Publ. RIMS, Kyoto Univ.
45 (2009), 135–186

A Prime-to-p Version of Grothendieck's Anabelian Conjecture for Hyperbolic Curves over Finite Fields of Characteristic $p>0$

By

Mohamed SAÏDI[*] and Akio TAMAGAWA[**]

Contents

Abstract

In this paper, we prove a prime-to-p version of Grothendieck's anabelian conjecture for hyperbolic curves over finite fields of characteristic $p > 0$, whose original (full profinite) version was proved by Tamagawa in the affine case and by Mochizuki in the proper case.

§0. Introduction

Let k be a finite field of characteristic $p > 0$ and U a hyperbolic curve over k. Namely, $U = X \smallsetminus S$, where X is a proper, smooth, geometrically connected

Communicated by S. Mukai. Received July 2, 2007. Revised February 10, 2008.
2000 Mathematics Subject Classification(s): 11G20, 14G15, 14H30, 14H25.

[*]School of Engineering, Computer Science and Mathematics, University of Exeter, Harrison Building, North Park Road, Exeter EX4 4QF, United Kingdom.
e-mail: M.Saidi@exeter.ac.uk

[**]Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan.
e-mail: tamagawa@kurims.kyoto-u.ac.jp

curve of genus g over k and $S \subset X$ is a divisor which is finite étale of degree r over k, such that $2 - 2g - r < 0$. We have the following exact sequence of profinite groups:

$$1 \to \pi_1(U \times_k \bar{k}, *) \to \pi_1(U, *) \to G_k \to 1.$$

Here, $\bar{k}$ is an algebraic closure of k, G_k is the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$, $*$ means a suitable geometric point, and π_1 stands for the étale fundamental group. The following result is fundamental in the anabelian geometry of hyperbolic curves over finite fields.

Theorem (Tamagawa, Mochizuki). *Let U, V be hyperbolic curves over finite fields k_U, k_V, respectively. Let*

$$\alpha : \pi_1(U, *) \overset{\sim}{\to} \pi_1(V, *)$$

be an isomorphism of profinite groups. Then α arises from a uniquely determined commutative diagram of schemes:

$$\begin{tikzcd}
\tilde{U} \arrow[r, "\sim"] \arrow[d] & \tilde{V} \arrow[d] \\
U \arrow[r, "\sim"] & V
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms, and the vertical arrows are the profinite étale universal coverings determined by the profinite groups $\pi_1(U, *)$, $\pi_1(V, *)$, respectively.

This result was proved by Tamagawa (cf. [Tamagawa1], Theorem (4.3)) in the affine case (together with a certain tame version), and more recently by Mochizuki (cf. [Mochizuki2], Theorem 3.2) in the proper case. It implies, in particular, that one can embed a suitable category of hyperbolic curves over finite fields into the category of profinite groups. It is essential in the anabelian philosophy of Grothendieck, as was formulated in [Grothendieck], to be able to determine the image of this functor. Recall that the full structure of the profinite group $\pi_1(U \times_k \bar{k}, *)$ is unknown (for any single example of U which is hyperbolic). Hence, a fortiori, the structure of $\pi_1(U, *)$ is unknown. (Even if we replace the fundamental groups $\pi_1(U \times_k \bar{k}, *)$, $\pi_1(U, *)$ by the tame fundamental groups $\pi_1^t(U \times_k \bar{k}, *)$, $\pi_1^t(U, *)$, respectively, the situation is just the same.) Thus, the problem of determining the image of the above functor seems to be quite difficult, at least for the moment. In this paper we investigate the following question:

Question 1. Is it possible to prove any result analogous to the above Theorem where $\pi_1(U,*)$ is replaced by some (continuous) quotient of $\pi_1(U,*)$ whose structure is better understood?

The first quotients that come into mind are the following. Let $\mathcal{C}$ (respectively, $\mathcal{C}^l$) be the class of finite groups of order prime to p (respectively, finite l-groups, where $l \neq p$ is a fixed prime number). Let Δ_U be the maximal pro-prime-to-p (i.e., pro-$\mathcal{C}$) quotient of $\pi_1(U \times_k \bar{k}, *)$. For a profinite group Γ, Γ^l stands for the maximal pro-l (i.e., pro-$\mathcal{C}^l$) quotient of Γ. Thus, in particular, Δ_U^l coincides with $\pi_1(U \times_k \bar{k}, *)^l$. Here, the structures of Δ_U and Δ_U^l are well understood — Δ_U (respectively, Δ_U^l) is isomorphic to the pro-prime-to-p (respectively, pro-l) completion of a certain well-known finitely generated discrete group (i.e., either a free group or a surface group). Let $\Pi_U \overset{\text{def}}{=} \pi_1(U,*)/\operatorname{Ker}(\pi_1(U \times_k \bar{k}, *) \twoheadrightarrow \Delta_U)$, $\Pi_U^{(l)} \overset{\text{def}}{=} \pi_1(U,*)/\operatorname{Ker}(\pi_1(U\times\, {}_k\bar{k}, *) \twoheadrightarrow \Delta_U^l$ be the corresponding quotients of $\pi_1(U \times_k \bar{k}, *)$, respectively. We shall refer to Π_U as the geometrically pro-Σ_U étale fundamental group of U, where $\Sigma_U \overset{\text{def}}{=} \mathfrak{Primes} \smallsetminus \{\operatorname{char}(k)\}$, and $\mathfrak{Primes}$ stands for the set of all prime numbers.

Question 2. Is it possible to prove any result analogous to the above Theorem where $\pi_1(U,*)$ is replaced by Π_U, $\Pi_U^{(l)}$, respectively?

Our main result in this paper is the following (cf. Corollary 3.10):

Theorem 1 (A Prime-to-p Version of Grothendieck's Anabelian Conjecture for Hyperbolic Curves over Finite Fields)**.** *Let U, V be hyperbolic curves over finite fields k_U, k_V, respectively. Let $\Sigma_U \overset{\text{def}}{=} \mathfrak{Primes} \smallsetminus \{\operatorname{char}(k_U)\}$, $\Sigma_V \overset{\text{def}}{=} \mathfrak{Primes} \smallsetminus \{\operatorname{char}(k_V)\}$, and write Π_U, Π_V for the geometrically pro-Σ_U étale fundamental group of U, and the geometrically pro-Σ_V étale fundamental group of V, respectively. Let*

$$\alpha : \Pi_U \xrightarrow{\sim} \Pi_V$$

be an isomorphism of profinite groups. Then α arises from a uniquely determined commutative diagram of schemes:

$$\begin{tikzcd}
\tilde{U} \arrow[r, "\sim"] \arrow[d] & \tilde{V} \arrow[d] \\
U \arrow[r, "\sim"] & V
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups Π_U, Π_V, respectively.

As an important consequence of Theorem 1, we deduce in Corollary 3.11 the following prime-to-p version of Uchida's Theorem on isomorphisms between absolute Galois groups of function fields (cf. [Uchida]).

Theorem 2. *Let X, Y be proper, smooth, geometrically connected curves over finite fields k_X, k_Y, respectively. Let K_X, K_Y be the function fields of X, Y, respectively. Let G_{K_X}, G_{K_Y} be the absolute Galois groups of K_X, K_Y, respectively, and let Γ_{K_X}, Γ_{K_Y} be their geometrically pro-prime-to-characteristic quotients* (*cf. the discussion before Corollary* 3.11). *Let*

$$\alpha : \Gamma_{K_X} \overset{\sim}{\to} \Gamma_{K_Y}$$

be an isomorphism of profinite groups. Then α arises from a uniquely determined commutative diagram of field extensions:

$$\begin{tikzcd}
(K_X)^{\sim} \arrow[r, "\sim"] & (K_Y)^{\sim} \\
K_X \arrow[u] \arrow[r, "\sim"] & K_Y \arrow[u]
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the extensions corresponding to the Galois groups Γ_{K_X}, Γ_{K_Y}, respectively.

