSITION (3.7). *Let $\mathcal{H}$ be an open subgroup of Π. Then $\mathcal{H} \supset I(\Pi)$ if and only if $2g_{\mathcal{H}} - 2 = (\overline{\Pi} : \mathcal{H})(2g - 2)$.*

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Moreover,

$$I(\Pi) = \bigcap_{\mathcal{H}\subset\Pi:\,\text{open},\,2g_{\mathcal{H}}-2=(\overline{\Pi}:\,\mathcal{H})(2g-2)} \mathcal{H}.$$

Proof. The first statement follows from the Hurwitz genus formula. The second follows from the first. □

5. The number of rational points (for k finite).

PROPOSITION (3.8). *Assume that k is finite, and let L/k be a finite sub-extension of $\bar{k}/k$. Then*

$$\sharp(X(L)) = 1 + \sharp(L) - \mathrm{tr}_{\widehat{\mathbb{Z}}^{p'}}(\varphi_L \mid ((\overline{\Pi}/I(\Pi))^{\mathrm{ab}})^{p'}),$$

where $\varphi_L \in G_L \subset G_k$ is the $\sharp(L)$-th power Frobenius element (*which coincides with $\varphi_k^{[G_k:G_L]}$*).

In particular, $\sharp(X(L))$ is not empty if and only if

$$1 + \sharp(L) - \mathrm{tr}_{\widehat{\mathbb{Z}}^{p'}}(\varphi_L \mid ((\overline{\Pi}/I(\Pi))^{\mathrm{ab}})^{p'}) > 0.$$

Proof. Lefschetz trace formula. (Recall (1-3) that $((\overline{\Pi}/I(\Pi))^{\mathrm{ab}})^{p'}$ is isomorphic to $T(J_X)^{p'}$ as a G_k-module.) □

4. The Grothendieck conjecture for curves over finite fields

For $i = 1, 2$, let k_i be a field of characteristic $p_i \geqslant 0$. Let U_i be a smooth, geometrically connected curve over k_i, and X_i the smooth compactification of U_i. Put $S_i = X_i - U_i$. Define non-negative integers g_i and n_i to be the genus of X_i over k_i and the cardinality of $S_i(\bar{k}_i)$, respectively. Let ξ_i be the generic point of U_i, and put $K_i = \kappa(\xi_i)$, the function field of U_i.

Fix a separable closure k_i^{sep}, and define $\bar{U}_i$, $\bar{X}_i$, $\bar{S}_i$, and $\bar{\xi}_i$ to be $U_i \otimes_{k_i} k_i^{\mathrm{sep}}$, $X_i \otimes_{k_i} k_i^{\mathrm{sep}}$, $S_i \otimes_{k_i} k_i^{\mathrm{sep}}$, and $\xi_i \otimes_{k_i} k_i^{\mathrm{sep}}$, respectively.

Take a geometric point $\overline{\bar{\xi}}_i$ of $\bar{U}_i$ above the generic point $\bar{\xi}_i$. Let the symbol $\cdot$ denote either (unrestricted) or tame, and fix a full class $\mathcal{C}$ of finite groups containing $\mathbb{Z}/l\mathbb{Z}$ for all prime numbers l.

Put

$$\Pi_i = \pi_1^{\cdot}(U_i, \overline{\bar{\xi}}_i)^{(\mathcal{C})}$$

and

$$\overline{\Pi}_i = \pi_1^{\cdot}(\bar{U}_i, \overline{\bar{\xi}}_i)^{\mathcal{C}},$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

for simplicity. Define $\tilde{K}_i$ to be the maximal pro-$\mathcal{C}$ Galois extension of $K_i k_i^{\text{sep}}$ in $\kappa(\overline{\overline{\xi}}_i)/K_i k_i^{\text{sep}}$, unramified on U_i, and, if $\cdot = \text{tame}$, (at most) tamely ramified on S_i, and $\tilde{U}_i$ the integral closure of U_i in $\tilde{K}_i$. Note that we have:

$$\Pi_i = \text{Gal}(\tilde{K}_i/K_i) = \text{Aut}(\tilde{U}_i/U_i)$$

and

$$\overline{\Pi}_i = \text{Gal}(\tilde{K}_i/K_i k_i^{\text{sep}}) = \text{Aut}(\tilde{U}_i/\bar{U}_i).$$

Define

$$\text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$$

$$\stackrel{\text{def}}{=} \left\{ (\tilde{F}, F) \in \text{Isom}(\tilde{U}_1, \tilde{U}_2) \times \text{Isom}(U_1, U_2) \;\middle|\; \begin{array}{ccc} \tilde{U}_1 & \xrightarrow{\tilde{F}} & \tilde{U}_2 \\ \downarrow & & \downarrow \\ U_1 & \xrightarrow{F} & U_2 \end{array} \text{ is commutative} \right\},$$

where Isom means $\text{Isom}_{(\text{Schemes})}$.

LEMMA (4.1). (i) *The projection*

$$\tilde{p}\colon \text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \text{Isom}(\tilde{U}_1, \tilde{U}_2)$$

is injective. Thus $\text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$ *is identified with*

$$\left\{ \tilde{F} \in \text{Isom}(\tilde{U}_1, \tilde{U}_2) \;\middle|\; \begin{array}{ccc} \tilde{U}_1 & \xrightarrow{\tilde{F}} & \tilde{U}_2 \\ \downarrow & & \downarrow \\ U_1 & \xrightarrow{F} & U_2 \end{array} \text{ is commutative for some } F \in \text{Isom}(U_1, U_2) \right\}.$$

(ii) *The projection*

$$p\colon \text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \text{Isom}(U_1, U_2)$$

is surjective, and

$$p^{-1}p((\tilde{F}, F)) = \tilde{F}\,\text{Aut}(\tilde{U}_1/U_1) = \text{Aut}(\tilde{U}_2/U_2)\tilde{F}.$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Proof. (i) follows from the fact that $\tilde{U}_1 \to U_1$ is faithfully flat.

To prove (ii), we need the following lemma:

LEMMA (4.2). *Let A be a finitely generated integral domain over a field k, and assume that k is integrally closed in A. Then any subfield of A is contained in k, i.e. k is the maximal subfield of A.*

Proof. Suppose that there exists a subfield K of A, not contained in k. Take any $t \in K - k$, then t is transcendental over k by assumption. Since A is finitely generated over its subring $k[t]$, the image of $\mathrm{Spec}(A) \to \mathrm{Spec}(k[t])$ is constructible and dense, hence is open (and dense). (Observe the topology of $\mathrm{Spec}(k[t])$.) Let $\mathbb{F}$ be the prime field of k, then it is easy to see that $\mathrm{Spec}(k[t]) \to \mathrm{Spec}(\mathbb{F}[t])$ is an open map. Thus, the image of $\mathrm{Spec}(A) \to \mathrm{Spec}(\mathbb{F}[t])$ is open. On the other hand, since $\mathbb{F}(t) \subset K \subset A$, the image of $\mathrm{Spec}(A) \to \mathrm{Spec}(\mathbb{F}[t])$ is the generic point $\mathrm{Spec}(\mathbb{F}(t))$ of $\mathrm{Spec}(\mathbb{F}[t])$. This is absurd. □

By this lemma, any isomorphism $F\colon U_1 \simeq U_2$ induces an isomorphism $k_1 \simeq k_2$ compatible with F. (Choose affine open coverings if necessary.) Then, we see that there exists an isomorphism $\bar{F}\colon \bar{U}_1 \simeq \bar{U}_2$ extending F. Now, it is clear that there exists an isomorphism $\tilde{U}_1 \simeq \tilde{U}_2$ extending $\bar{F}$. (If G_k is a pro-$\mathcal{C}$ group, then we can directly prove the existence of an isomorphism $\tilde{U}_1 \simeq \tilde{U}_2$ extending F.)

The second statement of (ii) directly follows from the definition. □

The aim of this section is to prove the following theorem.

THEOREM (4.3). *Assume that both k_1 and k_2 are finite, and that $n_i > 0$* (resp. *$n_i > 0$ and $2 - 2g_i - n_i < 0$) for some $i \in \{1, 2\}$, if $\cdot =$ (unrestricted)* (resp. *$\cdot =$ tame*). (*Observe that this condition is equivalent to saying that $n_i > 0$ and $\overline{\Pi}_i$ is not abelian.*)

Then the map

$$\mathrm{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}(\Pi_1, \Pi_2),\ (\tilde{F}, F) \mapsto \tilde{F}(\cdot)\tilde{F}^{-1}$$

is bijective.

We shall prove this by constructing the inverse map, borrowing some techniques of [Uchida].

Let $\mathcal{F}$ be an isomorphism $\Pi_1 \to \Pi_2$ (as topological groups). We may assume that $n_1 > 0$ (resp. $n_1 > 0$ and $2 - 2g_1 - n_1 < 0$) if $\cdot =$ (unrestricted) (resp. $\cdot =$ tame), considering $\mathcal{F}^{-1}$ if necessary. Then $\overline{\Pi}_1$ is not abelian, and neither is Π_1, a fortiori. Thus Π_2 is also not abelian, hence $\overline{\Pi}_2$ is not trivial. Therefore, we apply the results in Section 3 to both U_1 and U_2.

By (3.3), $\mathcal{F}(\overline{\Pi}_1) = \overline{\Pi}_2$, and, by (3.1), $p_1 = p_2$. Denote this prime number by p. Now, $\mathcal{F}$ induces an isomorphism $G_{k_1} = \Pi_1/\overline{\Pi}_1 \to \Pi_2/\overline{\Pi}_2 = G_{k_2}$, which

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

we also denote by $\mathcal{F}$, and, by (3.4), $\mathcal{F}(\varphi_{k_1}) = \varphi_{k_2}$ and $\sharp(k_1) = \sharp(k_2)$. By (3.5), $(g_1, n_1) = (g_2, n_2)$, which we denote by (g, n).

By (2.10), together with (3.7) and (3.8) (for each open subgroup of Π_i), $\mathcal{F}$ induces a bijection $\Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$, which we denote by $f = f_{\mathcal{F}}$, characterized by: $D_{f(\tilde{v}_1)} = \mathcal{F}(D_{\tilde{v}_1})$ for each $\tilde{v}_1 \in \Sigma_{\tilde{X}_1}$. Note that $f(\Sigma_{\tilde{X}_1} \cap \tilde{U}_1) = \Sigma_{\tilde{X}_2} \cap \tilde{U}_2$ by (2.8)(iii). This bijection induces a bijection $\Sigma_{X_{1,\mathcal{H}_1}} \to \Sigma_{X_{2,\mathcal{F}(\mathcal{H}_1)}}$ for each closed subgroup $\mathcal{H}_1$ of Π_1, which we also denote by f. In particular, we obtain a bijection

$$X_{1,\bar{\mathcal{H}}_1}(\bar{k}_1) = \Sigma_{X_{1,\bar{\mathcal{H}}_1}} \to \Sigma_{X_{2,\overline{\mathcal{F}(\mathcal{H}_1)}}} = X_{2,\overline{\mathcal{F}(\mathcal{H}_1)}}(\bar{k}_2),$$

for each open subgroup $\mathcal{H}_1$ of Π_1. (Observe $\mathcal{F}(\bar{\mathcal{H}}_1) = \overline{\mathcal{F}(\mathcal{H}_1)}$.) Since the bijection $f\colon \Sigma_{X_1} \to \Sigma_{X_2}$ sends $\Sigma_{X_1} \cap U_1$ onto $\Sigma_{X_2} \cap U_2$, we have $\sharp(S_1) = \sharp(S_2)$, which we denote by n_0. Note that $n_0 \leqslant n$ and the equality holds if and only if all points on S_i are k_i-rational for some (or all) $i \in \{1, 2\}$.

For each $v_i \in \Sigma_{X_i}$, choose a $\tilde{v}_i \in \Sigma_{\tilde{X}_i}$ above v_i. Let $F_{\tilde{v}_i}$ be the inverse image of $\varphi_{k_i}^{\mathbb{Z}}$ by $D_{\tilde{v}_i}^{\mathrm{ab}} \to G_{k_i}$. If both $\tilde{v}_i$ and $\tilde{v}_i'$ are above v_i, then $F_{\tilde{v}_i}$ and $F_{\tilde{v}_i'}$ are canonically isomorphic to each other. So, we may and do write F_{v_i} instead of $F_{\tilde{v}_i}$. By local class field theory, together with (2.2), we have:

$$F_{v_i} = \begin{cases} K_{v_i}^{\times}/O_{v_i}^{\times} = \mathbb{Z}, & \text{if } v_i \in U_i \\ K_{v_i}^{\times}, & \text{if } v_i \in S_i \text{ and } \cdot = (\text{unrestricted}) \\ K_{v_i}^{\times}/(1 + \mathfrak{M}_{v_i}), & \text{if } v_i \in S_i \text{ and } \cdot = \text{tame}, \end{cases}$$

where K_{v_i} is the v_i-adic completion of K_i, O_{v_i} is the valuation ring of K_{v_i}, and $\mathfrak{M}_{v_i}$ is the maximal ideal of O_{v_i}.

In any case, $\mathcal{F}$ induces isomorphisms $\Pi_1^{\mathrm{ab}} \to \Pi_2^{\mathrm{ab}}$ and $F_{v_1} \to F_{f(v_1)}$ $(v_1 \in \Sigma_{X_1})$, which are also denoted by $\mathcal{F}$. Now, taking the restricted direct product Π' of F_{v_i} $(v_i \in \Sigma_{X_i})$ with respect to $\mathrm{Ker}(F_{v_i} \to G_{k_i})$, we obtain the following commutative diagram:

$$\begin{array}{ccc} \prod_{v_1 \in \Sigma_{X_1}}{}' F_{v_1} & \longrightarrow & \prod_{v_2 \in \Sigma_{X_2}}{}' F_{v_2} \\ \downarrow & & \downarrow \\ \Pi_1^{\mathrm{ab}} & \longrightarrow & \Pi_2^{\mathrm{ab}}. \end{array}$$

(In fact, Π' coincides with $\bigoplus$.) The horizontal arrows are isomorphisms. Define F_1 (resp. F_2) to be the kernel of the left (resp. right) vertical arrow, then we obtain an isomorphism $F_1 \to F_2$, which we also denote by $\mathcal{F}$.

By (global) class field theory, we have

$$F_i = K_i^{\times}.$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

(So far we have only used the assumption that $\overline{\Pi}_i$ is not abelian. Here we use the assumption $n_i > 0$ for the first time. In fact, if $n_i = 0$, then $F_i = K_i^\times / k_i^\times$.)