Our proof of Theorem 1 relies substantially on the methods of Tamagawa and Mochizuki. We shall explain this briefly in the case where U is proper (hence, $U = X$). (cf. Theorem 3.9. The general case can be reduced to this special case.) Starting from Π_X, Tamagawa's method characterizes group-theoretically the decomposition groups at points of X in Π_X. The problem of recovering the points of X from the corresponding decomposition groups is related to the question of whether the natural map

$$X^{\mathrm{cl}} \to \mathrm{Sub}(\Pi_X)_{\Pi_X}$$

from the set of closed points of X to the set of conjugacy classes of closed subgroups of Π_X, which maps a point x to the conjugacy class of its decomposition group D_x, is injective. This map is known to be injective in the full profinite case, i.e., when one starts from $\pi_1(X, *)$ instead of Π_X. In our case we are only able to prove that the above map is almost injective, i.e., injective outside a finite set $E_X \subset X^{\mathrm{cl}}$. Thus, we can only recover from Π_X the set of points in a nonempty open subset $X \setminus E_X$.

In [Mochizuki2], Mochizuki developed a theory of cuspidalizations of étale fundamental groups of proper hyperbolic curves. One of the consequences of the main results of this theory is that, starting from Π_X, one can recover in a functorial way the Kummer theory of open affine subsets $U_S \overset{\text{def}}{=} X \smallsetminus S$, where S is a finite set of closed points contained in $X \smallsetminus E_X$. Using Kummer theory, one then recovers (up to Frobenius twist) the multiplicative group $\mathcal{O}^\times_{E_X}$ of rational functions on X whose divisor has support disjoint from E_X. Thus, starting from an isomorphism

$$\Pi_X \xrightarrow{\sim} \Pi_Y$$

as in Theorem 1 we can recover, up to Frobenius twist, an injective embedding between multiplicative groups

$$\mathcal{O}^\times_{E_X} \hookrightarrow \mathcal{O}^\times_{E_Y}.$$

The issue is then to show that this embedding arises from a uniquely determined embedding of fields $K_X \hookrightarrow K_Y$, between the corresponding function fields. This kind of problem of recovering the additive structure of function fields has been treated in [Uchida] and [Tamagawa1], using certain auxiliary functions called the minimal elements, i.e., functions with a minimal pole. The arguments of loc. cit. work well in the case of a bijection between multiplicative groups, but fail in our case where we only have an embedding $\mathcal{O}^\times_{E_X} \hookrightarrow \mathcal{O}^\times_{E_Y}$ between multiplicative groups. In our case, instead of using minimal elements, we can recover the additivity by using functions whose divisor has a unique pole. Also, the fact that we can only evaluate functions at all but finitely many points of X (or, more precisely, all points of $X \smallsetminus E_X$) presents an additional difficulty, which we overcome, roughly speaking, by passing to an infinite algebraic extension of the base field, and using "infinitely many" auxiliary functions.

In §1, we review some (mostly known but partly new) results which show that various invariants of the curve X (among other things, the set of decomposition groups at closed points of X) can be recovered group-theoretically, starting from Π_X. We also prove the almost injectivity of the above map from the set of closed points of X to the set of conjugacy classes of decomposition groups. In §2, we review the main results of Mochizuki's theory of cuspidalizations of étale fundamental groups of proper hyperbolic curves, which plays an essential role in this paper. In §3, we prove our main results, assuming the results of §4. Finally, In §4, we investigate the problem of recovering the additive structure of functions mentioned above. Using the above "one pole argument", we prove Proposition 4.4, which is used in §3.

§1. Characterization of Decomposition Groups

Let X be a proper, smooth, geometrically connected curve over a finite field $k = k_X$ of characteristic $p = p_X > 0$. Write $K = K_X$ for the function field of X.

Let S be a (possibly empty) finite set of closed points of X, and set $U = U_S \overset{\text{def}}{=} X \smallsetminus S$. We assume that U is hyperbolic.

Fix a separable closure $K^{\text{sep}} = K_X^{\text{sep}}$ of K, and write $\overline{k} = \overline{k_X}$ for the algebraic closure of k in K^{sep}. Write

$$G_K \overset{\text{def}}{=} \operatorname{Gal}(K^{\text{sep}}/K),$$

$$G_k \overset{\text{def}}{=} \operatorname{Gal}(\overline{k}/k)$$

for the absolute Galois groups of K and k, respectively.

The tame fundamental group $\pi_1^t(U)$ with respect to the base point defined by K^{sep} (where "tame" is with respect to the complement of U in X) can be naturally identified with a quotient of G_K. Write $\operatorname{Gal}(K_U^t/K)$ for this quotient. (In case $S = \emptyset$, we also write K_U^{ur} for K_U^t.) It is easy to see that K_U^t contains $K\overline{k}$.

Let $\Sigma = \Sigma_X$ be a set of prime numbers that contains at least one prime number different from p. Write

$$\Sigma^\dagger \overset{\text{def}}{=} \Sigma \smallsetminus \{p\}.$$

Thus, $\Sigma^\dagger \neq \emptyset$ by our assumption. Denote by $\hat{\mathbb{Z}}^{\Sigma^\dagger}$ the maximal pro-$\Sigma^\dagger$ quotient of $\hat{\mathbb{Z}}$. Set $\Sigma' = \Sigma'_X = \mathfrak{Primes} \smallsetminus \Sigma_X$. We say that Σ is cofinite if $\sharp(\Sigma') < \infty$. Note that, if Σ is cofinite, then Σ is of (Dirichlet) density 1.

We define $\tilde{K}_U$ to be the maximal pro-Σ subextension of $K\overline{k}$ in K_U^t. Now, set

$$\Pi_U = \operatorname{Gal}(\tilde{K}_U/K),$$

which is a quotient of $\pi_1^t(U) = \operatorname{Gal}(K_U^t/K)$. This fits into the exact sequence

$$1 \to \Delta_U \to \Pi_U \overset{\text{pr}_U}{\to} G_k \to 1.$$

Here, Δ_U is the maximal pro-Σ quotient of $\pi_1^t(\overline{U})$, where, for a k-scheme Z, we set $\overline{Z} \overset{\text{def}}{=} Z \times_k \overline{k}$.

Define $\tilde{X}_U$ to be the integral closure of X in $\tilde{K}_U$. Define $\tilde{U}$ to be the integral closure of U in $\tilde{K}_U$, which can be naturally identified with the inverse image (as an open subscheme) of U in $\tilde{X}_U$. Define $\tilde{S}_U$ to be the inverse image (as a set) of S in $\tilde{X}_U$.

For a scheme Z, write Z^{cl} for the set of closed points of Z. Then we have

$$X^{\mathrm{cl}} = U^{\mathrm{cl}} \coprod S,$$

$$(\tilde{X}_U)^{\mathrm{cl}} = \tilde{U}^{\mathrm{cl}} \coprod \tilde{S}_U.$$

Moreover, $(\tilde{X}_U)^{\mathrm{cl}}$ admits a natural action of Π_U, and the corresponding quotient can be naturally identified with X^{cl}.

For each $\tilde{x} \in (\tilde{X}_U)^{\mathrm{cl}}$, we define the decomposition group $D_{\tilde{x}} \subset \Pi_U$ (respectively, the inertia group $I_{\tilde{x}} \subset D_{\tilde{x}}$) to be the stabilizer at $\tilde{x}$ of the natural action of Π_U on $(\tilde{X}_U)^{\mathrm{cl}}$ (respectively, the kernel of the natural action of $D_{\tilde{x}}$ on $k(\tilde{x}) = \overline{k(x)} = \overline{k}$). These groups fit into the following commutative diagram in which both rows are exact:

$$\begin{tikzcd}
1 \arrow[r] & I_{\tilde{x}} \arrow[r] \arrow[d, phantom, "\cap"] & D_{\tilde{x}} \arrow[r] \arrow[d, phantom, "\cap"] & G_{k(x)} \arrow[r] \arrow[d, phantom, "\cap"] & 1 \\
1 \arrow[r] & \Delta_U \arrow[r] & \Pi_U \arrow[r] & G_k \arrow[r] & 1
\end{tikzcd}$$

Moreover, $I_{\tilde{x}} = \{1\}$ (respectively, $I_{\tilde{x}}$ is (non-canonically) isomorphic to $\hat{\mathbb{Z}}^{\Sigma^\dagger}$), if $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ (respectively, $\tilde{x} \in \tilde{S}_U$). Since $I_{\tilde{x}}$ is normal in $D_{\tilde{x}}$, $D_{\tilde{x}}$ acts on $I_{\tilde{x}}$ by conjugation. Since $I_{\tilde{x}}$ is abelian, this action factors through $D_{\tilde{x}} \to G_{k(x)}$ and induces a natural action of $G_{k(x)}$ on $I_{\tilde{x}}$.

Lemma 1.1. *Assume $\tilde{x} \in \tilde{S}_U$. Then:*
(i) *The subgroup $I_{\tilde{x}}^{G_{k(x)}}$ of $I_{\tilde{x}}$ that consists of elements fixed by the $G_{k(x)}$-action is trivial.*
(ii) *Assume moreover that Σ is of density* 1. *Then the map $G_{k(x)} \to \mathrm{Aut}(I_{\tilde{x}})$ is injective.*

Proof. By assumption, $I_{\tilde{x}} \simeq \hat{\mathbb{Z}}^{\Sigma^\dagger}$, and it is well-known that the map $G_{k(x)} \to \mathrm{Aut}(I_{\tilde{x}}) = (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$ coincides with the cyclotomic character and sends the $\sharp(k(x))$-th power Frobenius element $\varphi_{k(x)} \in G_{k(x)}$, which is a (topological) generator of $G_{k(x)}$, to $\sharp(k(x)) \in (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$. The assertion of (i) follows from this, since $\sharp(k(x)) - 1$ is not a zero divisor of the ring $\hat{\mathbb{Z}}^{\Sigma^\dagger}$. The assertion of (ii) also follows from this, together with a theorem of Chevalley ([Chevalley], Théorème 1, see also [GS]). More precisely, by applying Chevalley's theorem to the finitely generated subgroup $\langle \sharp(k(x)) \rangle$ of $\mathbb{Q}^\times$, we see that the map $\hat{\mathbb{Z}} \to (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$, $\alpha \mapsto \sharp(k(x))^\alpha$ is injective, as desired. □

Let G be a profinite group. Then, define $\mathrm{Sub}(G)$ (respectively, $\mathrm{OSub}(G)$) to be the set of closed (respectively, open) subgroups of G.

By conjugation, G acts on $\mathrm{Sub}(G)$. More generally, let H and K be closed subgroups of G such that K normalizes H. Then, by conjugation, K acts on $\mathrm{Sub}(H)$. We denote by $\mathrm{Sub}(H)_K$ the quotient $\mathrm{Sub}(H)/K$ by this action. In particular, $\mathrm{Sub}(G)_G$ is the set of conjugacy classes of closed subgroups of G.

For any closed subgroups H, K of G with $K \subset H$, we have a natural inclusion $\mathrm{Sub}(K) \subset \mathrm{Sub}(H)$, as well as a natural map $\mathrm{Sub}(H) \to \mathrm{Sub}(K)$, $J \mapsto J \cap K$. By using this latter natural map, we define

$$\overline{\mathrm{Sub}}(G) \overset{\mathrm{def}}{=} \varinjlim_{H \in \mathrm{OSub}(G)} \mathrm{Sub}(H).$$

Observe that $\overline{\mathrm{Sub}}(G)$ can be identified with the set of commensurate classes of closed subgroups of G. (Closed subgroups J_1 and J_2 of G are called commensurate (to each other), if $J_1 \cap J_1$ is open both in J_1 and in J_2.)

With these notations, we obtain natural maps

$$D = D[U] : (\tilde{X}_U)^{\mathrm{cl}} \to \mathrm{Sub}(\Pi_U), \tilde{x} \mapsto D_{\tilde{x}},$$

$$I = I[U] : (\tilde{X}_U)^{\mathrm{cl}} \to \mathrm{Sub}(\Delta_U) \subset \mathrm{Sub}(\Pi_U), \tilde{x} \mapsto I_{\tilde{x}},$$

which fit into the commutative diagram

$$\begin{tikzcd}
(\tilde{X}_U)^{\mathrm{cl}} \arrow[r, "D"] \arrow[d, equal] & \mathrm{Sub}(\Pi_U) \arrow[d] \\
(\tilde{X}_U)^{\mathrm{cl}} \arrow[r, "I"] & \mathrm{Sub}(\Delta_U),
\end{tikzcd}$$

where the vertical arrow stands for the natural map $\mathrm{Sub}(\Pi_U) \to \mathrm{Sub}(\Delta_U)$, $J \mapsto J \cap \Delta_U$. By composition with the natural map $\mathrm{Sub}(\Pi_U) \to \overline{\mathrm{Sub}}(\Pi_U)$, D, I yield

$$\overline{D} = \overline{D}[U] : (\tilde{X}_U)^{\mathrm{cl}} \to \overline{\mathrm{Sub}}(\Pi_U),$$

$$\overline{I} = \overline{I}[U] : (\tilde{X}_U)^{\mathrm{cl}} \to \overline{\mathrm{Sub}}(\Delta_U) \subset \overline{\mathrm{Sub}}(\Pi_U).$$

Remark 1.2. Unlike the case of D, I, the maps $\overline{D}, \overline{I}$ are essentially unchanged if we replace U by any covering corresponding to an open subgroup of Π_U.

Since the maps D, I are Π_U-equivariant, they induce natural maps

$$D_{\Pi_U} = D[U]_{\Pi_U} : X^{\mathrm{cl}} \to \mathrm{Sub}(\Pi_U)_{\Pi_U},$$

$$I_{\Pi_U} = I[U]_{\Pi_U} : X^{\mathrm{cl}} \to \mathrm{Sub}(\Delta_U)_{\Pi_U} \subset \mathrm{Sub}(\Pi_U)_{\Pi_U},$$

respectively.

Definition 1.3. Let $f : A \to B$ be a map of sets.
(i) We define $\mu_f : B \to \mathbb{Z} \cup \{\infty\}$ by $\mu_f(b) = \sharp(f^{-1}(b))$. (Thus, f is injective (respectively, surjective) if $\mu_f(b) \leq 1$ (respectively, $\mu_f(b) \geq 1$) for any $b \in B$. We also have $f(A) = \{b \in B \mid \mu_f(b) \geq 1\}$.)
(ii) We say that f is quasi-finite, if $\mu_f(b) < \infty$ for any $b \in B$.
(iii) We say that an element a of A is an exceptional element of f (in A), if $\mu_f(f(a)) > 1$. We refer to the set of exceptional elements as the exceptional set.
(iv) We say that a pair (a_1, a_2) of elements of A is an exceptional pair of f (in A), if $a_1 \neq a_2$ and $f(a_1) = f(a_2)$ hold.
(v) We say that f is almost injective (in the strong sense), if the exceptional set of f is finite. (Observe that almost injectivity implies quasi-finiteness.)

Lemma 1.4. *Let $f : A \to B$ and $g : B \to C$ be maps of sets. Then we have*:

Both f and g are quasi-finite (*respectively, almost injective*).

$$\Downarrow$$

$g \circ f$ is quasi-finite (*respectively, almost injective*).

$$\Downarrow$$

f is quasi-finite (*respectively, almost injective*).