Let $\mathcal{H}_1$ be any open subgroup of Π_1, and put $\mathcal{H}_2 = \mathcal{F}(\mathcal{H}_1)$. We can apply the arguments until now to the isomorphism

$$\pi_1^{\cdot}(U_{1,\mathcal{H}_1}, \overline{\overline{\xi}}) = \mathcal{H}_1 \overset{\mathcal{F}}{\to} \mathcal{H}_2 = \pi_1^{\cdot}(U_{2,\mathcal{H}_2}, \overline{\overline{\xi}}).$$

In this situation, we write various symbols with index $\mathcal{H}_1$ or $\mathcal{H}_2$.

LEMMA (4.4). *The isomorphism*

$$K^\times_{1,\mathcal{H}_1} = F_{1,\mathcal{H}_1} \to F_{2,\mathcal{H}_2} = K^\times_{2,\mathcal{H}_2}$$

induced by $\mathcal{F}$ is an extension of

$$K_1^\times = F_1 \to F_2 = K_2^\times.$$

Proof. Similar to [Uchida, Lemma 9]. (Observe that, for each $w_i \in \Sigma_{X_i,\mathcal{H}_i}$ above $v_i \in \Sigma_{X_i}$, the transfer map induces $F_{v_i} \to F_{\mathcal{H}_i,w_i}$.) □

COROLLARY (4.5). *Let $\mathcal{I}_1$ be a closed subgroup of Π_1 and put $\mathcal{I}_2 = \mathcal{F}(\mathcal{I}_1)$. Then $\mathcal{F}$ induces an isomorphism*

$$K^\times_{1,\mathcal{I}_1} \to K^\times_{2,\mathcal{I}_2},$$

(*which we also denote by $\mathcal{F}$.*)

In particular, $\mathcal{F}$ induces an isomorphism

$$\tilde{K}_1^\times \to \tilde{K}_2^\times.$$ □

Extend by $0 \mapsto 0$ the group isomorphism $\mathcal{F}\colon \tilde{K}_1^\times \to \tilde{K}_2^\times$ to the (multiplicative) monoid isomorphism $\tilde{K}_1 \to \tilde{K}_2$, which we also denote by $\mathcal{F}$.

CLAIM (4.6). The isomorphism $\mathcal{F}\colon \tilde{K}_1 \to \tilde{K}_2$ is *additive*.

This is the main difficulty in the proof. *Assuming* this, we shall first complete the proof.

Since $A_i \overset{\text{def}}{=} \Gamma(U_i, \mathcal{O}_{X_i})$ in K_i coincides with

$$\left\{ a \in K_i^\times \mid \text{the image of } a \text{ by } K_i^\times = F_i \overset{\text{proj.}}{\longrightarrow} F_{v_i} \subset D_{\tilde{v}_i}^{\text{ab}} \to G_{k_i} \right.$$
$$\left. \text{is in } \varphi_{k_i}^{\mathbb{Z}_{\geqslant 0}} \text{ for each } v_i \in U_i. \right\} \cup \{0\},$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

we see $\mathcal{F}(A_1) = A_2$. Hence $\mathcal{F}(\tilde{A}_1) = \tilde{A}_2$ also holds, where

$$\tilde{A}_i \stackrel{\text{def}}{=} \Gamma(\tilde{U}_i, \mathcal{O}_{\tilde{X}_i}).$$

(Note that $\tilde{A}_i$ is the integral closure of A_i in $\tilde{K}_i$.) Thus we obtain a map

$$\text{Isom}(\Pi_1, \Pi_2) \to \text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2).$$

From the functorialities it follows that

$$\text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \text{Isom}(\Pi_1, \Pi_2) \to \text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$$

is the identity. We have to prove that

$$\text{Isom}(\Pi_1, \Pi_2) \to \text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \text{Isom}(\Pi_1, \Pi_2)$$

is also the identity. For this it suffices to prove that

$$\text{Isom}(\Pi_1, \Pi_2) \to \text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$$

is injective. Let $\mathcal{F}, \mathcal{F}'$ be elements of $\text{Isom}(\Pi_1, \Pi_2)$ which induce a same element of $\text{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$. Put $\mathcal{E} = \mathcal{F}'^{-1}\mathcal{F}$, then $\mathcal{E}$ induces the identity in $\text{Isom}(\tilde{U}_1/U_1, \tilde{U}_1/U_1)$. In particular, for any closed subgroup $\mathcal{H}$ of Π_1, we have $\mathcal{E}(\mathcal{H}) = \mathcal{H}$. Applying this to the closed subgroup $\mathcal{H} = x^{\widehat{\mathbb{Z}}}$ for each element x of Π_1, we obtain $\mathcal{E}(x) = x^{\alpha(x)}$ for some $\alpha(x) \in \widehat{\mathbb{Z}}^\times$. When x is a lifting of $\varphi_{k_1} \in G_{k_1}$, (3.4) implies $\alpha(x) = 1$. Since Π_1 is topologically generated by such x's, we obtain that $\mathcal{E}$ is the identity.

Now only the claim (4.6) remains. For this, we resort to the following:

LEMMA (4.7). *For each $i = 1, 2$, let k_i be an algebraically closed field, and X_i a proper, smooth, connected curve over k_i. Put $K_i = k_i(X_i)$ and $\Sigma_i = X_i(k_i)$. Let S_i be a subset of Σ_i.*

Now, assume that we are given an isomorphism $\mathcal{F}: K_1 \to K_2$ as multiplicative monoids and a bijection $f: \Sigma_1 \to \Sigma_2$ with $f(S_1) = S_2$, satisfying the following (a)(b)(c)*:*

(a) *For each $P_1 \in \Sigma_1$, the diagram*

$$\begin{array}{ccc} K_1 & \xrightarrow{\text{ord}_{P_1}} & \mathbb{Z} \cup \{+\infty\} \\ \downarrow & & \| \\ K_2 & \xrightarrow{\text{ord}_{P_2}} & \mathbb{Z} \cup \{+\infty\} \end{array}$$

is commutative, where $P_2 \stackrel{\text{def}}{=} f(P_1)$.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

(b) *For each* $P_1 \in S_1$, *we have* $\mathcal{F}(1+\mathfrak{M}_{X_1,P_1}) = 1+\mathfrak{M}_{X_2,P_2}$, *where* $P_2 \overset{\text{def}}{=} f(P_1)$. (*Note that we have* $\mathcal{F}(\mathcal{O}_{X_1,P_1}) = \mathcal{O}_{X_2,P_2}$, $\mathcal{F}(\mathcal{O}^{\times}_{X_1,P_1}) = \mathcal{O}^{\times}_{X_2,P_2}$, *and* $\mathcal{F}(\mathfrak{M}_{X_1,P_1}) = \mathfrak{M}_{X_2,P_2}$, *by* (a).)

(c) $\sharp(S_1) \geqslant 3$.

Then $\mathcal{F}\colon K_1 \to K_2$ *is additive.*

We can apply this lemma to $\mathcal{F}\colon K_{1,\bar{\mathcal{H}}_1} \to K_{2,\bar{\mathcal{H}}_2}$, where $\mathcal{H}_1$ is an open subgroup of Π_1 with $n_{\mathcal{H}_1} \geqslant 3$ and $\mathcal{H}_2 = \mathcal{F}(\mathcal{H}_1)$. In fact, (a) follows from the fact that the composite of

$$K^{\times}_{i,\bar{\mathcal{H}}_i} = \varinjlim_{\substack{\bar{\mathcal{H}}_i \subset \mathcal{H}_i' \subset \mathcal{H}_i \\ \text{open}}} F_{i,\mathcal{H}_i'} \to \varinjlim_{\substack{\bar{\mathcal{H}}_i \subset \mathcal{H}_i' \subset \mathcal{H}_i \\ \text{open}}} F_{\mathcal{H}_i', P_{i,\mathcal{H}_i'}}$$

$$\to \varinjlim_{\substack{\bar{\mathcal{H}}_i \subset \mathcal{H}_i' \subset \mathcal{H}_i \\ \text{open}}} F_{i,P_{i,\mathcal{H}_i'}}/\mathrm{Ker}(F_{i,P_{i,\mathcal{H}_i'}} \to G_{k_i}) = \mathbb{Z}$$

coincides with ord_{P_i}. (b) follows from the fact

$$1+\mathfrak{M}_{X_{\bar{\mathcal{H}}_i,P_i}} = \mathrm{Ker}\left(\mathcal{O}^{\times}_{X_{\bar{\mathcal{H}}_i,P_i}} \to \varinjlim_{\substack{\bar{\mathcal{H}}_i \subset \mathcal{H}_i' \subset \mathcal{H}_i \\ \text{open}}} (\mathrm{Ker}(F_{i,P_{i,\mathcal{H}_i'}} \to G_{k_i}))^{p'} = \bar{k}_i^{\times} \right).$$

(c) follows from our assumption. Since, by (1.10),

$$\tilde{K}_i = \bigcup_{\substack{\mathcal{H}_i \subset \Pi_i, n_{\mathcal{H}_i} \geqslant 3 \\ \text{open}}} K_{i,\bar{\mathcal{H}}_i},$$

$\mathcal{F}\colon \tilde{K}_1 \to \tilde{K}_2$ is additive.

Until the end of this section, we concentrate on the proof of (4.7). So we follow the assumptions and the notations in (4.7).

We need the definition of minimal elements in a function field (following [Uchida]) and some lemmas. Uchida uses infinitely many ramified points to prove the additivity, but in the present case, only finitely many ramified points are at our disposal. Here is a difficulty.

Let k be an algebraically closed field, and X a proper, smooth, connected curve of genus g over k. Put $K = k(X)$ and $\Sigma = X(k)$.

DEFINITION (4.8). (i) Let x be an element of $K^{\times}$, and define $(x)_0$ (resp. $(x)_\infty$) to be the numerator (resp. denominator) divisor of x. (Note $(x) = (x)_0 - (x)_\infty$.)

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Then we say that x is *minimal*, if $l((x)_\infty) = 2$. Here, for a divisor D on X, we define $l(D) = \dim_k(\Gamma(X, \mathcal{O}(D)))$.

(ii) Let D be an effective (= non-negative) divisor on X. Then we say that D is *minimal*, if there exists a minimal element $x \in K^\times$ with $(x)_\infty = D$. This is equivalent to: $l(D) = 2$ and $l(D') = 1$ for any effective divisor $D' \precneqq D$.

LEMMA (4.9). *Let x be a minimal element of K and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a matrix in $\mathrm{GL}_2(k)$. Then $(ax+b)/(cx+d)$ is also minimal.*

Proof. This reduces to the following two cases: $c = 0, d = 1$; $a = d = 0, b = c = 1$. The first case is clear, since $(ax+b)_\infty = (x)_\infty$. The second follows from $(x^{-1})_\infty = (x)_0$ and $l((x)_0) = l((x)_\infty)$. □

LEMMA (4.10). *Let D be an effective divisor of degree g with $l(D) = 1$. Then for each $P \in \Sigma$, we have $l(D+P) = 2$. In particular, any element $x \in \Gamma(X, \mathcal{O}(D+P)) - k$ is minimal. (Note: this does not necessarily imply that the divisor $D+P$ is minimal.)*

Proof.

$$2 = \deg(D+P) - g + 1 \overset{\text{Riemann}-\text{Roch}}{\leqslant} l(D+P) \leqslant l(D) + 1 = 2.$$

The second statement follows from the first. □

Let S be a subset of Σ. The following lemmas (4.11) and (4.13) assure that sufficiently many minimal elements exist in K.

LEMMA (4.11). *Let P_0, P_1, P_∞ be distinct points in Σ. Then there exists a minimal element $x \in K$ satisfying $x(P_i) = i$ for each $i \in \{0, 1, \infty\}$.*

Proof. We have the following:

CLAIM (4.12). There exists an effective divisor D of degree g which satisfies: $l(D) = 1$; $l(D + P_\infty - P_0 - P_1) = 0$; and $\mathrm{Supp}(D) \not\ni P_0, P_1$.

If $g = 0$, the divisor $D = 0$ satisfies the conditions. Assume $g > 0$, then such D is 'general'. To be more precise, let J_X^g be the degree g part of the Picard variety of X. (J_X^g is isomorphic to $J_X = J_X^0$, since k is algebraically closed.) Put $X^{(n)} = X^n/\mathfrak{S}_n$ for each $n \geqslant 0$ ($X^{(0)} = \mathrm{Spec}(k)$), and define a morphism $j : X^{(g)} \to J_X^g$ by $(Q_1, \ldots, Q_g) \mapsto Q_1 + \cdots + Q_g$. Then it is well-known that j is birational, hence there exists a non-empty open subset V of J_X^g such that $j\colon j^{-1}(V) \to V$ is an isomorphism. For $i = 0, 1$, define $j_i'\colon X^{(g-1)} \to J_X^g$ by $(Q_1, \ldots, Q_{g-1}) \mapsto Q_1 + \cdots + Q_{g-1} + P_i$, and define $j_2'\colon X^{(g-1)} \to J_X^g$ by $(Q_1, \ldots, Q_{g-1}) \mapsto Q_1 + \cdots + Q_{g-1} + P_0 + P_1 - P_\infty$. Then, for each

$$(Q_1, \ldots, Q_g) \in j^{-1}\left(V - \bigcup_{i=0}^{2} j_i'(X^{(g-1)})\right)(k),$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

the effective divisor $D = Q_1 + \cdots + Q_g$ satisfies the conditions.

Now, choose an effective divisor satisfying the conditions of (4.12). Then, by (4.10), $l(D + P_\infty) = 2$, and any $z \in \Gamma(X, \mathcal{O}(D + P_\infty)) - k$ is minimal. Put $y = z - z(P_0)$. (Note $\mathrm{ord}_{P_0}(z) \geqslant 0$, since $\mathrm{Supp}(D) \not\ni P_0$.) Then $y(P_i) = i$ for $i = 0, \infty$. Suppose $y(P_1) = 0$, then y is a nontrivial element of $\Gamma(X, \mathcal{O}(D + P_\infty - P_0 - P_1))$, which contradicts to the choice of D. Thus we can define

$$x = \frac{y}{y(P_1)},$$

which satisfies $x(P_i) = i$ for $i = 0, 1, \infty$. By (4.9), x is minimal. □

LEMMA (4.13). *Assume* $\sharp(S) \geqslant 2$. *Consider the following conditions for an element* x *in* $K^\times$:

(1) x *is minimal and* $\sharp(\{x(P) \in k \cup \{\infty\} \mid P \in S\}) \geqslant 2$;
(2) x *is minimal and* $\{x(P) \in k \cup \{\infty\} \mid P \in S\} \supset \{0, \infty\}$.

(*Clearly* (2) *implies* (1).) *Then we have*

$$\begin{aligned} K^\times &= \langle x \in K^\times \mid x \textit{ satisfies } (1) \rangle \\ &= \langle k(x)^\times \mid x \textit{ satisfies } (2) \rangle. \end{aligned}$$

Proof. We may assume $\sharp(S) < \infty$, taking a finite subset of S (with cardinality $\geqslant 2$) if necessary. Choosing three distinct points $P_0, P_\infty \in S$ and $P_1 \in \Sigma$, we see, by (4.11), that there exists at least one element $x \in K^\times$ satisfying (2), hence (1). So any constant $c \in k^\times \subset K^\times$ is written as a product of elements satisfying (1): $c = (cx)x^{-1}$.

Now, take any $f \in K^\times$. Then we can write

$$(f) = \sum_{i=1}^{N} (P_i - Q_i),$$

with $\{P_i, Q_i\} \cap S \neq \emptyset$ for each $i = 1, \ldots, N$. In fact, choose $P_0 \in S$, then:

$$\begin{aligned} (f) &= \sum_{i=1}^{n} (P_i' - Q_i'),\ P_i', Q_i' \in \Sigma \\ &= \sum_{i=1}^{n} (P_i' - P_0) + \sum_{i=1}^{n} (P_0 - Q_i'). \end{aligned}$$

Put $S' = \{P_1, \ldots, P_N, Q_1, \ldots, Q_N\} \cup S$, which is a finite subset of Σ.

CLAIM (4.14). There exist effective divisors $D_1, \ldots, D_N, D_{N+1} = D_1$ of degree g which satisfy: $l(D_i) = 1$; $\mathrm{Supp}(D_i) \cap S' = \emptyset$; and $D_i - D_{i+1}$ is linearly equivalent to $P_i - Q_i$, for each $i = 1, \ldots, N$.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Follow the notations in the proof of (4.11). Define a non-empty open subset W of J_X^g by

$$W = V - \bigcup_{Q \in S'} j_Q(X^{(g-1)}),$$

where $j_Q : X^{(g-1)} \to J_X^g$ is defined by $(R_1, \ldots, R_{g-1}) \mapsto R_1 + \cdots + R_{g-1} + Q$. Then for each $(R_1, \ldots, R_g) \in j^{-1}(\bigcap_{m=1}^{N+1}(W + \Sigma_{i=1}^{m-1}(P_i - Q_i)))$, put $D_1 = R_1 + \cdots + R_g$. Define $D_m = R_1^{(m)} + \cdots + R_g^{(m)}$ by $j(R_1^{(m)}, \ldots, R_g^{(m)}) = j(R_1, \ldots, R_g) - \Sigma_{i=1}^{m-1}(P_i - Q_i)$ for $m = 2, \ldots, N+1$. Then all the conditions are satisfied.

Take $D_1, \ldots, D_N, D_{N+1} = D_1$ as in (4.14). There exists $f_i \in K^\times$ satisfying

$$(f_i) = P_i - Q_i + D_{i+1} - D_i,$$

for each $i = 1, \ldots, N$. Then we see

$$(f) = (f_1) + \cdots + (f_N).$$

Hence there exists a constant $c \in k^\times$ such that

$$f = c f_1 \ldots f_N.$$

Now c is a product of elements in $K^\times$ satisfying (1) as we have already seen, and, for each $i = 1, \ldots, N$, either f_i is a constant $\in k^\times$ or f_i satisfies (1). In fact, f_i belongs to $\Gamma(X, \mathcal{O}(D_i + Q_i)) - \{0\}$. Hence f_i is either in $k^\times (\Longleftrightarrow P_i = Q_i)$ or minimal, by (4.10). If f_i is minimal, then we see $f_i(P_i) = 0$ and $f_i(Q_i) = \infty$. Since $f_i(S - \{P_i, Q_i\}) \subset k^\times$, f_i satisfies (1). (Recall $\sharp(S) \geqslant 2$ and $\{P_i, Q_i\} \cap S \neq \emptyset$.) This completes the proof of the first equality.

The second follows from the first, together with (4.9). □

Now turn to the proof of (4.7). First we note that $\mathcal{F}(k_1) = k_2$. In fact, k_i is the set of divisible elements in the multiplicative monoid K_i for each $i = 1, 2$. Consider the following condition

(c′) $\sharp(S_1) \geqslant 2$ and $\mathcal{F}|_{k_1}$ is additive.

We first prove (a)(b)(c) $\Longrightarrow$ (a)(b)(c′).

Let $P_{1,0}, P_{1,1}, P_{1,\infty}$ be distinct points in S_1. By (4.11), there exists a minimal $x_1 \in K_1^\times$ satisfying $x_1(P_{1,i}) = i$ for each $i = 0, 1, \infty$. Then $x_2 \stackrel{\text{def}}{=} \mathcal{F}(x_1)$ is a minimal element in K_2, by the condition (a). (Observe that x_i is minimal in K_i if and only if $\Gamma(X_i, \mathcal{O}((x_i)_\infty)) \supsetneq k_i$ and $\Gamma(X_i, \mathcal{O}(D_i')) = k_i$ for any effective divisor $D_i' \precneqq (x_i)_\infty$ on X_i.) Put $P_{2,i} = f(P_{1,i})$ for each $i = 0, 1, \infty$. Then we have $x_2(P_{2,i}) = i$ for each $i = 0, 1, \infty$. In fact, this follows from the condition (a) (resp. (b)) for $i = 0, \infty$ (resp. $i = 1$).

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Let ξ_1, η_1 be any two elements of k_1, and we shall prove $\mathcal{F}(\xi_1+\eta_1) = \mathcal{F}(\xi_1) + \mathcal{F}(\eta_1)$. Since $\mathcal{F}(0) = 0$ and $\mathcal{F}(-1) = -1$, we may assume $\xi_1 \neq 0$, $\eta_1 \neq 0$, and $\xi_1+\eta_1 \neq 0$. As $\xi_1 x_1 + \eta_1$ is a minimal element in K_1 with $(\xi_1 x_1 + \eta_1)_\infty = (x_1)_\infty$, $\mathcal{F}(\xi_1 x_1 + \eta_1)$ is a minimal element in K_2 with $(\mathcal{F}(\xi_1 x_1 + \eta_1))_\infty = (\mathcal{F}(x_1))_\infty$, by the condition (a). Therefore, there exist $\xi_2, \eta_2 \in k_2$ with $\mathcal{F}(\xi_1 x_1 + \eta_1) = \xi_2 \mathcal{F}(x_1) + \eta_2$. Considering the images of both sides in $\mathcal{O}^\times_{X_2,P_{2,0}}/(1+\mathfrak{M}_{X_2,P_{2,0}}) = k_2^\times$, we have $\mathcal{F}(\eta_1) = \eta_2$. (Use the condition (b).) On the other hand, we have

$$\begin{aligned}\mathcal{F}(\xi_1 + \eta_1 x_1^{-1}) &= \mathcal{F}(\xi_1 x_1 + \eta_1)\mathcal{F}(x_1^{-1}) \\ &= (\xi_2 \mathcal{F}(x_1) + \eta_2)\mathcal{F}(x_1)^{-1} = \xi_2 + \eta_2 \mathcal{F}(x_1)^{-1}.\end{aligned}$$

Considering the images of both sides in $\mathcal{O}^\times_{X_2,P_{2,\infty}}/(1+\mathfrak{M}_{X_2,P_{2,\infty}}) = k_2^\times$, we have $\mathcal{F}(\xi_1) = \xi_2$. Finally, considering the images of both sides of $\mathcal{F}(\xi_1 x_1 + \eta_1) = \xi_2 \mathcal{F}(x_1) + \eta_2$ in $\mathcal{O}^\times_{X_2,P_{2,1}}/(1+\mathfrak{M}_{X_2,P_{2,1}}) = k_2^\times$, we obtain

$$\mathcal{F}(\xi_1 + \eta_1) = \xi_2 + \eta_2 = \mathcal{F}(\xi_1) + \mathcal{F}(\eta_1).$$

Next we prove that (a)(b)(c′) implies the additivity of $\mathcal{F}$.

CLAIM (4.15). Let x_1 be any minimal element in K_1 satisfying $\{x_1(P_1) \in k \cup \{\infty\} \mid P_1 \in S_1\} \supset \{0, \infty\}$. Then $\mathcal{F}|_{k_1(x_1)}$ is additive, and $\mathcal{F}(k_1(x_1)) = k_2(\mathcal{F}(x_1))$.

In fact, we have $\mathcal{F}(\xi_1 x_1 + \eta_1) = \mathcal{F}(\xi_1)\mathcal{F}(x_1) + \mathcal{F}(\eta_1)$ for each $\xi_1, \eta_1 \in k_1$, just as above. Thereby we obtain

$$\mathcal{F}\left(\gamma_1 \frac{\Pi_i (x_1 - \alpha_{1,i})}{\Pi_j (x_1 - \beta_{1,j})}\right) = \mathcal{F}(\gamma_1) \frac{\Pi_i (\mathcal{F}(x_1) - \mathcal{F}(\alpha_{1,i}))}{\Pi_j (\mathcal{F}(x_1) - \mathcal{F}(\beta_{1,j}))}.$$

From this and the additivity of $\mathcal{F}|_{k_1}$, we can easily deduce the additivity of $\mathcal{F}|_{k_1(x_1)}$. The second statement follows from the first and the fact $\mathcal{F}(k_1) = k_2$.

Now, (4.15) together with (4.13) reduces the problem to the following lemma. (Identify k_1 with $k_2 = \mathcal{F}(k_1)$ via $\mathcal{F}$.)

LEMMA (4.16). *Let k be an algebraically closed field, and X and Y integral schemes separated of finite type over k. Let ϕ: $k(Y) \to k(X)$ and f: $\Sigma_X \to \Sigma_Y$ (or, equivalently, f: $X(k) \to Y(k)$) be (set-theoretical) maps. Assume the following*:

(a) $\phi|_k = \mathrm{id}_k$.
(b) *f is continuous and dominating in Zariski topology.*
(c) $\phi^{-1}(\mathfrak{M}_{X,x}) \cap \mathcal{O}_{Y,f(x)} = \mathfrak{M}_{Y,f(x)}$ *for each closed point x of X.*

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Assume moreover that we are given a family $\{L_\lambda\}_{\lambda\in\Lambda}$ *of subfields of* $k(Y)$ *containing* k *such that*

(d) $\phi|_{L_\lambda}: L_\lambda \to k(X)$ *is a ring homomorphism for each* $\lambda \in \Lambda$.

(i) *Assume that* $k(Y)$ *is generated by* L_λ *(*$\lambda \in \Lambda$*) as a field. Then, there exists a unique* k*-algebra homomorphism* $\psi: k(Y) \to k(X)$ *such that*

(A) $\psi|_{L_\lambda} = \phi|_{L_\lambda}$ *for each* $\lambda \in \Lambda$.

(B) *There exists a non-empty affine open subscheme* U *of* X *on which* g_ψ *is defined as a morphism:* $U \to Y$ *such that* f *and* g_ψ *coincide with each other on* $U(k)$. *Here* g_ψ *is the dominating rational map* $X \rightsquigarrow Y$ *defined by the field homomorphism* $\psi: k(Y) \to k(X)$.

(ii) *Assume that* ϕ *is a homomorphism of multiplicative monoids and that* $k(Y)$ *is generated by* $L_\lambda(\lambda \in \Lambda)$ *as a multiplicative monoid. Then* ψ *in* (i) *coincides with* ϕ, g_ψ *is defined as a morphism everywhere on* X, *and* f *and* g_ψ *coincide with each other on* $X(k)$.

In particular, ϕ *is then additive.*

Proof. (i) The uniqueness immediately follows from (A) or (B).

Assume first that Λ is a finite set. For each $\lambda \in \Lambda$, choose a finitely generated k-subalgebra B_λ of L_λ whose fractional field is L_λ. (Note that L_λ/k is finitely generated field, as $k(Y)/k$ is finitely generated.) Put $B = k[B_\lambda]_{\lambda\in\Lambda}$, whose fractional field is $k(Y)$ by the assumption. Since Y and $\mathrm{Spec}(B)$ are integral schemes of finite type over k whose function field is the same field $k(Y)$, there exists a common non-empty affine open subscheme $\mathrm{Spec}(B')$ of Y and $\mathrm{Spec}(B)$. Then, since f is Zariski continuous, there exists a non-empty affine open subscheme $\mathrm{Spec}(A)$ of X, such that the image of $\mathrm{Spec}(A)(k) \subset X(k)$ by f is contained in $\mathrm{Spec}(B')(k) \subset Y(k)$. Put $A' = A[\phi(B_\lambda)]_{\lambda\in\Lambda}$. Since $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A')$ are integral schemes of finite type over k whose function field is the same field $k(X)$, there exists a common non-empty affine open subscheme $U = \mathrm{Spec}(A'')$ of $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A')$. Let $\tilde{\psi}$ be a k-algebra homomorphism

$$\bigotimes_{\substack{k\\ \lambda\in\Lambda}} B_\lambda \to A'$$

defined by $\tilde{\psi}(\otimes b_\lambda) = \prod \phi(b_\lambda)$.