Proof. Easy. □

Definition 1.5. Denote by $E_{\tilde{U}}$ the exceptional set of $\overline{D}$ in $(\tilde{X}_U)^{\mathrm{cl}}$

Definition 1.6. Let G be a profinite group and H a closed subgroup. Then we denote by $Z_G(H)$, $N_G(H)$ and $C_G(H)$ the centralizer, the normalizer and the commensurator, respectively, of H in G. Namely,

$$\begin{aligned} Z_G(H) &= \{g \in G \mid ghg^{-1} = h \text{ for any } h \in H\}, \\ &\cap \\ N_G(H) &= \{g \in G \mid gHg^{-1} = H\} \supset H, \\ &\cap \\ C_G(H) &= \{g \in G \mid gHg^{-1} \text{ and } H \text{ are commensurate}\}. \end{aligned}$$

Lemma 1.7. *Let Z be a closed subgroup of Π_U such that $\mathrm{pr}_U(Z)$ is open in G_k and that $\mathrm{pr}_U|_Z$ is injective. Then pr_U induces an injection $C_{\Pi_U}(Z) \hookrightarrow G_k$, and we have $C_{\Pi_U}(Z) = N_{\Pi_U}(Z) = Z_{\Pi_U}(Z) \supset Z$ and $(C_{\Pi_U}(Z) : Z) < \infty$.*

Proof. Take any $\sigma \in C_{\Pi_U}(Z) \cap \Delta_U$. Thus, $Z_0 \overset{\mathrm{def}}{=} Z \cap \sigma Z \sigma^{-1}$ is open both in Z and in $\sigma Z \sigma^{-1}$. We claim that σ commutes with any element τ of Z_0. Indeed, first, observe that $\tau \in Z_0 \subset \sigma Z \sigma^{-1}$ and $\sigma \tau \sigma^{-1} \in \sigma Z_0 \sigma^{-1} \subset \sigma Z \sigma^{-1}$ hold. Or, equivalently, $\sigma^{-1}\tau\sigma, \tau \in Z$. Second, observe that $\mathrm{pr}_U(\sigma^{-1}\tau\sigma) = \mathrm{pr}_U(\tau)$ holds, since $\mathrm{pr}_U(\sigma) = 1$. Now since $\mathrm{pr}_U|_Z$ is injective, the equality $\mathrm{pr}_U(\sigma^{-1}\tau\sigma) = \mathrm{pr}_U(\tau)$ implies $\sigma^{-1}\tau\sigma = \tau$, as desired.

Next, we prove $\sigma = 1$. To see this, suppose $\sigma \neq 1$ and take any sufficiently small, open characteristic subgroup $\overline{N}$ of Δ_U such that $\sigma \notin \overline{N}$. Set $\overline{H} \overset{\mathrm{def}}{=} \langle \overline{N}, \sigma \rangle \subset \Delta_U$. Then the image of σ in $\overline{H}^{\mathrm{ab}}$ is nontrivial. (Indeed, the image of σ in $\overline{H}/\overline{N}$ is nontrivial by definition. Since $\overline{H}/\overline{N}$ is cyclic, the surjection $\overline{H} \to \overline{H}/\overline{N}$ factors through the surjection $\overline{H} \to \overline{H}^{\mathrm{ab}}$.) Observe that Z_0 normalizes $\overline{H}$, since $\overline{N}$ is characteristic in Δ_U and σ commutes with Z_0. So, the open subgroup $H \overset{\mathrm{def}}{=} \langle \overline{H}, Z_0 \rangle$ of Π_U can be regarded as a semidirect-product extension of Z_0 by $\overline{H}$ and satisfies $H \cap \Delta_U = \overline{H}$. Now, the image of σ in $\overline{H}^{\mathrm{ab}}$ is nontrivial and fixed by the action of Z_0. This is impossible, as can be easily seen by observing the Frobenius weights in the action of Z_0, or of $\mathrm{pr}_U(Z_0)$, which is an open subgroup of G_k.

Thus, we have proved $\sigma = 1$, and the first assertion follows from this. In particular, $C_{\Pi_U}(Z)$ ($\hookrightarrow G_k$) is abelian, hence the second assertion follows. Finally, since pr_U induces an isomorphism $C_{\Pi_U}(Z) \xrightarrow{\sim} \mathrm{pr}_U(C_{\Pi_U}(Z))$ and $\mathrm{pr}_U(Z)$ is open in G_k, the third assertion holds. □

The first main result in this § is:

Proposition 1.8. (i) *$\overline{I}|_{\tilde{S}_U} : \tilde{S}_U \to \overline{\mathrm{Sub}}(\Pi_U)$ is injective.*

(ii) *$E_{\tilde{U}}$ is disjoint from $\tilde{S}_U$. (Or, equivalently, $E_{\tilde{U}} \subset \tilde{U}^{\mathrm{cl}}$.)*

(iii) *Let $\overline{\rho}$ denote the natural morphism $\tilde{X}_U \to \overline{X}$. Then, for each $\overline{x} \in \overline{X}^{\mathrm{cl}}$, $\overline{D}|_{\overline{\rho}^{-1}(\overline{x})}$ is injective.*

(iv) *Let ρ denote the natural morphism $\tilde{X}_U \to X$. Then, for each $x \in X^{\mathrm{cl}}$, $\overline{D}|_{\rho^{-1}(x)}$ is quasi-finite. If, moreover, $k(x) = k$ holds (i.e., x is a k-rational point of X), then $\overline{D}|_{\rho^{-1}(x)}$ is injective.*

(v) *$E_{\tilde{U}}$ is Π_U-stable.*

Assume, moreover, that Σ is cofinite. Then:

(vi) *The quotient $E_{\tilde{U}}/\Pi_U$ is finite.*

(vii) *$\overline{D} : (\tilde{X}_U)^{\mathrm{cl}} \to \overline{\mathrm{Sub}}(\Pi_U)$ is quasi-finite.*

Proof. (i) Take any $\tilde{x}, \tilde{x}' \in \tilde{S}_U$, and assume $\tilde{x} \neq \tilde{x}'$. Then there exists an open subgroup H_0 of Π_U, such that the following holds: Let U_0 denote the covering of U corresponding to $H_0 \subset \Pi_U$ and X_0 the integral closure of X in U_0 (i.e., X_0 is the smooth compactification of U_0), then the images x_0, x_0' of $\tilde{x}, \tilde{x}'$ in X_0 are distinct from each other. Moreover, by replacing H_0 by a smaller open subgroup if necessary, we may assume that the cardinality of the point set $\overline{X}_0 \smallsetminus \overline{U}_0$ is ≥ 3 (see, e.g., [Tamagawa1], Lemma (1.10)).

Now, to show the desired injectivity, it suffices to prove that $I_{\tilde{x}} \cap H_1 \neq I_{\tilde{x}'} \cap H_1$ holds for any open subgroup H_1 of H_0. Let U_1 denote the covering of U corresponding to $H_1 \subset \Pi_U$ and X_1 the integral closure of X in U_1. Then, by the choice of H_1, we see that the images of $\tilde{x}, \tilde{x}'$ in $\overline{S}_1 \overset{\text{def}}{=} \overline{X}_1 \smallsetminus \overline{U}_1$ are distinct from each other and that the cardinality of $\overline{S}_1$ is ≥ 3. Then it is easy to see that the images of $I_{\tilde{x}} \cap H_1, I_{\tilde{x}'} \cap H_1$ in $\overline{H}_1^{\text{ab}}$ are isomorphic to $\hat{\mathbb{Z}}^{\Sigma^\dagger}$ and that the intersection of these images is $\{0\}$. (Observe (the pro-$\Sigma^\dagger$ part of) exact sequence (1-5) in [Tamagawa1].) Thus, a fortiori, $I_{\tilde{x}} \cap H_1 \neq I_{\tilde{x}'} \cap H_1$ holds, as desired.

(ii) Take any $\tilde{x} \in \tilde{S}_U$ and $\tilde{x}' \in (\tilde{X}_U)^{\text{cl}}$, such that $\tilde{x} \neq \tilde{x}'$ holds; then we shall prove that the images of $\tilde{x}, \tilde{x}'$ by $\overline{D}$ are distinct from each other. To see this, it suffices, by definition, to prove that, for any open subgroup H of Π_U, the images $D_{\tilde{x}} \cap H, D_{\tilde{x}'} \cap H$ of $\tilde{x}, \tilde{x}'$ in $\text{Sub}(H)$ are distinct from each other. Now, replacing U by the covering of U corresponding to $H \subset \Pi_U$, it suffices to prove that $D_{\tilde{x}}, D_{\tilde{x}'}$ are distinct from each other. Now, recall that $D_{\tilde{x}} \cap \Delta_U = I_{\tilde{x}}$, $D_{\tilde{x}'} \cap \Delta_U = I_{\tilde{x}'}$. Thus, if $\tilde{x}' \in \tilde{S}_U$, the last assertion follows from (i). On the other hand, if $\tilde{x}' \in \tilde{U}^{\text{cl}}$, the last assertion follows from the fact $I_{\tilde{x}} \simeq \hat{\mathbb{Z}}^{\Sigma^\dagger}$, $I_{\tilde{x}'} = \{1\}$.

(iii) If $\overline{x} \in \overline{S} \overset{\text{def}}{=} \overline{X} \smallsetminus \overline{U}$, the assertion follows from (ii). So, we may and shall assume $\overline{x} \in \overline{U}^{\text{cl}}$. Take any $\tilde{x}, \tilde{x}' \in \overline{\rho}^{-1}(\overline{x})$. Then there exists $\sigma \in \Delta_U$ such that $\tilde{x}' = \sigma\tilde{x}$ holds. (Such σ is unique by the assumption $\overline{x} \in \overline{U}^{\text{cl}}$, though we do not use this fact in the proof.) Now, suppose that the images of $\tilde{x}, \tilde{x}'$ by $\overline{D}$ coincide with each other. Namely, $D_{\tilde{x}}$ and $D_{\tilde{x}'} = D_{\sigma\tilde{x}} = \sigma D_{\tilde{x}} \sigma^{-1}$ are commensurate to each other. Thus, $\sigma \in C_{\Pi_U}(D_{\tilde{x}}) \cap \Delta_U$, and it follows from Lemma 1.7 that $\sigma = 1$ holds, hence $\tilde{x}' = \sigma\tilde{x} = \tilde{x}$. Namely, $\overline{D}|_{\overline{\rho}^{-1}(\overline{x})}$ is injective, as desired.

(iv) Let π denote the natural morphism $\overline{X} \to X$, so that $\rho = \pi \circ \overline{\rho}$ holds. Since $\sharp(\pi^{-1}(x)) = [k(x) : k] < \infty$, the assertions follow directly from (iii).

(v) This follows from the fact that $\overline{D}$ is Π_U-equivariant.

(vi) To prove this (assuming that Σ is cofinite), we may replace U by any covering corresponding to an open subgroup of Π_U. Thus, we may assume that the genus of X is > 1 and that X is non-hyperelliptic. (See, e.g., [Tamagawa1], Lemma (1.10) for the former, and either [Tamagawa3], §2 or the proof (in characteristic zero) of [Mochizuki1], Lemma 10.4(4) for the latter.) We shall prove that $\rho(E_{\tilde{U}})$, which can be identified with $E_{\tilde{U}}/\Pi_U$, is finite, or, more strongly, that $\overline{\rho}(E_{\tilde{U}})$, which can be identified with $E_{\tilde{U}}/\Delta_U$, is finite.

Take any pair of elements $\tilde{x}, \tilde{x}' \in \tilde{U}^{\text{cl}}$, and denote by $\overline{x}, \overline{x}'$ the images of $\tilde{x}, \tilde{x}'$ in $\overline{U}^{\text{cl}}$, respectively. The images $\text{pr}_U(D_{\tilde{x}})$ and $\text{pr}_U(D_{\tilde{x}'})$ are open in G_k, hence so is the intersection $G_0 \overset{\text{def}}{=} \text{pr}_U(D_{\tilde{x}}) \cap \text{pr}_U(D_{\tilde{x}'})$. Let s, s' be the inverse maps of the isomorphisms $\text{pr}_U|_{D_{\tilde{x}}} : D_{\tilde{x}} \to \text{pr}_U(D_{\tilde{x}})$, $\text{pr}_U|_{D_{\tilde{x}'}} : D_{\tilde{x}'} \to \text{pr}_U(D_{\tilde{x}'})$, respectively. Then, it is well-known and easy to see that the map $\phi : G_0 \to \Delta_U$, $\gamma \mapsto s(\gamma)s'(\gamma)^{-1}$ is a continuous 1-cocycle (with respect to the left, conjugacy action of G_0 on Δ_U via the section s'). Thus, ϕ defines a cohomology class in $H^1(G_0, \Delta_U)$. We denote by $\phi_{0,X}^{\text{ab}} = \phi_{0,X}^{\text{ab}}(\tilde{x}, \tilde{x}')$ the image of this class in $H^1(G_0, \Delta_X^{\text{ab}})$. (Note that the G_0-action on Δ_X^{ab} induced by that on Δ_U extends to a canonical G_k-action, hence, in particular, is independent of the choice of $\tilde{x}'$.) Moreover, we set

$$\mathcal{H}_X \overset{\text{def}}{=} \varinjlim_{G \in \text{OSub}(G_k)} H^1(G, \Delta_X^{\text{ab}})$$

(where the transition maps are the restriction maps) and denote by $\phi_X^{\text{ab}} = \phi_X^{\text{ab}}(\tilde{x}, \tilde{x}')$ the image of $\phi_{0,X}^{\text{ab}}$ in $\mathcal{H}_X$.

On the other hand, it is well-known that Δ_X^{ab} is canonically isomorphic as a G_k-module to the pro-Σ part $T(J)^\Sigma$ of the full Tate module $T(J)$ of the Jacobian variety J (tensored with $\overline{k}$) of X. Thus, by Kummer theory (for the abelian variety J), we obtain an injective map $J(k_G)/(J(k_G)\{\Sigma'\}) \to H^1(G, \Delta_X^{\text{ab}})$, where G is an open subgroup of G_k, k_G is the finite extension of k corresponding to G, and, for an abelian group M, $M\{\Sigma'\}$ stands for the subgroup of torsion elements a of M such that every prime divisor of the order of a belongs to Σ'. (In fact, the above injective map is bijective by Lang's theorem, though we do not use this fact in the proof.) By taking the inductive limit, we obtain an injective map $J(\overline{k})/(J(\overline{k})\{\Sigma'\}) \to \mathcal{H}_X$. Now, it is widely known that the image in $\mathcal{H}_X$ of the class of $\overline{x} - \overline{x}'$ in $\overline{J}^{\text{cl}} = J(\overline{k})$ coincides with ϕ_X^{ab}. For this, see [NT], Lemma (4.14). (See also [Nakamura2], 2.2 and [Tamagawa1], Lemma (2.6).)

Suppose moreover that $(\tilde{x}, \tilde{x}')$ is an exceptional pair of $\overline{D}$. Then it follows from the various definitions that $\phi_X^{\text{ab}} \in \mathcal{H}_X$ is trivial. Therefore the class of $\overline{x} - \overline{x}'$ in $J(\overline{k})/(J(\overline{k})\{\Sigma'\})$ is trivial, or, equivalently, the class $\text{cl}(\overline{x} - \overline{x}')$ in $J(\overline{k})$ lies in $J(\overline{k})\{\Sigma'\}$. On the other hand, by (iii), it holds that $\overline{x} \neq \overline{x}'$, or, equivalently (by the assumption that the genus of X is > 1), $\text{cl}(\overline{x} - \overline{x}') \neq 0$.