CLAIM (4.17). The following diagram (of sets) is commutative

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

$$\begin{array}{ccc}
\Sigma_{\mathrm{Spec}(A)} & \xrightarrow{f} & \Sigma_{\mathrm{Spec}(B')} \\
\bigcup & & \bigcap \\
\Sigma_U & & \mathrm{Spec}(B') \\
\bigcap & & \bigcap \\
U & & \mathrm{Spec}(B) \\
\bigcap & & \downarrow (*) \\
\mathrm{Spec}(A') & \xrightarrow{\tilde{\psi}^a} & \mathrm{Spec}\left(\bigotimes_{\substack{k \\ \lambda\in\Lambda}} B_\lambda\right),
\end{array}$$

where $(*)$ is the closed immersion associated with

$$\bigotimes_{\substack{k \\ \lambda\in\Lambda}} B_\lambda \twoheadrightarrow B, \otimes b_\lambda \mapsto \prod b_\lambda.$$

Since the diagram starts from Σ_U, it suffices to check the commutativity restricting everything to the set of its closed points or, equivalently, its k-rational points. Since

$$\mathrm{Spec}\left(\bigotimes_{\substack{k \\ \lambda\in\Lambda}} B_\lambda\right)(k) = \prod_{\lambda\in\Lambda} \mathrm{Spec}(B_\lambda)(k),$$

we only have to check the commutativity of the following:

$$\begin{array}{ccc}
\Sigma_{\mathrm{Spec}(A)} & \xrightarrow{f} & \Sigma_{\mathrm{Spec}(B')} \\
\bigcup & & \bigcap \\
\Sigma_U & & \Sigma_{\mathrm{Spec}(B)} \\
\bigcap & & \downarrow \\
\Sigma_{\mathrm{Spec}(A')} & \xrightarrow{\phi^a} & \Sigma_{\mathrm{Spec}(B_\lambda)},
\end{array}$$

for each $\lambda \in \Lambda$. Now, take any $x \in \Sigma_U$. Then the commutativity follows from the following equalities:

$$\begin{aligned}
\phi^{-1}(\mathfrak{M}_{U,x} \cap A') \cap B_\lambda &= \phi^{-1}(\mathfrak{M}_{U,x}) \cap B_\lambda \\
&= \phi^{-1}(\mathfrak{M}_{U,x}) \cap \mathcal{O}_{\mathrm{Spec}(B'),f(x)} \cap B_\lambda \\
&\overset{(c)}{=} \mathfrak{M}_{\mathrm{Spec}(B'),f(x)} \cap B_\lambda \\
&= (\mathfrak{M}_{\mathrm{Spec}(B'),f(x)} \cap B') \cap B_\lambda.
\end{aligned}$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

By (4.17), the morphism

$$\mathrm{Spec}\left(\bigotimes_{\substack{k\\ \lambda\in\Lambda}} B_\lambda\right)$$

associated with $\tilde{\psi}$ maps Σ_U into the subscheme $\mathrm{Spec}(B')$ of $\mathrm{Spec}\left(\bigotimes_{\substack{k\\ \lambda\in\Lambda}} B_\lambda\right)$. Recall

$$\mathrm{Spec}(B') \underset{\text{open}}{\subset} \mathrm{Spec}(B) \underset{\text{closed}}{\subset} \mathrm{Spec}\left(\bigotimes_{\substack{k\\ \lambda\in\Lambda}} B_\lambda\right).$$

Therefore it induces a morphism $U \to \mathrm{Spec}(B')$. Composing this with $\mathrm{Spec}(B') \hookrightarrow Y$, we obtain a morphism $g\colon U \to Y$. By definition and (4.17), g coincides with f on $U(k)$. Since f is dominating, so is g. Hence we can associate a field inclusion $\psi\colon k(Y) \to k(U) = k(X)$ with g. ($g_\psi = g$ by definition.) Now, we have two ring homomorphisms ψ and $\phi\colon L_\lambda \to k(X)$. Since $\psi|_{B_\lambda} = \tilde{\psi}|_{B_\lambda} = \phi|_{B_\lambda}$, these coincide with each other. From this, we also see that ψ is a k-homomorphism.

For general Λ, we can take a finite subset Λ' such that $k(Y)$ is generated by L_λ ($\lambda \in \Lambda'$). From the preceding arguments we can associate $\psi_{\Lambda'}\colon k(Y) \to k(X)$. If Λ'' is another such subset of Λ, we see $\psi_{\Lambda'} = \psi_{\Lambda'\cup\Lambda''} = \psi_{\Lambda''}$, using the uniqueness. This settles the general case.

(ii) For each $b \in k(Y)$, we can write $b = b_{\lambda_1}\cdots b_{\lambda_N}$, ($\lambda_i \in \Lambda$, $b_{\lambda_i} \in L_{\lambda_i}$). Then we have

$$\psi(b) = \psi(b_{\lambda_1})\cdots\psi(b_{\lambda_N}) = \phi(b_{\lambda_1})\cdots\phi(b_{\lambda_N}) = \phi(b).$$

In particular, ϕ is a ring homomorphism. Now, for each $x \in \Sigma_X$, we have

$$\begin{aligned}\phi(\mathcal{O}_{Y,f(x)}) &= \phi(k + \mathfrak{M}_{Y,f(x)})\\ &= \phi(k) + \phi(\mathfrak{M}_{Y,f(x)}) \subset k + \mathfrak{M}_{X,x} = \mathcal{O}_{X,x}.\end{aligned}$$

Therefore, for each open subset V of Y, we obtain a ring homomorphism

$$\Gamma(V,\mathcal{O}_Y) = \bigcap_{y\in\Sigma_V} \mathcal{O}_{Y,y} \to \bigcap_{x\in\Sigma_{f^{-1}(V)}} \mathcal{O}_{X,x} = \Gamma(f^{-1}(V),\mathcal{O}_X),$$

where $f^{-1}(V)$ is the unique open subset of X satisfying $\Sigma_{f^{-1}(V)} = f^{-1}(\Sigma_V)$. This gives a morphism $X \to Y$, which coincides with f on Σ_X and which induces $\phi = \psi\colon k(Y) \to k(X)$. □

5. The fundamental groups of curves over local fields

In the next section, we reduce the Grothendieck conjecture for curves over fields finitely generated over $\mathbb{Q}$ to the Grothendieck conjecture for curves over finite fields,

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

which is already proved in affine cases in the previous section. For this, given a curve over a discrete valuation field, we have to recover the tame fundamental group of the reduction of the curve from the (tame) fundamental group of the curve itself. This is the main goal of this section. We solve this problem by relating it to a criterion for good reduction of a curve over a discrete valuation field.

The notation in this section is partially independent of that of the other sections. Let S be the spectrum of a discrete valuation ring R, η the generic point of S, s the closed point of S, $K = \kappa(\eta)$ the fractional field of R, and $k = \kappa(s)$ the residue field of R. Let $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $I \subset G$ the inertia group at s (determined up to conjugacy). Put $p = \mathrm{char}(k)(\geqslant 0)$, the residue characteristic of R. For a proper, smooth K-scheme X, we say that X has good reduction at s, if there exists a proper, smooth S-scheme $\mathfrak{X}$ whose generic fiber $\mathfrak{X}_\eta$ is isomorphic to X over K. For X an abelian variety, the following criterion for good reduction is well-known.

THEOREM (Néron–Ogg–Shafarevich–Serre–Tate). *Let X be an abelian variety over K. Then X has good reduction at s if and only if I acts trivially on the l-adic Tate module $T(X)^l$ for some (or, equivalently, all) prime number $l \neq p$.* □

On the other hand, when X is a proper, smooth, geometrically connected curve, the following criterion for good reduction and its proof has been given by Takayuki Oda ([Oda 1], [Oda 2]). (He states his theorem only when S is a localization or a completion of the integer ring of an algebraic number field.)

THEOREM (Oda). *Let X be a proper, smooth, geometrically connected curve of genus $\geqslant 2$ over K. Then X has good reduction at s if and only if the image of I in $\mathrm{Out}(\pi_1(X_{K^{\mathrm{sep}}}, *)^l)$ is trivial for some (or all) prime number $l \neq p$.* □

(In this section, we do not have to specify the geometric point $*$.)

This theorem now can be regarded as a corollary of deep results by Asada–Matsumoto–Oda ([AMO]) on the universal local monodromy, which are based on transcendental and topological methods. In this section, we generalize Oda's theorem for not necessarily proper curves by 'algebraic' methods.

From now on, X always denotes a proper, smooth, geometrically connected curve over K, and D denotes a relatively étale effective divisor in X/K. Note that, when $\mathrm{char}(K) = 0$, a relatively étale divisor in X/K is just a reduced (effective) divisor in X/K. Put $U = X - D$. The divisor D is uniquely determined by U.

DEFINITION (5.1). We say that (X, D) *has good reduction at s*, if there exist a proper, smooth S-scheme $\mathfrak{X}$ and a relatively étale divisor $\mathfrak{D}$ in $\mathfrak{X}/S$ whose generic fiber $(\mathfrak{X}_\eta, \mathfrak{D}_\eta)$ is isomorphic to (X, D) over K. We refer such an $(\mathfrak{X}, \mathfrak{D})$ as a smooth model of (X, D).

Let g be the genus of the curve X and n the number of $D(\bar{K}) = D(K^{\mathrm{sep}})$.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Remark (5.2). The smooth model $(\mathfrak{X}, \mathfrak{D})$ is unique if $2-2g-n<0$. This follows, for example, from the uniqueness of the stable model. (See [DM], [Knudsen].)

Now our criterion for good reduction of X is given as follows:

THEOREM (5.3). *Assume* $2-2g-n<0$. *Then the following conditions are all equivalent:*

(a) (X, D) *has good reduction at* s.
(b) *The image of* I *in* $\mathrm{Out}(\pi_1(U_{K^{\mathrm{sep}}}, *)^{p'})$ *is trivial.*
(c) *For each prime number* $l \neq p$, *the image of* I *in* $\mathrm{Out}(\pi_1(U_{K^{\mathrm{sep}}}, *)^{l})$ *is trivial.*
(d) *There exists a prime number* $l \neq p$, *such that the image of* I *in* $\mathrm{Out}(\pi_1(U_{K^{\mathrm{sep}}}, *)^{l})$ *is trivial.*

Proof. The implication (a)⇒(b) follows from [SGA, Exp. XIII], and the implications (b)⇒(c)⇒(d) are trivial. We shall concentrate on the proof of (d)⇒(a). By descent theory, we can easily reduce the problem to the case where R is strictly henselian, hence $G=I$.

We denote $\pi_1(U, *)$ (resp. $\pi_1(U_{K^{\mathrm{sep}}}, *)$) by Π (resp. $\overline{\Pi}$). By (1-3) and (1-5), we have:

$$\begin{cases} (\overline{\Pi}^l)^{\mathrm{ab}} \simeq T(J_X)^l, & n=0, \\ 0 \to \mathbb{Z}_l(1) \to \mathbb{Z}[D(K^{\mathrm{sep}})] \bigotimes_{\mathbb{Z}} \mathbb{Z}_l(1) \to (\overline{\Pi}^l)^{\mathrm{ab}} & \\ \quad \to T(J_X)^l \to 0 \ (\text{exact}), & n>0. \end{cases}$$

Since I acts trivially on $(\overline{\Pi}^l)^{\mathrm{ab}}$, we see that it also acts trivially both on $D(K^{\mathrm{sep}})$ and on $T(J_X)^l$. The former means $D(K^{\mathrm{sep}}) = D(K)$ and the latter implies the jacobian variety J_X has good reduction at s. In particular, (X, D) admits a stable model. Since stable models are preserved by any base change, we may and do assume that the residue field k is algebraically closed. After blowing-up the stable model, we obtain a regular semi-stable model $(\mathfrak{X}, \mathfrak{D})$. Namely, $\mathfrak{X}$ is a proper, flat, regular S-scheme whose special fiber $\mathfrak{X}_s$ is a (reduced) normal crossing divisor of $\mathfrak{X}$, $\mathfrak{D}$ is a relatively étale divisor in $\mathfrak{X}/S$, and the generic fiber $(\mathfrak{X}_\eta, \mathfrak{D}_\eta)$ is identified with (X, D). We may and do assume that the number of the irreducible components of $\mathfrak{X}_s$ is minimal. Then there are no irreducible component of $\mathfrak{X}_s$, isomorphic to $\mathbb{P}^1_k$, which meets only one other component and contains not more than one point of $\mathfrak{D}_s$.

Let Γ be the dual graph attached to the semi-stable curve $\mathfrak{X}_s$. (See [DM].) Since J_X has good reduction, we have $H^1(\Gamma, \mathbb{Z}) = 0$, i.e. Γ is a tree. (Note that $\mathfrak{X}_s$ is connected.)

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Now consider the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{\Pi}^l & \longrightarrow & \Pi^{(l)} & \longrightarrow & I & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle 1} & & \\ 1 & \longrightarrow & \mathrm{Inn}(\overline{\Pi}^l) & \longrightarrow & \mathrm{Aut}(\overline{\Pi}^l) & \longrightarrow & \mathrm{Out}(\overline{\Pi}^l) & \longrightarrow & 1, \end{array}$$

where the rows are exact. Note that $\overline{\Pi}^l$ is center-free (1.11). From this we can identify I with the subgroup $J = \mathrm{Ker}(\Pi^{(l)} \to \mathrm{Aut}(\overline{\Pi}^l))$ of $\Pi^{(l)}$, and we have $\Pi^{(l)} = \overline{\Pi}^l \times J$ canonically.

Now let $\mathcal{H}$ be an open subgroup of $\Pi^{(l)}$, V the étale covering of U corresponding to $\mathcal{H}$, Y the normalization of X in U, which is the smooth compactification of V/K. Put $E = Y - V$, which is regarded as a reduced divisor on Y. Assume that the map $\mathcal{H} \subset \Pi^{(l)} \to I$ is surjective. Then the following (1)–(5) are all equivalent.

(1) Y has a regular semi-stable model and the dual graph of any such model is a tree, and $E(\bar{K}) = E(K)$.
(2) Y has a regular semi-stable model, and $E(\bar{K}) = E(K)$.
(3) The image of I in $\mathrm{Out}(\bar{\mathcal{H}})$ is trivial, where $\bar{\mathcal{H}} \stackrel{\mathrm{def}}{=} \mathcal{H} \cap \overline{\Pi}^l$.
(4) $\mathcal{H} = \bar{\mathcal{H}} \times J$.
(5) $\mathcal{H} \supset J$.

In fact, (1)⇒(2) is clear. The image of I in $\mathrm{Out}(\bar{\mathcal{H}})$ is finite, since the image of $\mathcal{H} \cap J$ in I is an open subgroup of I. Thus, to show (2)⇒(3), it suffices to prove that the image of I in $\mathrm{Aut}(\bar{\mathcal{H}}^{\mathrm{ab}})$ is trivial, since the kernel of $\mathrm{Out}(\bar{\mathcal{H}}) \to \mathrm{Aut}(\bar{\mathcal{H}}^{\mathrm{ab}})$ is torsion-free ([AK], [Kaneko], [Asada], [NT]). Now the condition (2) implies that the image of I in $\mathrm{Aut}(\bar{\mathcal{H}}^{\mathrm{ab}})$ is unipotent, hence is trivial since it is finite. Thus (2)⇒(3). As we have already seen, the condition (3) implies that $\mathcal{H}$ can be written as $\bar{\mathcal{H}} \times J'$ for some subgroup J' of $\mathcal{H}$ which is isomorphically mapped onto I. Now, by the center-freeness (1.11) of $\bar{\mathcal{H}}$ and the torsion-freeness (1.6) for $\overline{\Pi}^l$, we see that the centralizer of $\bar{\mathcal{H}}$ in $\overline{\Pi}^l$ is trivial. (See the proof of (1.8)(ii).) So J' should coincide with J. Thus (3) ⇒ (4). (4) ⇒ (5) is clear. The condition (5) implies (3) and the fact that E is étale over K. (For the latter, observe that the Galois closure of the covering Y/X has l-th power degree.) So, as we have already seen, (1) follows.