Consider the morphism $\delta : X \times X \to J$, $(P, Q) \mapsto \text{cl}(P - Q)$. We claim:

Claim 1.9. (i) $\delta|_{X\times X-\iota(X)}$ is injective (on $\overline{k}$-valued points), where $\iota : X \to X \times X$ is the diagonal morphism.
(ii) The image W of δ does not contain any translate of a positive-dimensional abelian subvariety of J.

Indeed, for (i), suppose that $(P, Q), (P', Q') \in (X \times X \smallsetminus \iota(X))(\overline{k})$ have the same image under δ. Namely, the divisors $P - Q$ and $P' - Q'$ are linearly equivalent: $P - Q \sim P' - Q'$, or, equivalently, $P + Q' \sim P' + Q$. Since we have assumed that X is of genus > 1 and non-hyperelliptic, this implies that $P + Q'$ and $P' + Q$ coincide with each other as divisors. This implies that either $P = P', Q = Q'$ or $P = Q, P' = Q'$ holds. The former implies that $(P, Q) = (P', Q')$, as desired, and the latter implies that $(P, Q), (P', Q') \in \iota(X)$, which contradicts the assumption. For (ii), suppose that W contains a translate B' of some positive-dimensional abelian subvariety B of J. As $\dim(W) \leq \dim(X \times X) = 2$, we have $\dim(B') \leq 2$, i.e., either $\dim(B') = 2$ or $\dim(B') = 1$. The former implies that $B' = W$, since W is defined as the image of $X \times X$, hence irreducible of dimension ≤ 2. Since $0 \in W = B'$, we conclude $W = B' = B$. Now, since J is generated by W, we must have $J = B$. This implies that the genus of X (i.e., $\dim(J)$) is 2, which implies that X is hyperelliptic. This contradicts the assumption. So, suppose $\dim(B') = 1$. By (i), we see that δ induces a bijective morphism $X \times X \smallsetminus \iota(X) \to W \smallsetminus \{0\}$. From this, we deduce that there exists a finite radicial covering B'' of B' that admits a non-constant morphism to $X \times X$. In particular, considering a suitable one of two projections, we see that B'' admits a non-constant morphism to X. This is absurd, since the genus of B'' (respectively, X) is 1 (respectively, > 1). This completes the proof of Claim 1.9.

By Claim 1.9(ii) and [Boxall] (which is the most nontrivial ingredient of the proof of Proposition 1.8), we see that $W(\overline{k}) \cap (J(\overline{k})\{\Sigma'\})$ is finite. Now, by Claim 1.9(i), we conclude that there exists a finite subset $\mathcal{S}$ of $(X \times X)(\overline{k})$ that contains any pair $(\overline{x}, \overline{x}')$ as above. This implies the desired assertion that $\overline{p}(E_{\tilde{U}})$ is a finite set.
(vii) Note that $\rho(E_{\tilde{U}})$ can be identified with $E_{\tilde{U}}/\Pi_U$ by (v). Thus, the assertion of (vii) directly follows from (vi) and the first part of (iv). □

Definition 1.10. We define E_U to be the image of $E_{\tilde{U}}$ in X^{cl}. (This can be identified with $E_{\tilde{U}}/\Pi_U$. Thus, if Σ is cofinite, then it is finite by Proposition 1.8(vi).)

Corollary 1.11. (i) $D_{\Pi_U}|_{X^{\mathrm{cl}}\smallsetminus E_U} : X^{\mathrm{cl}} \smallsetminus E_U \to \mathrm{Sub}(\Pi_U)_{\Pi_U}$ *is injective.*

(ii) *E_U is disjoint from S. (Or, equivalently, $E_U \subset U^{\mathrm{cl}}$.)*

Assume, moreover, that Σ is cofinite. Then:

(iii) *$D_{\Pi_U} : X^{\mathrm{cl}} \to \mathrm{Sub}(\Pi_U)_{\Pi_U}$ is almost injective.*

Proof. (i) As $D|_{(\tilde{X}_U)^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}} : (\tilde{X}_U)^{\mathrm{cl}} \smallsetminus E_{\tilde{U}} \to \mathrm{Sub}(\Pi_U)$ is injective by definition and Π_U-equivariant, its quotient by Π_U, which is naturally identified with $D_{\Pi_U}|_{X^{\mathrm{cl}} \smallsetminus E_U} : X^{\mathrm{cl}} \smallsetminus E_U \to \mathrm{Sub}(\Pi_U)_{\Pi_U}$, is also injective. This completes the proof.

(ii) This follows from Proposition 1.8(ii).

(iii) This follows from (i) and the fact that E_U is finite (Proposition 1.8(vi)). □

Corollary 1.12. (i) *For each $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$, pr_U induces an injection*

$$C_{\Pi_U}(D_{\tilde{x}}) \hookrightarrow G_k,$$

and we have

$$C_{\Pi_U}(D_{\tilde{x}}) = N_{\Pi_U}(D_{\tilde{x}}) = Z_{\Pi_U}(D_{\tilde{x}}) \supset D_{\tilde{x}}$$

and

$$(C_{\Pi_U}(D_{\tilde{x}}) : D_{\tilde{x}}) < \infty.$$

If, moreover, $\tilde{x} \in \tilde{U}^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}$, we have

$$C_{\Pi_U}(D_{\tilde{x}}) = N_{\Pi_U}(D_{\tilde{x}}) = Z_{\Pi_U}(D_{\tilde{x}}) = D_{\tilde{x}}.$$

(ii) *For each $\tilde{x} \in \tilde{S}_U$, we have*

$$C_{\Pi_U}(D_{\tilde{x}}) = N_{\Pi_U}(D_{\tilde{x}}) = D_{\tilde{x}},\ Z_{\Pi_U}(D_{\tilde{x}}) = Z_{D_{\tilde{x}}}(D_{\tilde{x}})$$

and

$$C_{\Pi_U}(I_{\tilde{x}}) = N_{\Pi_U}(I_{\tilde{x}}) = D_{\tilde{x}},\ Z_{\Pi_U}(I_{\tilde{x}}) = Z_{D_{\tilde{x}}}(I_{\tilde{x}}).$$

If, moreover, Σ is of density 1, then $Z_{D_{\tilde{x}}}(D_{\tilde{x}}) = \{1\}$ and $Z_{D_{\tilde{x}}}(I_{\tilde{x}}) = I_{\tilde{x}}$.

(iii) *Assume, moreover, that Σ is cofinite. Then there exists an open subgroup G_0 of G_k, such that, for any open subgroup H of $\mathrm{pr}_U^{-1}(G_0)$ and any element $\tilde{x}$ of $(\tilde{X}_U)^{\mathrm{cl}} = \tilde{U}^{\mathrm{cl}} \coprod \tilde{S}_U$, we have*

$$C_H(D_{\tilde{x}} \cap H) = N_H(D_{\tilde{x}} \cap H) = D_{\tilde{x}} \cap H,$$

$$Z_H(D_{\tilde{x}} \cap H) = \begin{cases} D_{\tilde{x}} \cap H, & \text{for } \tilde{x} \in \tilde{U}^{\mathrm{cl}}, \\ \{1\}, & \text{for } \tilde{x} \in \tilde{S}_U. \end{cases}$$

In other words, if we replace U *by a covering corresponding to such* H*, we have, for any* $\tilde{x} \in (\tilde{X}_U)^{\mathrm{cl}}$*,*

$$C_{\Pi_U}(D_{\tilde{x}}) = N_{\Pi_U}(D_{\tilde{x}}) = D_{\tilde{x}},$$

$$Z_{\Pi_U}(D_{\tilde{x}}) = \begin{cases} D_{\tilde{x}}, & \textit{for } \tilde{x} \in \tilde{U}^{\mathrm{cl}}, \\ \{1\}, & \textit{for } \tilde{x} \in \tilde{S}_U. \end{cases}$$

Proof. First, since $\overline{D}|_{(\tilde{X}_U)^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}} : (\tilde{X}_U)^{\mathrm{cl}} \smallsetminus E_{\tilde{U}} \to \overline{\mathrm{Sub}}(\Pi_U)$ is injective and Π_U-equivariant, we see that $C_{\Pi_U}(D_{\tilde{x}}) = D_{\tilde{x}}$ holds for any $\tilde{x} \in (\tilde{X}_U)^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}$.
(i) The first assertion follows from Lemma 1.7. The second assertion follows from the first assertion and the fact shown at the beginning of the proof.
(ii) Let $\tilde{x} \in \tilde{S}_U$. Then $\tilde{x} \notin E_{\tilde{U}}$ by Proposition 1.8(ii). Thus, we have $C_{\Pi_U}(D_{\tilde{x}}) = N_{\Pi_U}(D_{\tilde{x}}) = D_{\tilde{x}}$. From this, we also have $Z_{\Pi_U}(D_{\tilde{x}}) = Z_{D_{\tilde{x}}}(D_{\tilde{x}})$.