Now, by [SGA, Exp. XIII], we have $\pi_1^{\mathrm{tame}}(\mathfrak{U}_s, *) \simeq \pi_1^{\mathrm{tame}}(\mathfrak{U}, *)$, which is identified with a quotient of $\pi_1^{\mathrm{tame}}(U_{K^{\mathrm{sep}}}, *)$. Here we put $\mathfrak{U} = \mathfrak{X} - \mathfrak{D}$. In particular, we have

$$\overline{\Pi}^l \twoheadrightarrow \pi_1(\mathfrak{U}, *)^l \simeq \pi_1(\mathfrak{U}_s, *)^l.$$

Define N to be the kernel of $\Pi^{(l)} \twoheadrightarrow \pi_1(\mathfrak{U}, *)^l$, then for each open subgroup $\mathcal{H}$ of Π containing N satisfies the condition (2) above. (It immediately follows from Abhyankar's lemma.) Thus it satisfies (5). Since N is the intersection of open subgroups, we see $N \supset J$.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

From now on, our argument is essentially due to Mochizuki. Let $\{Z_i \mid i = 1, \ldots, r\}$ be the set of irreducible components in $\mathfrak{X}_s$, and put $W_i = Z_i - \mathfrak{D}_s$. Since the dual graph Γ of $\mathfrak{X}_s$ is a tree, we see:

$$(\pi_1(\mathfrak{U}_s, *)^l)^{\mathrm{ab}} \simeq \prod_{i=1}^{r} (\pi_1(W_i, *)^l)^{\mathrm{ab}}.$$

We may assume that for $i = 1, \ldots, r'$ we have $W_i \not\simeq \mathbb{P}^1_k, \mathbb{A}^1_k$ ($\Longleftrightarrow (\pi_1(W_i, *)^l)^{\mathrm{ab}} \neq \{1\}$) and for $i = r'+1, \ldots, r$ we have $W_i \simeq \mathbb{P}^1_k$ or $\mathbb{A}^1_k$ ($\Longleftrightarrow (\pi_1(W_i, *)^l)^{\mathrm{ab}} = \{1\}$). Then we can easily construct a quotient of $(\pi_1(\mathfrak{U}_s, *)^l)^{\mathrm{ab}}$, isomorphic to $\mathbb{Z}/l\mathbb{Z}$, such that $(\pi_1(W_i, *)^l)^{\mathrm{ab}}$ is surjectively mapped onto the quotient for each $i = 1, \ldots, r'$. Easy calculation shows that, for the covering corresponding to this quotient, the number of the components is $r' + l(r - r')$ and the number of the singular points is $l(r-1)$. Since its dual graph is a tree by (1), we should have

$$r' + l(r - r') = l(r - 1) + 1,$$

which implies $r' = 1$. Since Γ is a tree, this, together with the minimality, implies $r = 1$. (Observe that, if $r > 1$, then the number of the irreducible components which meet only one other component is also greater than one.) Namely, $(\mathfrak{X}, \mathfrak{D})$ is a smooth model! □

Remark (5.4). By [AK], [Kaneko], [Asada], [NT], we have the weight filtration of $\pi_1(U_{K^{\mathrm{sep}}}, *)^l$, which induces the weight filtration of I:

$$I \supset I(1) \supset I(2) \supset \cdots \supset I(\infty).$$

Here $I/I(1)$ is isomorphic to a subgroup of $GSp_{2g}(\mathbb{Z}_l) \times S_n$, and, for $i \geqslant 1$, $\mathrm{gr}^i(I) = I(i)/I(i+1)$ is a free $\mathbb{Z}_l$-module of rank $\leqslant 1$. Then one (and only one) of the following occurs

(i) $I \supsetneq I(1) = I(\infty)$, $I/I(1)$: infinite;
(ii) $I \supsetneq I(1) = I(2) \supsetneq I(3) = I(\infty)$, $I/I(1)$: finite, $I(2)/I(3) \simeq \mathbb{Z}_l$;
(iii) $I \supsetneq I(1) = I(\infty)$, $I/I(1)$: finite;
(iv) $I = I(1) = I(2) \supsetneq I(3) = I(\infty)$, $I(2)/I(3) \simeq \mathbb{Z}_l$;
(v) $I = I(\infty)$.

In each case, the reduction at s of the jacobian variety J_X of X and that of (X, D) are as follows:

(i) Both J_X and (X, D) have essentially bad reduction;
(ii) J_X has potentially good reduction, (X, D) has essentially bad reduction, and either J_X has bad reduction or $D(\bar{K}) \supsetneq D(\bar{K}^I)$;
(iii) Both J_X and (X, D) have potentially good reduction, and either J_X has bad reduction or $D(\bar{K}) \supsetneq D(\bar{K}^I)$;

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

(iv) J_X has good reduction, $D(\bar{K}) = D(\bar{K}^I)$, and (X, D) has essentially bad reduction;

(v) Both J_X and (X, D) have good reduction.

Here 'having bad reduction' (resp. 'having essentially bad reduction') means 'not having good reduction' (resp. 'not having potentially good reduction').

We can prove these facts by using Frobenius weights. (Take a model of (X, D) over a subfield of K which is finitely generated over the prime field.) But we omit this proof, since we will not use this fact later.

The following is the key lemma for our group-theoretical recovery of the tame fundamental group of the special fiber.

LEMMA (5.5). *Assume* $2 - 2g - n < 0$. *Assume that* R *is strictly henselian. Let* V *be a connected Galois étale covering of* U*, at most tamely ramified along* D*, and* Y *its compactification. Put* $E = Y - V$*, which we regard as a reduced divisor of* Y*. Then the following are equivalent:*

(i) (X, D) *has good reduction at* s *and* V/U *extends to an étale covering of* $\mathfrak{U}$*, at most tamely ramified along* $\mathfrak{D}$*, where* $(\mathfrak{X}, \mathfrak{D})$ *is a smooth model of* (X, D) *and* $\mathfrak{U} = \mathfrak{X} - \mathfrak{D}$.

(ii) *Both* (Y, E) *and* (X, D) *have good reduction at* s.

(ii′) (Y, E) *has good reduction at* s.

(*When we say that* (Y, E) *has good reduction, we require that the constant field of* Y *is* K.)

Proof. (i)⇒(ii) immediately follows from Abhyankar's lemma and (ii)⇒(ii′) is clear.

Prove (ii′)⇒(ii). Let $(\mathfrak{Y}, \mathfrak{E})$ be the smooth model of (Y, E). The uniqueness implies that the action of $G \overset{\text{def}}{=} \mathrm{Aut}(Y/X)$ on (Y, E) extends to that on $(\mathfrak{Y}, \mathfrak{E})$. Since $\mathfrak{Y}$ is projective over S ([Lichtenbaum, Theorem 2.8]), the quotient $\mathfrak{Y}/G$ exists, and is (proper) smooth over S by [KM, p. 508 Theorem]. Since $(\mathfrak{Y}/G)_\eta \simeq \mathfrak{Y}_\eta/G = X$, this completes the proof for $n = 0$. For $n > 0$, $\mathfrak{E}$ is a disjoint union of (finite) copies of S: $\mathfrak{E} = \coprod_{\lambda \in \Lambda} S(\Lambda = \pi_0(\mathfrak{E}))$. Let Λ_i $(i = 1, \ldots, r)$ be the G-orbits of Λ, then we see

$$\mathfrak{E}/G = \coprod_{i=1,\ldots,r} S.$$

Now, we claim that $\mathfrak{E}/G \to \mathfrak{Y}/G$ is a closed immersion (which implies that (X, D) has good reduction.) Since $\mathfrak{Y}$ is projective over S, we can easily find out, for each

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

$i = 1, \ldots, r$, a G-stable affine open subset $\mathrm{Spec}(B_i)$ of $\mathfrak{Y}$ containing $\coprod_{\lambda\in\Lambda_i} S$ and not meeting with $\coprod_{\lambda\in\Lambda-\Lambda_i} S$. Then our claim is equivalent to: the homomorphism

$$B_i^G \to \left(\prod_{\lambda\in\Lambda_i} R\right)^G = R,$$

which is induced by the surjective homomorphism $B_i \to \prod_{\lambda\in\Lambda_i} R$ defining the closed subscheme $\mathfrak{E} \cap \mathrm{Spec}(B_i)$, is also surjective. But this is clear because B_i contains R.

Prove (ii)⇒(i). As we have just seen, $(\mathfrak{Y}/G, \mathfrak{E}/G)$ is a smooth model of (X, D). Since a smooth model is unique (5.2), we may identify $(\mathfrak{Y}/G, \mathfrak{E}/G)$ with $(\mathfrak{X}, \mathfrak{D})$. Now, to prove (i), we may and do assume that the finite group $G = \mathrm{Aut}(Y/X)$ is simple, since any finite group is a successive extension of simple groups. (Use also (ii′)⇒(ii) above.) Now, since G is simple, the action of G on $\mathfrak{Y}_s$ is either trivial or faithful. Suppose that it is trivial. Then, by [KM, Theorem A7.2.1], the natural morphism $\mathfrak{Y}_s = \mathfrak{Y}_s/G \to (\mathfrak{Y}/G)_s = \mathfrak{X}_s$ is radicial. Thus $g_Y = g$. Moreover, since $\mathfrak{E}_s$ is the set-theoretical pull-back of $\mathfrak{D}_s$, we also see $n_Y = n$. Now, Hurwitz' formula gives: $(2g_Y - 2 + n_Y) = \sharp(G)(2g - 2 + n)$, which is absurd since $2g - 2 + n > 0$ by assumption. Therefore, the action of G on $\mathfrak{Y}_s$ is faithful. This implies that the covering $\mathfrak{Y}/\mathfrak{X}$ is unramified at the generic point of $\mathfrak{X}_s$. So, by Zariski–Nagata purity, the covering $\mathfrak{V}/\mathfrak{U}$ is étale, where $\mathfrak{V} \overset{\text{def}}{=} \mathfrak{Y} - \mathfrak{E}$. Since V/U is at most tamely ramified along D, $\mathfrak{V}/\mathfrak{U}$ is at most tamely ramified along $\mathfrak{D}$. (Abhyankar's lemma.) This completes the proof. □

Remark (5.6). Even if V/U is not Galois, (ii′)⇒(ii) is still true. In fact, take a prime number $l \neq p$ not dividing the degree of V/U. Then the natural map $\pi_1(V, *)^{(l)} \to \pi_1(U, *)^{(l)}$ is surjective. (Note that the constant field of Y is K.) Then the image of I in $\mathrm{Out}(\pi_1(U_{K^{\mathrm{sep}}}, *)^l)$ is a quotient of that in $\mathrm{Out}(\pi_1(V_{K^{\mathrm{sep}}}, *)^l)$. Now the claim follows from (5.3).

Assume that R is henselian and (X, D) has good reduction at s. Assume $2 - 2g - n < 0$. Let $(\mathfrak{X}, \mathfrak{D})$ be the smooth model of (X, D) and put $\mathfrak{U} = \mathfrak{X} - \mathfrak{D}$. Then by [SGA, Exp. XIII], we have

$$\pi_1^{\mathrm{tame}}(U, *) \twoheadrightarrow \pi_1^{\mathrm{tame}}(\mathfrak{U}, *) \simeq \pi_1^{\mathrm{tame}}(\mathfrak{U}_s, *).$$

The following gives a group-theoretical characterization of the quotient $\pi_1^{\mathrm{tame}}(\mathfrak{U}, *) \simeq \pi_1^{\mathrm{tame}}(\mathfrak{U}_s, *)$ of $\pi_1^{\mathrm{tame}}(U, *)$.

THEOREM (5.7). *Let $\mathcal{H}$ be an open normal subgroup of $\pi_1^{\mathrm{tame}}(U, *)$. Then $\mathcal{H}$ contains the kernel of $\pi_1^{\mathrm{tame}}(U, *) \twoheadrightarrow \pi_1^{\mathrm{tame}}(\mathfrak{U}, *)(\simeq \pi_1^{\mathrm{tame}}(\mathfrak{U}_s, *))$ if and only if the following two conditions hold*

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

(a) *the image of* $\mathcal{H}$ *in* G *contains* I*;*
(b) *the image of* I *in* $\mathrm{Out}(\bar{\mathcal{H}}^{p'})$ *is trivial, where* $\bar{\mathcal{H}} = \mathcal{H} \cap \pi_1(U_{K^{\mathrm{sep}}}, *)$.

Moreover, the kernel coincides with the intersection of all open subgroups $\mathcal{H}$ *satisfying* (a) *and* (b).

Proof. The first statement now follows immediately from (5.3) and (5.5). The second follows from the first. □

6. The Grothendieck conjecture for curves over fields finitely generated over $\mathbb{Q}$

Follow the notation of Section 4 (before (4.3)). The following, which is the absolute version of the Grothendieck conjecture for affine curves over fields finitely generated over $\mathbb{Q}$, is one of the main results in this section.

THEOREM (6.1). *Assume that both* k_1 *and* k_2 *are finitely generated over* $\mathbb{Q}$*, and that* $n_i > 0$ *and* $2 - 2g_i - n_i < 0$ *for some* $i \in \{1, 2\}$.

Then the map

$$\mathrm{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}(\Pi_1, \Pi_2),\ (\tilde{F}, F) \mapsto \tilde{F}(\cdot)\tilde{F}^{-1}$$

is bijective.

Next, we shall formulate a relative version of this theorem. Assume $k_1 = k_2 = k$ and $\bar{k}_1 = \bar{k}_2 = \bar{k}$. Define

$$\begin{aligned}&\mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)\\ &\quad \stackrel{\mathrm{def}}{=} \mathrm{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)\\ &\qquad \cap (\mathrm{Isom}_{(\mathrm{Schemes}/\bar{k})}(\tilde{U}_1, \tilde{U}_2)\ \mathrm{Isom}_{(\mathrm{Schemes}/k)}(U_1, U_2)).\end{aligned}$$

LEMMA (6.2). (i) *The projection*

$$\tilde{p}_{\bar{k}/k} : \mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}_{\bar{k}}(\tilde{U}_1, \tilde{U}_2)$$

is injective.

(ii) *The projection*

$$p_{\bar{k}/k} : \mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}_{k}(U_1, U_2)$$

is surjective, and

$$p^{-1}_{\bar{k}/k} p_{\bar{k}/k}((\tilde{F}, F)) = \tilde{F}\mathrm{Aut}(\tilde{U}_1/\bar{U}_1) = \mathrm{Aut}(\tilde{U}_2/\bar{U}_2)\tilde{F}.$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Proof. (i) directly follows from (4.1)(i). (ii) is easier to see than (4.1)(ii). □

Define also

$$\mathrm{Isom}_{G_k}(\Pi_1,\Pi_2) \overset{\text{def}}{=} \left\{ \mathcal{F} \in \mathrm{Isom}(\Pi_1,\Pi_2) \;\middle|\; \begin{array}{ccc} \Pi_1 & \xrightarrow{\mathcal{F}} & \Pi_2 \\ \downarrow & & \downarrow \\ G_k & = & G_k \end{array} \text{ is commutative} \right\}.$$

Here is a relative version of (6.1):

THEOREM (6.3). *Assume that k is finitely generated over $\mathbb{Q}$, and that $n_i > 0$ and $2 - 2g_i - n_i < 0$ for some $i \in \{1,2\}$.*

Then the map

$$\mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}_{G_k}(\Pi_1,\Pi_2),\ (\tilde{F},F) \mapsto \tilde{F}(\cdot)\tilde{F}^{-1}$$

is bijective.

Remark (6.4). When k is finite, the situation is completely different from (6.3). In fact, in this case, (3.3) and (3.4) imply

$$\mathrm{Isom}_{G_k}(\Pi_1,\Pi_2) = \mathrm{Isom}(\Pi_1,\Pi_2).$$

Pop's theorem [Pop 3], together with (3.2), reduces (6.1) to (6.3). So, we shall prove (6.3). We do this by constructing the inverse map, using the main result (4.3) of Section 4.

Remark (6.5). In the following argument, the assumption $n_i > 0$ is necessary only to apply (4.3). So, if (4.3) is generalized for $n_i = 0$, (6.3) (hence (6.1)) is also generalized for $n_i = 0$.

Take any $\mathcal{F} \in \mathrm{Isom}_{G_k}(\Pi_1,\Pi_2)$. Using the weight of a suitable Frobenius element in G_k, we see $(g_1,n_1) = (g_2,n_2)$, which we denote by (g,n). (See (3.5) and (3.6)(i).)

Let $\mathcal{H}_1$ be an open subgroup of Π_1 with $g_{\mathcal{H}_1} \geqslant 2$, and put $\mathcal{H}_2 = \mathcal{F}(\mathcal{H}_1)$. Note $k_{\mathcal{H}_1} = k_{\mathcal{H}_2}$, which we denote by $k_{\mathcal{H}}$. Assume $g_{\mathcal{H}_1} (= g_{\mathcal{H}_2}) \geqslant 2$. Then we have the following injective maps:

$$\begin{aligned} &\mathrm{Isom}_{k_{\mathcal{H}}}(U_{1,\mathcal{H}_1}, U_{2,\mathcal{H}_2}) \\ &\quad\to \mathrm{Isom}_{k_{\mathcal{H}}}(X_{1,\mathcal{H}_1}, X_{2,\mathcal{H}_2}) \to \mathrm{Isom}_{k_{\mathcal{H}}}(J_{X_{1,\mathcal{H}_1}}, J_{X_{2,\mathcal{H}_2}}) \\ &\quad\to \mathrm{Isom}_{\widehat{\mathbb{Z}}[G_{k_{\mathcal{H}}}]}(T(J_{X_{1,\mathcal{H}_1}}), T(J_{X_{2,\mathcal{H}_2}})) \to \mathrm{Isom}_{\widehat{\mathbb{Z}}}(T(J_{X_{1,\mathcal{H}_1}}), T(J_{X_{2,\mathcal{H}_2}})). \end{aligned}$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Since $\mathcal{F}$ maps $\bar{\mathcal{H}}_1$ onto $\bar{\mathcal{H}}_2$ and $I(\mathcal{H}_1)$ onto $I(\mathcal{H}_2)$ (3.7), $\mathcal{F}$ induces an element of

$$\mathrm{Isom}_{\hat{\mathbb{Z}}}(T(J_{X_{1,\mathcal{H}_1}}), T(J_{X_{2,\mathcal{H}_2}})),$$

which we also denote by $\mathcal{F}$.

CLAIM (6.6). $\mathcal{F}$ belongs to (the injective image of) $\mathrm{Isom}_{k_{\mathcal{H}}}(U_{1,\mathcal{H}_1}, U_{2,\mathcal{H}_2})$.

Assuming this claim, we shall first complete the proof of (6.3).

Let $\mathcal{H}_1' \subset \mathcal{H}_1$ be two open subgroups of Π_1 with $(g_{\mathcal{H}_1'} \geqslant) g_{\mathcal{H}_1} \geqslant 2$, and put $\mathcal{H}_2 = \mathcal{F}(\mathcal{H}_1)$, $\mathcal{H}_2' = \mathcal{F}(\mathcal{H}_1')$. Then the diagram

$$\begin{array}{ccc} U_{1,\mathcal{H}_1'} & \xrightarrow{\mathcal{F}} & U_{2,\mathcal{H}_2'} \\ \downarrow & & \downarrow \\ U_{1,\mathcal{H}_1} & \xrightarrow{\mathcal{F}} & U_{2,\mathcal{H}_2} \end{array}$$

is commutative. This is clear by definition. So, $\mathcal{F}$ defines an element of $\mathrm{Isom}_{\bar{k}}(\tilde{U}_1, \tilde{U}_2)$, which we also denote by $\mathcal{F}$.

LEMMA (6.7). *Π_1 is generated by its open subgroups $\mathcal{H}_1$ with $g_{\mathcal{H}_1} \geqslant 2$.*

Proof. Since k is hilbertian, Π_1 is topologically generated by (geometric) quasi-sections. Hence it suffices to prove that, for each quasi-section $s\colon G_L \to \Pi_1$, where L is a finite extension of k in $\bar{k}$, there exists an open subgroup $\mathcal{H}_1$ with $g_{\mathcal{H}_1} \geqslant 2$ containing $s(G_L)$. Since $\overline{\Pi}_1$ is a finitely generated profinite group, the set of its open (topologically) characteristic subgroups is a fundamental system of neighborhoods at 1. From this it follows that there exists an open characteristic subgroup H_1 of $\overline{\Pi}_1$ with $g_{H_1} \geqslant 2$. (Use (1.10).) Now $\mathcal{H}_1 \overset{\text{def}}{=} H_1 s(G_L)$ satisfies the desired property. This completes the proof. □

By this lemma, the $\bar{k}$-isomorphism $\mathcal{F}\colon \tilde{U}_1 \to \tilde{U}_2$ induces a (unique) k-isomorphism $U_1 \to U_2$. Thus we obtain a map

$$\mathrm{Isom}_{G_k}(\Pi_1, \Pi_2) \to \mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2).$$

From the functorialities it follows that

$$\mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}_{G_k}(\Pi_1, \Pi_2) \to \mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$$

is the identity. We have to prove that

$$\mathrm{Isom}_{G_k}(\Pi_1, \Pi_2) \to \mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}_{G_k}(\Pi_1, \Pi_2)$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

is also the identity. For this it suffices to prove that

$$\mathrm{Isom}_{G_k}(\Pi_1, \Pi_2) \to \mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$$

is injective. Let $\mathcal{F}, \mathcal{F}'$ be elements of $\mathrm{Isom}_{G_k}(\Pi_1, \Pi_2)$ which induce a same element of $\mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2)$. Put $\mathcal{E} = \mathcal{F}'^{-1}\mathcal{F}$, then $\mathcal{E}$ induces the identity in $\mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_1/U_1)$. By the definition of the map, for any open subgroup $\mathcal{H}_1$ of Π_1 with $g_{\mathcal{H}_1} \geqslant 2$, we have $\mathcal{E}(\mathcal{H}_1) = \mathcal{H}_1$. We see that this is true for any open subgroup $\mathcal{H}_1$ of Π_1, applying (6.7) to $U_{1,\mathcal{H}_1}$. Since a closed subgroup is the intersection of open subgroups containing it, this is also true for any closed subgroup $\mathcal{H}_1$ of Π_1. Apply this to the closed subgroup $s(G_L)$ for each quasi-section s: $G_L \to \Pi_1$, then we see that $\mathcal{E}$ fixes each element in $s(G_L)$. (Recall that $\mathcal{E}$ belongs to $\mathrm{Isom}_{G_k}(\Pi_1, \Pi_1)$.) Since Π_1 is topologically generated by quasi-sections, we obtain that $\mathcal{E}$ is the identity.

Now only the claim (6.6) remains. Replacing U_i by $U_{i,\mathcal{H}_i}$ if necessary, we may assume that $\mathcal{H}_1 = \Pi_1$ and $g \geqslant 2$.

First, we treat the case where k is a finite extension of $\mathbb{Q}$. Let O_k be the integer ring of k, and take a non-empty open subscheme T of $\mathrm{Spec}(O_k)$ such that (X_i, S_i) has a smooth model $(\mathfrak{X}_i, \mathfrak{S}_i)$ over T for each $i = 1, 2$. Namely, $\mathfrak{X}_i$ is a smooth proper over T, $\mathfrak{S}_i$ is a relatively étale divisor in $\mathfrak{X}_i/T$, and $(\mathfrak{X}_i \times_T k, \mathfrak{S}_i \times_T k)$ is identified with (X_i, S_i). Then by [DM], $\underline{\mathrm{Isom}}_T(\mathfrak{X}_1, \mathfrak{X}_2)$ is represented by a finite unramified T-scheme. Shrinking T if necessary, we may and do assume that this scheme is finite *étale*.

Now, let $\mathfrak{p}$ be a closed point of T, and $\bar{\mathfrak{p}}$ an extension of $\mathfrak{p}$ in (the integral closure of T in) $\bar{k}$. Put $p_{\mathfrak{p}} = \mathrm{char}(\kappa(\mathfrak{p}))$. Then the decomposition group $G_{\bar{\mathfrak{p}}}$ of $\bar{\mathfrak{p}}$ in G_k is identified with the absolute Galois group of $k_{\mathfrak{p}}^{\mathrm{h}}$, the fractional field of the henselization of $\mathcal{O}_{T,\mathfrak{p}}$, and the inverse image of $G_{\bar{\mathfrak{p}}}$ in Π_i is identified with $\pi_1(U_i \otimes_k k_{\mathfrak{p}}^{\mathrm{h}}, \overline{\overline{\xi}}_i)^{(\mathcal{C})}$. Thus $\mathcal{F}$ induces an element of

$$\mathrm{Isom}_{G_{k_{\mathfrak{p}}^{\mathrm{h}}}}\left(\pi_1\left(U_1 \bigotimes_k k_{\mathfrak{p}}^{\mathrm{h}}, \overline{\overline{\xi}}_1\right)^{(\mathcal{C})}, \pi_1\left(U_2 \bigotimes_k k_{\mathfrak{p}}^{\mathrm{h}}, \overline{\overline{\xi}}_2\right)^{(\mathcal{C})}\right),$$

which induces an element of

$$\mathrm{Isom}\left(\pi_1^{\mathrm{tame}}\left(\mathfrak{U}_1 \underset{T}{\times} \kappa(\mathfrak{p}), *\right)^{(\mathcal{C})}, \pi_1^{\mathrm{tame}}\left(\mathfrak{U}_2 \underset{T}{\times} \kappa(\mathfrak{p}), *\right)^{(\mathcal{C})}\right)$$

by (5.7), where $\mathfrak{U}_i \overset{\mathrm{def}}{=} \mathfrak{X}_i - \mathfrak{S}_i$. By (4.3), the last set is identified with

$$\mathrm{Isom}\left(\left(\mathfrak{U}_1 \underset{T}{\times} \kappa(\mathfrak{p})\right)^{\sim} \Big/ \mathfrak{U}_1 \underset{T}{\times} \kappa(\mathfrak{p}), \left(\mathfrak{U}_2 \underset{T}{\times} \kappa(\mathfrak{p})\right)^{\sim} \Big/ \mathfrak{U}_2 \underset{T}{\times} \kappa(\mathfrak{p})\right).$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

Thus the image of $\mathcal{F}$ in

$$\begin{aligned}&\mathrm{Isom}_{\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}}}(T(J_{X_1})^{p'_{\mathfrak{p}}}, T(J_{X_2})^{p'_{\mathfrak{p}}})\\ &\quad = \mathrm{Isom}_{\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}}}(T(J_{\mathfrak{X}_1\times_T\kappa(\mathfrak{p})})^{p'_{\mathfrak{p}}}, T(J_{\mathfrak{X}_2\times_T\kappa(\mathfrak{p})})^{p'_{\mathfrak{p}}})\end{aligned}$$

is in (the injective image) of

$$\begin{aligned}&\mathrm{Isom}\left(\mathfrak{U}_1\underset{T}{\times}\kappa(\bar{\mathfrak{p}})/\mathfrak{U}_1\underset{T}{\times}\kappa(\mathfrak{p}), \mathfrak{U}_2\underset{T}{\times}\kappa(\bar{\mathfrak{p}})/\mathfrak{U}_2\underset{T}{\times}\kappa(\mathfrak{p})\right)\\ &\quad\subset \mathrm{Isom}\left(\mathfrak{U}_1\underset{T}{\times}\kappa(\bar{\mathfrak{p}}), \mathfrak{U}_2\underset{T}{\times}\kappa(\bar{\mathfrak{p}})\right).\end{aligned}$$

CLAIM (6.8). $\mathcal{F}$ belongs to (the injective image) of

$$\begin{aligned}&\mathrm{Isom}_{\kappa(\mathfrak{p})}\left(\mathfrak{U}_1\underset{T}{\times}\kappa(\mathfrak{p}), \mathfrak{U}_2\underset{T}{\times}\kappa(\mathfrak{p})\right) \hookrightarrow \mathrm{Isom}_{\kappa(\bar{\mathfrak{p}})}\left(\mathfrak{U}_1\underset{T}{\times}\kappa(\bar{\mathfrak{p}}), \mathfrak{U}_2\underset{T}{\times}\kappa(\bar{\mathfrak{p}})\right)\\ &\quad\subset \mathrm{Isom}\left(\mathfrak{U}_1\underset{T}{\times}\kappa(\bar{\mathfrak{p}}), \mathfrak{U}_2\underset{T}{\times}\kappa(\bar{\mathfrak{p}})\right).\end{aligned}$$

In fact, since $\mathcal{F}$ commutes with $\mathrm{Gal}(\kappa(\bar{\mathfrak{p}})/\kappa(\mathfrak{p}))$, it suffices to prove that $\mathcal{F}$ belongs to $\mathrm{Isom}_{\kappa(\bar{\mathfrak{p}})}(\mathfrak{U}_1\times_T\kappa(\bar{\mathfrak{p}}), \mathfrak{U}_2\times_T\kappa(\bar{\mathfrak{p}}))$. By (4.2), $\mathcal{F}$ defines an element $\iota_{\mathfrak{p}}$ of $\mathrm{Aut}(\kappa(\bar{\mathfrak{p}}))$. Then the following diagram is commutative

$$\begin{array}{ccc} T(J_{X_1})^{p'_{\mathfrak{p}}}\times T(J_{X_1})^{p'_{\mathfrak{p}}} & \xrightarrow{\text{Weil pairing}} & \widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}}(1)\\ \downarrow{\scriptstyle \mathcal{F}\times\mathcal{F}} & & \downarrow{\scriptstyle \iota_{\mathfrak{p}}}\\ T(J_{X_2})^{p'_{\mathfrak{p}}}\times T(J_{X_2})^{p'_{\mathfrak{p}}} & \xrightarrow{\text{Weil pairing}} & \widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}}(1). \end{array}$$

Note that this diagram is regarded as one over the global field k. So, if $\mathfrak{q}$ is another closed point of T, then we have $\iota_{\mathfrak{p}} = \iota_{\mathfrak{q}}$ in $\mathrm{Aut}(\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}, p'_{\mathfrak{q}}}(1)) = (\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}, p'_{\mathfrak{q}}})^{\times}$. Now, take two closed points $\mathfrak{q}_1, \mathfrak{q}_2$ of T with $p_{\mathfrak{q}_i} \neq p_{\mathfrak{p}}$ $(i = 1, 2)$ and $p_{\mathfrak{q}_1} \neq p_{\mathfrak{q}_2}$. Then the image of $\iota_{\mathfrak{p}} = \iota_{\mathfrak{q}_i}$ in $(\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}, p'_{\mathfrak{q}_i}})^{\times}$ is in $\langle p_{\mathfrak{p}}\rangle \cap \langle p_{\mathfrak{q}_i}\rangle$, which is $\{1\}$ by a theorem of Chevalley ([Chevalley, Théorème 1]). Thus $\iota_{\mathfrak{p}} \in (\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}})^{\times}$ is trivial. This completes the proof of (6.8).