Next, by Proposition 1.8(i), the map $\overline{I}|_{\tilde{S}_U} : \tilde{S}_U \to \overline{\mathrm{Sub}}(\Pi_U)$ is injective. Since this map is also Π_U-equivariant, we see that $C_{\Pi_U}(I_{\tilde{x}}) = D_{\tilde{x}}$. As $C_{\Pi_U}(I_{\tilde{x}}) \supset N_{\Pi_U}(I_{\tilde{x}}) \supset D_{\tilde{x}}$, we have $N_{\Pi_U}(I_{\tilde{x}}) = D_{\tilde{x}}$. From this, we also have $Z_{\Pi_U}(I_{\tilde{x}}) = Z_{D_{\tilde{x}}}(I_{\tilde{x}})$.

If Σ is of density 1, then this last group coincides with $I_{\tilde{x}}$ by Lemma 1.1(ii). In particular, $Z_{D_{\tilde{x}}}(D_{\tilde{x}}) \subset I_{\tilde{x}}$, which implies $Z_{D_{\tilde{x}}}(D_{\tilde{x}}) = I_{\tilde{x}} \cap Z_{D_{\tilde{x}}}(D_{\tilde{x}}) = \{1\}$ by Lemma 1.1(i).
(iii) Define G_0 to be the intersection (in G_k) of $G_{k(x)}$ for $x \in E_U$. Since E_U is finite by Proposition 1.8(vi), G_0 is an open subgroup of G_k. By (i) and (ii), it is easy to see that this G_0 satisfies the desired properties. □

Next, we shall show that various invariants and structures of U can be recovered group-theoretically (or φ-group-theoretically) from Π_U, in the following sense.

Definition 1.13. (i) We say that $\Pi = (\Pi, \Delta, \varphi_\Pi)$ is a φ-(profinite)group, if Π is a profinite group, Δ is a closed normal subgroup of Π and φ_Π is an element of Π/Δ.
(ii) An isomorphism from a φ-group $\Pi = (\Pi, \Delta, \varphi_\Pi)$ to another φ-group $\Pi' = (\Pi', \Delta', \varphi_{\Pi'})$ is an isomorphism $\Pi \xrightarrow{\sim} \Pi'$ as profinite groups that induces an isomorphism $\Delta \xrightarrow{\sim} \Delta'$, hence also an isomorphism $\Pi/\Delta \xrightarrow{\sim} \Pi'/\Delta'$, such that the last isomorphism sends φ_Π to $\varphi_{\Pi'}$.

From now on, we regard Π_U as a φ-group by $\Pi_U = (\Pi_U, \Delta_U, \varphi_k)$, where φ_k stands for the $\sharp(k)$-th power Frobenius element in $G_k = \Pi_U/\Delta_U$. We shall say that an isomorphism $\alpha : \Pi_U \xrightarrow{\sim} \Pi_{U'}$ of profinite groups is Frobenius-preserving if α determines an isomorphism of φ-groups.

Definition 1.14. (i) Given an invariant $F(U)$ that depends on the isomorphism class (as a scheme) of a hyperbolic curve U over a finite field, we say that $F(U)$ can be recovered group-theoretically (respectively, φ-group-theoretically) from Π_U, if any isomorphism (respectively, any Frobenius-preserving isomorphism) $\Pi_U \overset{\sim}{\to} \Pi_V$ implies $F(U) = F(V)$ for two such curves U, V.
(ii) Given an additional structure $\mathcal{F}(U)$ (e.g., a family of subgroups, quotients, elements, etc.) on the profinite group Π_U that depends functorially on a hyperbolic curve U over a finite field (in the sense that, for any isomorphism (as schemes) between two such curves U, V, any isomorphism $\Pi_U \overset{\sim}{\to} \Pi_V$ induced by this isomorphism $U \overset{\sim}{\to} V$ (unique up to composition with inner automorphisms) preserves the structures $\mathcal{F}(U)$ and $\mathcal{F}(V)$), we say that $\mathcal{F}(U)$ can be recovered group-theoretically (respectively, φ-group-theoretically) from Π_U, if any isomorphism (respectively, any Frobenius-preserving isomorphism) $\Pi_U \overset{\sim}{\to} \Pi_V$ between two such curves U, V preserves the structures $\mathcal{F}(U)$ and $\mathcal{F}(V)$.

Proposition 1.15. I. *The following invariants and structures can be recovered group-theoretically from* Π_U:
(i) *The subgroup* Δ_U *of* Π_U, *hence the quotient* $G_k = \Pi_U/\Delta_U$.
(ii) *The subsets* Σ *and* $\Sigma^\dagger$ *of* $\mathfrak{Primes}$.

II. *The following invariants and structures can be recovered* φ*-group-theoretically from* Π_U:
(iii) *The prime number* p.
(iv) *The cardinality* $\sharp(k)$ (*or, equivalently, the isomorphism class of the finite field* k).
(v) *The genus* $g = g_X$ *of* X *and the cardinality* $r = r_U \overset{\mathrm{def}}{=} \sharp(\overline{S})$, *where* $\overline{S} \overset{\mathrm{def}}{=} \overline{X} \setminus \overline{U}$.
(vi) *The kernel* I_U *of the natural surjection* $\Pi_U \to \Pi_X$ (*which coincides with the kernel of the natural surjection* $\Delta_U \to \Delta_X$), *hence the quotients* $\Pi_X = \Pi_U/I_U$, $\Delta_X = \Delta_U/I_U$.
(vii) *The cardinalities* $\sharp(X(k))$, $\sharp(U(k))$ *and* $\sharp(S(k))$.

III. *Assume, moreover, that* Σ *is of density* 1. *Then the following structure* (*hence also* (iii)–(vii) *above*) *can be recovered group-theoretically from* Π_U:
(viii) *The* $\sharp(k)$*-th power Frobenius element* $\varphi_k \in G_k$.

Proof. (i) Similar to [Tamagawa1], Proposition (3.3)(ii). (See also [Mochizuki2], Theorem 1.1(ii).)

(ii) Note that Δ_U^{ab} is isomorphic to $(\hat{\mathbb{Z}}^{\Sigma^\dagger})^{2g+r+b-1} \times \mathbb{Z}_p^c$, where $b = b_U$ stands for the second Betti number of U, i.e., $b = 1$ (respectively, 0) if $r = 0$ (respectively, $r > 0$), and c stands for the p-rank of the Jacobian variety of X (respectively, 0) if $p \in \Sigma$ (respectively, $p \notin \Sigma$). (See, e.g., [Tamagawa1], Corollary (1.2).) Here, we always have $2g + r + b - 1 > c \geq 0$. If, moreover, $p \in \Sigma$ and if we replace Π_U by a suitable open subgroup, then we have $c > 0$. (See, e.g., [Tamagawa1], Lemma (1.9). See also [Tamagawa2], Remark (3.11).) From these, it is easy to see that Σ and $\Sigma^\dagger$ can be recovered group-theoretically from Π_U. (See also [Mochizuki2], Theorem 1.1(i).)