From now on, our argument originates from a discussion between Mochizuki and the author. Since $\underline{\mathrm{Isom}}_T(\mathfrak{X}_1, \mathfrak{X}_2)$ is finite étale over T, we have

$$\mathrm{Isom}_{\bar{k}}(X_{1,\bar{k}}, X_{2,\bar{k}}) \simeq \mathrm{Isom}_{\kappa(\bar{\mathfrak{p}})}(\mathfrak{X}_1\underset{T}{\times}\kappa(\bar{\mathfrak{p}}), \mathfrak{X}_2\underset{T}{\times}\kappa(\bar{\mathfrak{p}})).$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

So, the image of $\mathcal{F}$ in

$$\begin{aligned}&\mathrm{Isom}_{\kappa(\bar{\mathfrak{p}})}\left(\mathfrak{X}_1 \underset{T}{\times} \kappa(\bar{\mathfrak{p}}), \mathfrak{X}_2 \underset{T}{\times} \kappa(\bar{\mathfrak{p}})\right) \subset \mathrm{Isom}_{\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}}}(T(J_{X_1})^{p'_{\mathfrak{p}}}, T(J_{X_2})^{p'_{\mathfrak{p}}})\\ &\quad = \mathrm{Isom}_{\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}}}(T(J_{\mathfrak{X}_1 \underset{T}{\times} \kappa(\mathfrak{p})})^{p'_{\mathfrak{p}}}, T(J_{\mathfrak{X}_2 \underset{T}{\times} \kappa(\mathfrak{p})})^{p'_{\mathfrak{p}}}),\end{aligned}$$

corresponds to an element $\widetilde{\mathcal{F}}_{\mathfrak{p}}$ of $\mathrm{Isom}_{\bar{k}}(X_{1,\bar{k}}, X_{2,\bar{k}})$.

Take two closed points $\mathfrak{p}$ and $\mathfrak{q}$ of T with $p_{\mathfrak{p}} \neq p_{\mathfrak{q}}$. Considering the injective map

$$\mathrm{Isom}_{\bar{k}}(X_{1,\bar{k}}, X_{2,\bar{k}}) \to \mathrm{Isom}_{\widehat{\mathbb{Z}}^{p'_{\mathfrak{p}}, p'_{\mathfrak{q}}}}(T(J_{X_1})^{p'_{\mathfrak{p}}, p'_{\mathfrak{q}}}, T(J_{X_2})^{p'_{\mathfrak{p}}, p'_{\mathfrak{q}}}),$$

we see $\widetilde{\mathcal{F}}_{\mathfrak{p}} = \widetilde{\mathcal{F}}_{\mathfrak{q}}$ first. Then we see $\mathcal{F} = \widetilde{\mathcal{F}}_{\mathfrak{p}} = \widetilde{\mathcal{F}}_{\mathfrak{q}}$ in $\mathrm{Isom}_{\widehat{\mathbb{Z}}}(T(J_{X_1}), T(J_{X_2}))$. Since $\mathcal{F}$ commutes with G_k, this implies that $\mathcal{F}$ belongs to (the injective image of) $\mathrm{Isom}_k(X_1, X_2) = \mathrm{Isom}_T(\mathfrak{X}_1, \mathfrak{X}_2)$. Moreover, considering reductions at infinitely many closed points in T, we see that $\mathcal{F}$ maps S_1 onto S_2. This completes the proof of (6.6) in the case $[k\colon \mathbb{Q}] < \infty$.

When k is finitely generated over $\mathbb{Q}$ in general, take a smooth, connected scheme $V/\mathbb{Q}$ whose function field is identified with k, such that (X_i, S_i) has a smooth model $(\mathcal{X}_i, \mathcal{S}_i)$ over V for $i = 1, 2$, and such that $\underline{\mathrm{Isom}}_V(\mathcal{X}_1, \mathcal{X}_2)$ is finite étale over V. Then the proof is quite similar as above but much easier: taking *one* closed point P in V and considering the (whole) Tate modules, we see $\mathcal{F} \in \mathrm{Isom}_k(X_1, X_2)$; considering reductions at closed points dense in V, we see $\mathcal{F}(S_1) = S_2$. (Note that the result in Section 5 is not necessary in this step.)

7. Complements

A. *Reformulation of the main results in terms of outer Galois representations.*

Let

$$1 \to \overline{\Pi}_i \to \Pi_i \to G \to 1,$$

be an exact sequence of profinite groups for each $i = 1, 2$. Then, as in (6.3), we define

$$\mathrm{Isom}_G(\Pi_1, \Pi_2) \overset{\text{def}}{=} \left\{ \mathcal{F} \in \mathrm{Isom}(\Pi_1, \Pi_2) \;\middle|\; \begin{array}{ccc} \Pi_1 & \xrightarrow{\mathcal{F}} & \Pi_2 \\ \downarrow & & \downarrow \\ G & = & G \end{array} \text{ is commutative} \right\}.$$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

On the other hand, the exact sequence above induces an outer representation

$$G \to \mathrm{Out}(\overline{\Pi}_i),$$

for each $i = 1, 2$. Then we define

$$\mathrm{Isom}_G^{\mathrm{Out}}(\overline{\Pi}_1, \overline{\Pi}_2) \stackrel{\mathrm{def}}{=} \left\{ \bar{\mathcal{F}} \in \mathrm{Isom}(\overline{\Pi}_1, \overline{\Pi}_2) \;\middle|\; \begin{array}{ccc} G & = & G \\ \downarrow & & \downarrow \\ \mathrm{Out}(\overline{\Pi}_1) & \xrightarrow{\mathrm{Out}(\bar{\mathcal{F}})} & \mathrm{Out}(\overline{\Pi}_2) \end{array} \text{ is commutative} \right\}.$$

Then the restriction gives a map

$$\mathrm{Isom}_G(\Pi_1, \Pi_2) \to \mathrm{Isom}_G^{\mathrm{Out}}(\overline{\Pi}_1, \overline{\Pi}_2).$$

Now the following is a slightly more general than [Nakamura 3, Corollary (1.5.7)].

LEMMA (7.1). *Assume that $\overline{\Pi}_i$ is center-free for some $i = 1, 2$. Then the map above is bijective.*

Proof. If $\overline{\Pi}_1$ and $\overline{\Pi}_2$ are not isomorphic to each other, then the statement is clear. So, we may assume that $\overline{\Pi}_i$ is center-free for *each* $i = 1, 2$.

We shall construct the inverse map. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{\Pi}_i & \longrightarrow & \Pi_i & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Inn}(\overline{\Pi}_i) & \longrightarrow & \mathrm{Aut}(\overline{\Pi}_i) & \longrightarrow & \mathrm{Out}(\overline{\Pi}_i) & \longrightarrow & 1, \end{array}$$

where the rows are exact and the left column is an isomorphism by assumption. Then we see that Π_i is naturally isomorphic to the pull-back:

$$\mathrm{Aut}(\overline{\Pi}_i) \underset{\mathrm{Out}(\overline{\Pi}_i)}{\times} G.$$

Thus, given $\bar{\mathcal{F}} \in \mathrm{Isom}_G^{\mathrm{Out}}(\overline{\Pi}_1, \overline{\Pi}_2)$, we can define $\mathcal{F} \in \mathrm{Isom}(\Pi_1, \Pi_2)$ as

$$\mathrm{Aut}(\bar{\mathcal{F}}) \underset{\mathrm{Out}(\bar{\mathcal{F}})}{\times} \mathrm{id}_G.$$

We can easily check that this gives the desired inverse map. □

Now, by (1.11), we obtain the following reformulation of (6.3).

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

THEOREM (7.2). *Follow the notations in* (6.3). *Then the map*

$$\mathrm{Isom}_{\bar{k}/k}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \to \mathrm{Isom}^{\mathrm{Out}}_{G_k}(\overline{\Pi}_1, \overline{\Pi}_2),\ (\tilde{F}, F) \mapsto \tilde{F}(\cdot)\tilde{F}^{-1}$$

is bijective. □

Remark (7.3). (i) Dividing by $\overline{\Pi}_2$, we also see that the map

$$\mathrm{Isom}_k(U_1, U_2) \to \mathrm{Isom}^{\mathrm{Out}}_{G_k}(\overline{\Pi}_1, \overline{\Pi}_2)/\mathrm{Inn}(\overline{\Pi}_2)$$

is bijective. In particular, if $U_1 = U_2 = U$, then $\mathrm{Aut}_k(U)$ is isomorphically mapped onto the centralizer of the image of G_k in $\mathrm{Out}(\overline{\Pi})$, where $\overline{\Pi} = \overline{\Pi}_1 = \overline{\Pi}_2$.

Note that this formulation is independent of the choices of the geometric points on $\bar{U}_i$ $(i = 1, 2)$.

(ii) Follow the notations and the assumptions in (4.3), and assume $k_1 = k_2 = k$ (finite) and $\bar{k}_1 = \bar{k}_2 = \bar{k}$. In this case, the right reformulations are

$$\mathrm{Isom}(\tilde{U}_1/U_1, \tilde{U}_2/U_2) \simeq \mathrm{Isom}^{\mathrm{Out}}_{G_k}(\overline{\Pi}_1, \overline{\Pi}_2),$$

$$\mathrm{Isom}(\bar{U}_1/U_1, \bar{U}_2/U_2) \simeq \mathrm{Isom}^{\mathrm{Out}}_{G_k}(\overline{\Pi}_1, \overline{\Pi}_2)/\mathrm{Inn}(\overline{\Pi}_2),$$

$$\mathrm{Isom}(U_1, U_2) \simeq \mathrm{Isom}^{\mathrm{Out}}_{G_k}(\overline{\Pi}_1, \overline{\Pi}_2)/\mathrm{Inn}(\Pi_2).$$

See (6.4).

B. *An application to profinite group theory.*

The author does not know if the following purely profinite-group-theoretical corollary of our main results is easily proved (or well-known).

THEOREM (7.4). *Let $\mathcal{C}$ be a full class of finite groups containing $\mathbb{Z}/l\mathbb{Z}$ for all prime number l. Then* $\mathrm{Out}(\widehat{F}_r^{\mathcal{C}})$ *is center-free for each* $r \geqslant 2$.

Proof. Take a field k finitely generated over $\mathbb{Q}$, and a finite extension L/k of degree $r+1$ with $\mathrm{Aut}(L/k) = \{1\}$. (For example, $k = \mathbb{Q}(T_1, \ldots, T_r)$ and $L = k[X]/(X^{r+1} + T_1X^r + \cdots + T_{r-1}X + T_r)$, where $T_1, \ldots, T_r$ are algebraically independent over $\mathbb{Q}$.) Take any closed immersion $\mathrm{Spec}(L) \to \mathbb{P}^1_k$ over $\mathrm{Spec}(k)$ and put $U = \mathbb{P}^1_k - \mathrm{Spec}(L)$. Then we see $\mathrm{Aut}_k(U) = \{1\}$. By (7.3)(i), this means that the centralizer of the image of G_k in $\mathrm{Out}(\pi_1(U_{\bar{k}}, *)^{\mathcal{C}}) \simeq \mathrm{Out}(\widehat{F}_r^{\mathcal{C}})$ is trivial. In particular, $\mathrm{Out}(\widehat{F}_r^{\mathcal{C}})$ is center-free. □

C. *An alternative proof of a theorem of Pop.*

The following is part of the main result of [Pop 2]. (See also [Pop 1], [Pop 3], and [Spiess].)

THEOREM (Pop). *Let k be a field finitely generated over $\mathbb{Q}$, and X_i a proper, smooth, geometrically connected curve over k for each $i = 1, 2$. Then we have*

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

$$\begin{aligned}&\mathrm{Isom}_k(\mathrm{Spec}(k(X_1)), \mathrm{Spec}(k(X_2)))\\ &\quad\simeq \mathrm{Isom}_{G_k}(G_{k(X_1)}, G_{k(X_2)})/\mathrm{Inn}(G_{\bar{k}(X_2)})\\ &(\simeq \mathrm{Isom}^{\mathrm{Out}}_{G_k}(G_{\bar{k}(X_1)}, G_{\bar{k}(X_2)})/\mathrm{Inn}(G_{\bar{k}(X_2)}).)\end{aligned}$$

We shall prove this as a corollary of our main result (6.3).

Let X be a proper, smooth, geometrically connected curve over k and $\overset{\approx}{X}$ the integral closure of X in a fixed algebraic closure $\overline{k(X)}$ of $\bar{k}(X)$. Then we have

$$G_{k(X)} = \varprojlim_U \pi_1(U, \overline{\overline{\xi}}),$$

$$G_{\bar{k}(X)} = \varprojlim_U \pi_1(\bar{U}, \overline{\overline{\xi}}),$$

where U runs over the set of (non-empty) open affine hyperbolic subscheme of X and $\overline{\overline{\xi}}$ means the generic geometric points defined by $\overline{k(X)}$.

For each $\overset{\approx}{v} \in \Sigma_{\overset{\approx}{X}}$, the decomposition group $D_{\overset{\approx}{v}}$ and the inertia group $I_{\overset{\approx}{v}}$ are defined as usual. We need a group-theoretical characterization of inertia groups. This is a special case of Pop's local theory in [Pop 2]. However, in the case of curves, we have much simpler solution, as follows, using Nakamura's weight characterization of inertia groups ([Nakamura 1, Section 3], [Nakamura 3, 2.1]), which is independent of model theory.

First we recall Nakamura's result briefly. (Although he treats only the case where k is a number field, it clearly extends to the case where k is finitely generated over $\mathbb{Q}$.) Let U be an affine, smooth, geometrically connected curve over k with hyperbolicity condition: $2-2g-n<0$. Follow the notations of Section 1. Then:

THEOREM (Nakamura). *A cyclic* $(=$ *topologically generated by one element*$)$ *subgroup* J *of* $\pi_1(\bar{U}, \overline{\overline{\xi}})$ *is contained in the inertia group of some element of* $\Sigma_{\tilde{S}}$ *if and only if* J *has a cyclotomic normalizer in* $\pi_1(U, \overline{\overline{\xi}})$. *Here* $\tilde{S} \overset{\text{def}}{=} \tilde{X} - \tilde{U}$. □

For the precise definition of the cyclotomic normalizer, see *loc. cit.* Roughly speaking, the condition turns out to be equivalent to saying that J behaves as (a quotient of) $\hat{\mathbb{Z}}(1)$ with respect to some quasi-section of $\pi_1(U, \overline{\overline{\xi}}) \to G_k$.

Remark (7.5). Let $\tilde{v}$, $\tilde{v}'$ be two distinct elements in $\Sigma_{\tilde{S}}$. Then $I_{\tilde{v}} \cap I_{\tilde{v}'} = \{1\}$. In fact, there exists an open subgroup $\mathcal{H}$ of $\pi_1(U, \overline{\overline{\xi}})$ with $\tilde{v}_{\bar{\mathcal{H}}} \neq \tilde{v}'_{\bar{\mathcal{H}}}$ and $n_{\mathcal{H}} \geqslant 3$. Then, by (1-5) (applied to $\mathcal{H}$), we see $I_{\tilde{v}} \cap I_{\tilde{v}'} \cap \bar{\mathcal{H}} = \{1\}$, which implies $I_{\tilde{v}} \cap I_{\tilde{v}'}$ is finite. By (1.6), this implies $I_{\tilde{v}} \cap I_{\tilde{v}'} = \{1\}$.

In particular, it follows that $D_{\tilde{v}}$ is the normalizer of $I_{\tilde{v}}$ in $\pi_1(U, \overline{\overline{\xi}})$.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

From (7.5), Nakamura's result gives the following bijection

$$\Sigma_{\tilde{S}} \to \{\text{the set of maximal subgroups of } \pi_1(\bar{U}, \overline{\overline{\xi}}) \text{ which are cyclic and have a cyclotomic normalizer in } \pi_1(U, \overline{\overline{\xi}})\},$$

$\tilde{v} \mapsto I_{\tilde{v}}$. By the projective limit argument, we get the following:

THEOREM (7.6). *The map* $\overset{\approx}{\overset{\approx}{v}} \mapsto I_{\overset{\approx}{\overset{\approx}{v}}}$ *gives the following bijection*:

$$\Sigma_{\overset{\approx}{\overset{\approx}{X}}} \to \{\textit{the set of maximal subgroups of } G_{\bar{k}(X)} \textit{ which are cyclic and have a cyclotomic normalizer in } G_{k(X)}\}. \qquad \square$$

This gives a group-theoretical characterization of the inertia groups.

Now, construct the inverse map of

$$\mathrm{Isom}_k(\mathrm{Spec}(k(X_1)), \mathrm{Spec}(k(X_2))) \to \mathrm{Isom}_{G_k}(G_{k(X_1)}, G_{k(X_2)})/\mathrm{Inn}(G_{\bar{k}(X_2)}).$$

Take any $F \in \mathrm{Isom}_{G_k}(G_{k(X_1)}, G_{k(X_2)})/\mathrm{Inn}(G_{\bar{k}(X_2)})$, and choose $\mathcal{F} \in \mathrm{Isom}_{G_k}(G_{k(X_1)}, G_{k(X_2)})$ representing F. By (7.6), this induces a bijection

$$f\colon \Sigma_{\overset{\approx}{\overset{\approx}{X_1}}} \to \Sigma_{\overset{\approx}{\overset{\approx}{X_2}}},$$

characterized by: $I_{f(\overset{\approx}{\overset{\approx}{v_1}})} = \mathcal{F}(I_{\overset{\approx}{\overset{\approx}{v_1}}})$ for each $\overset{\approx}{\overset{\approx}{v}}_1 \in \Sigma_{\overset{\approx}{\overset{\approx}{X_1}}}$. Dividing by the actions of $G_{k(X_i)}$ (resp. $G_{\bar{k}(X_i)}$) $(i = 1, 2)$, we also obtain a bijection $\Sigma_{X_1} \to \Sigma_{X_2}$ (resp. $\Sigma_{\bar{X}_1} \to \Sigma_{\bar{X}_2}$), which we also denote by f. The following diagram is commutative:

$$\begin{array}{ccc}
\Sigma_{\overset{\approx}{\overset{\approx}{X_1}}} & \xrightarrow{f} & \Sigma_{\overset{\approx}{\overset{\approx}{X_2}}} \\
\downarrow & & \downarrow \\
\Sigma_{\bar{X}_1} & \xrightarrow{f} & \Sigma_{\bar{X}_2} \\
\downarrow & & \downarrow \\
\Sigma_{X_1} & \xrightarrow{f} & \Sigma_{X_2}.
\end{array}$$

Now, take any finite subset S_1 of Σ_{X_1} whose inverse image in $\Sigma_{\bar{X}_1}$ has cardinality $\geqslant 3$, and put $S_2 = f(S_1)$. By (7.6), $\mathcal{F}$ induces an isomorphism $\pi_1(U_1, \overline{\overline{\xi}}_1) \to$

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press

$\pi_1(U_2, \overline{\overline{\xi}}_2)$ over G_k. By (6.3), this comes from a (unique) k-isomorphism $U_1 \to U_2$, which induces a k-isomorphism $\mathrm{Spec}(k(X_1)) \to \mathrm{Spec}(k(X_2))$. It is easy to see that this isomorphism is independent of the choices of $\mathcal{F}$ and S_1. Thus we obtain a well-defined map

$$\begin{aligned}&\mathrm{Isom}_{G_k}(G_{k(X_1)}, G_{k(X_2)})/\mathrm{Inn}(G_{\bar{k}(X_2)})\\ &\quad\to \mathrm{Isom}_k(\mathrm{Spec}(k(X_1)), \mathrm{Spec}(k(X_2))),\end{aligned}$$

which gives the desired inverse map.

Acknowledgements

The author would like to express his sincere gratitude to Professor Yasutaka Ihara, Takeshi Tsuji, Shinichi Mochizuki (staffs), and Professor Takayuki Oda, Makoto Matsumoto (ex-staffs) of the RIMS Number Theory Seminar for helpful discussions, warm encouragements, and valuable advices. He thanks Mochizuki also for simplifications of the proofs of (5.3) and (6.6). He is also very grateful to Hiroaki Nakamura for having invited him to the arithmetic of fundamental groups, and to Professor Shoichi Nakajima for having informed him of the existence of the paper [Raynaud].

Notes. (i) After the author obtained the results in the present paper (and before he finished writing them), Mochizuki gave two different proofs of Conjecture (0.2) or, equivalently, Conjecture (0.1) for not necessarily affine hyperbolic curves. In the first proof ([Mochizuki 1]), he proved Conjecture (0.2) by reducing it to one of our main results. More precisely, he derived Conjecture (0.2) from a certain logarithmic Grothendieck conjecture for proper *non-smooth* stable curves over finite fields, which he derived from our Theorem (0.5). In the second proof ([Mochizuki 2]), he obtained Conjecture (0.2) as a corollary of a much stronger result, namely a certain pro-p Grothendieck conjecture for hyperbolic curves over p-adic local fields, which he proved by applying p-adic Hodge theory, not using the results of the present paper.

(ii) The first version of the present paper is the author's doctoral dissertation (Kyoto University, 1996).

References

[Anderson] Anderson, M. P.: Exactness properties of profinite completion functors, *Topology*, 13 (1974) 229–239.

[Asada] Asada, M.: Two properties of the filtration of the outer automorphism groups of certain groups, *Math. Z.*, 218 (1995) 123–133.

[AK] Asada, M. and Kaneko, M.: On the automorphism group of some pro-l fundamental groups, in Galois Representations and Arithmetic Algebraic Geometry, *Advanced Studies in Pure Mathematics*, 12 (Y. Ihara, K. Ribet, and J.-P. Serre, eds.) Kinokuniya, Tokyo, 1987, 137–159.

[AMO] Asada, M., Matsumoto, M. and Oda, T.: Local monodromy on the fundamental groups of algebraic curves along a degenerate stable curve, *J. Pure Appl. Algebra*, 103 (1995) 235–283.

[Chevalley] Chevalley, C.: Deux théorèmes d'arithmétique, *J. Math. Soc. Japan*, 3 (1951) 36–44.

[DM] Deligne, P. and Mumford, D.: The irreducibility of the space of curves of given genus, *Publ. Math. IHES*, 36 (1969) 75–109.

[Faltings] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.*, 73 (1983) 349–366; *ibid.*, 75 (1984) 381.

[FW] Faltings, G. and Wüstholz, G. et al.,: *Rational Points*, Vieweg, 1984.

[FJ] Fried, M. D. and Jarden, M.: *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 11, Springer-Verlag, Berlin Heidelberg, 1986.

[GK] Gold, R. and Kisilevsky, H.: On geometric $\mathbb{Z}_p$-extensions of function fields, *Manuscripta Math.*, 62 (1988) 145–161.

[Grothendieck1] Grothendieck, A.: A letter to G. Faltings, (1983).

[Grothendieck2] Grothendieck, A.: Esquisse d'un programme, preprint (1984).

[GM] Grothendieck, A. and Murre, P. J.: The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme, *Lecture Notes in Mathematics*, 208, Springer-Verlag, Berlin/Heidelberg/New York, 1971.

[Harbater] Harbater, D.: Galois groups with prescribed ramification, *Contemporary Math.*, 174 (1994) 35–60.

[Kaneko] Kaneko, M.: Certain automorphism groups of pro-l fundamental groups of punctured Riemann surfaces, *J. Fac. Sci. Univ. Tokyo, Sect. IA, Math.*, 36 (1989) 363–372.

[KM] Katz, N. M. and Mazur, B.: *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematical Studies, No. 108, Princeton University Press, Princeton, New Jersey, 1985.

[Knudsen] Knudsen, F. F.: The projectivity of the moduli space of stable curves II: The stacks $M_{g,n}$, *Math. Scand.*, 52 (1983) 161–199.

[KPR] Kuhlmann, F.-V., Pank, M. and Roquette, P.: Immediate and purely wild extensions of valued fields, *Manuscripta Math.*, 55 (1986) 39–67.

[Lichtenbaum] Lichtenbaum, S.: Curves over discrete valuation rings, *Amer. J. Math.*, 25 (1968) 380–405.

[LV] Lubotzky, A. and Van Den Dries, L.: Subgroups of free profinite groups and large subfields of $\overline{\mathbb{Q}}$, *Israel J. Math.*, 39(1–2) (1981) 25–45.

[Mochizuki1] Mochizuki, S.: The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, *J. Math. Sci. Univ. Tokyo*, 3 (1996) 571–627.

[Mochizuki2] Mochizuki, S.: The local pro-p Grothendieck conjecture for hyperbolic curves, RIMS preprint, 1045 (1995).

[Nakamura1] Nakamura, H.: Rigidity of the arithmetic fundamental group of a punctured projective line, *J. Reine Angew. Math.*, 405 (1990) 117–130.

[Nakamura2] Nakamura, H.: Galois rigidity of the étale fundamental groups of punctured projective lines, *J. Reine Angew. Math.*, 411 (1990) 205–216.

[Nakamura3] Nakamura, H.: Galois rigidity of algebraic mappings into some hyperbolic varieties, *International Journal of Mathematics*, 4 (1993) 421–438.

[Nakamura4] Nakamura, H.: Galois rigidity of pure sphere braid groups and profinite calculus, *J. Math. Sci. Univ. Tokyo*, 1 (1994) 71–136.

[Nakamura5] Nakamura, H.: On exterior Galois representations associated with open elliptic curves, *J. Math. Sci. Univ. Tokyo*, 2 (1995) 197–231.

[NT] Nakamura, H. and Tsunogai, H.: Some finiteness theorems on Galois centralizers in pro-l mapping class groups, *J. Reine Angew. Math.*, 441 (1993) 115–144.

[Oda1] Oda, T.: A note on ramification of the Galois representation on the fundamental group of an algebraic curve, *J. Number Theory*, 34 (1990) 225–228.

[Oda2] Oda, T.: A note on ramification of the Galois representation on the fundamental group of an algebraic curve, II, *J. Number Theory*, 53 (1995) 342–355.

[Pop1] Pop, F.: On Galois theory of function fields of one variable over number fields, *J. Reine Angew. Math.*, 406 (1990) 200–218.
[Pop2] Pop, F.: On Grothendieck's conjecture of birational anabelian geometry, *Ann. of Math.*, 138 (1994) 145–182.
[Pop3] Pop, F.: On Grothendieck's conjecture of birational anabelian geometry II, preprint.
[Raynaud] Raynaud, M.: Sections des fibrés vectoriels sur une courbe, *Bull. Soc. Math. France*, 110 (1982) 103–125.
[SGA] Grothendieck, A. and Mme. Raynaud, M.: Séminaire de Géometrie Algébrique du Bois Marie 1960/61, Revêtements Etales et Groupe Fondamental (SGA 1), *Lecture Notes in Mathematics*, 224, Springer-Verlag, Berlin/Heidelberg/New York, 1971.
[Spiess] Spiess, M.: An arithmetic proof of Pop's theorem concerning Galois groups of function fields over number fields, *J. Reine Angew. Math.*, 478 (1996) 107–126.
[Uchida] Uchida, K.: Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math.*, 106 (1977) 589–598.
[Voevodskiĭ] Voevodskiĭ, V. A.: Galois representations connected with hyperbolic curves, *Math. USSR Izv.*, 39 (1992) 1281–1291.

https://doi.org/10.1023/A:1000114400142 Published online by Cambridge University Press