(iii) By conjugation, $G_k = \Pi_U/\Delta_U$ acts on $(\Delta_U^{\mathrm{ab}})^{\Sigma^\dagger}$, hence on the $\mathrm{rank}_{\hat{\mathbb{Z}}^{\Sigma^\dagger}}((\Delta_U^{\mathrm{ab}})^{\Sigma^\dagger})$-th exterior power $\bigwedge^{\max}_{\hat{\mathbb{Z}}^{\Sigma^\dagger}} (\Delta_U^{\mathrm{ab}})^{\Sigma^\dagger}$. Thus, we obtain (purely group-theoretically) the character

$$\rho^{\det} : G_k \to \mathrm{Aut}\left(\bigwedge_{\hat{\mathbb{Z}}^{\Sigma^\dagger}}^{\max} (\Delta_U^{\mathrm{ab}})^{\Sigma^\dagger} \right) = (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times.$$

As in the proof of [Tamagawa1], Proposition (3.4)(i), we have $\rho^{\det} = \epsilon \chi_{\Sigma^\dagger}^{g+n+b-1}$, where $\chi_{\Sigma^\dagger}$ is the pro-$\Sigma^\dagger$ cyclotomic character and ϵ is a certain character (depending on U) with values in $\{\pm 1\}$. Now, p can be characterized by $\rho^{\det}(\varphi_k) \in \pm p^{\mathbb{Z}}$ $(\subset (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times)$. (See also [Mochizuki2], Remark 11.)

(iv) Similar to [Tamagawa1], Proposition (3.4)(iii). (See also [Mochizuki2], Remark 11.)

(v) Similar to [Tamagawa1], Proposition (3.5). (See also [Mochizuki2], Theorem 1.1(i).)

(vi) Similar to [Tamagawa1], Proposition (3.7).

(vii) Similar to [Tamagawa1], Proposition (3.8). More precisely, by the Lefschetz trace formula, we have, for any prime $l \in \Sigma^\dagger$,

$$\begin{aligned} \sharp(X(k)) &= \sum_{i=0}^{2} (-1)^i \operatorname{tr}(\varphi_k^{-1} \mid H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_l)) \\ &= 1 + \sharp(k) - \operatorname{tr}(\varphi_k^{-1} \mid H^1(\Delta_X, \mathbb{Q}_l)). \end{aligned}$$

Here, observe $H^0_{\mathrm{et}}(\overline{X}, \mathbb{Q}_l) = \mathbb{Q}_l$, $H^2_{\mathrm{et}}(\overline{X}, \mathbb{Q}_l) = \mathbb{Q}_l(1)$, and

$$H^1_{\mathrm{et}}(\overline{X}, \mathbb{Q}_l) = H^1(\Delta_X, \mathbb{Q}_l).$$

We also have

$$\begin{aligned}\sharp(U(k)) &= \sum_{i=0}^{2}(-1)^i \operatorname{tr}(\varphi_k^{-1} \mid H_c^i(\overline{U}, \mathbb{Q}_l)) \\ &= \sum_{i=0}^{2}(-1)^i \operatorname{tr}(\varphi_k \mid H_{\mathrm{et}}^i(\overline{U}, \mathbb{Q}_l(1))) \\ &= \sharp(k)\sum_{i=0}^{2}(-1)^i \operatorname{tr}(\varphi_k \mid H_{\mathrm{et}}^i(\overline{U}, \mathbb{Q}_l)) \\ &= \sharp(k)\sum_{i=0}^{2}(-1)^i \operatorname{tr}(\varphi_k \mid H^i(\Delta_U, \mathbb{Q}_l)).\end{aligned}$$

Here, for a profinite group Γ, we define

$$H^i(\Gamma, \mathbb{Q}_l) \overset{\text{def}}{=} (\varprojlim H^i(\Gamma, \mathbb{Z}/l^n\mathbb{Z})) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l,$$

as usual. Thus, $\sharp(X(k))$ and $\sharp(U(k))$ can be recovered φ-group-theoretically. Finally, $\sharp(S(k))$ can be recovered as $\sharp(X(k)) - \sharp(U(k))$.
(viii) First, in the notation of the proof of (iii) above, the image of $(\rho^{\det})^2 = \chi^{2(g+n+b-1)}$ is an open subgroup of the subgroup $\overline{\langle p\rangle}$ of $(\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$ (topologically) generated by p. This characterizes group-theoretically the prime number p (in $(\Sigma^\dagger)' = \Sigma' \cup \{p\}$), by a theorem of Chevalley ([Chevalley], Théorème 1, see also [GS]). More precisely, take any prime $q \in (\Sigma^\dagger)'$ distinct from p. Then, by applying Chevalley's theorem to the finitely generated subgroup $\langle p, q\rangle$ of $\mathbb{Q}^\times$, we see that the map $\hat{\mathbb{Z}} \times \hat{\mathbb{Z}} \to (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$, $(\alpha, \beta) \mapsto p^\alpha q^\beta$ is injective, hence that there does not exist a subgroup of $(\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$ that is open both in $\overline{\langle p\rangle}$ and $\overline{\langle q\rangle}$. Next, define m to be the minimal positive integer with $p^m \in (\rho^{\det})^2(G_k)$ $(\subset (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times)$. Then φ_k can be characterized by $(\rho^{\det})^2(\varphi_k) = p^m$. (See also [Mochizuki2], Remark 9.) □

Definition 1.16. (i) For each closed subgroup G of G_k, we denote by k_G the subextension of k in $\overline{k}$ corresponding to G. Observe that, if G is open, then k_G is a finite field.
(ii) For each closed subgroup H of Π_U, we set $G_H \overset{\text{def}}{=} \operatorname{pr}_U(H)$ and $k_H \overset{\text{def}}{=} k_{G_H}$. We denote by U_H the (pro-finite, pro-tame, geometrically pro-Σ) covering of U corresponding to H. Observe that, if H is open, then U_H is a hyperbolic curve over the finite field k_H and H can be identified with Π_{U_H}.
(iii) Let H be a closed subgroup of Π_U and G a closed subgroup of G_H. Then we set $H_G \overset{\text{def}}{=} H \cap \operatorname{pr}_U^{-1}(G)$. Observe that U_{H_G} can be identified with $U_H \times_{k_H} k_G$.
(iv) For each open subgroup H of Π_U, we set

$$\nu_U(H) \overset{\text{def}}{=} \sharp(U_H(k_H)).$$

Corollary 1.17. *The map* $\mathrm{OSub}(\Pi_U) \to \mathbb{Z}_{\geq 0}$, $H \mapsto \nu_U(H)$ *can be recovered* φ*-group-theoretically from* Π_U*.*

Proof. Since $H = \Pi_{U_H}$, this is immediate from Proposition 1.15(vii). □

Finally, we shall prove that the set of decomposition groups in Π_U can be recovered φ-group-theoretically from Π_U. First, we shall treat decomposition groups at points of $\tilde{S}_U$.

Theorem 1.18. (i) *The set of inertia groups at points of* $\tilde{S}_U$ *(i.e., the image of the injective map* $I|_{\tilde{S}_U} : \tilde{S}_U \to \mathrm{Sub}(\Delta_U) \subset \mathrm{Sub}(\Pi_U)$*) can be recovered* φ*-group-theoretically from* Π_U*.*
(ii) *The set of decomposition groups at points of* $\tilde{S}_U$ *(i.e., the image of the injective map* $D|_{\tilde{S}_U} : \tilde{S}_U \to \mathrm{Sub}(\Pi_U)$*) can be recovered* φ*-group-theoretically from* Π_U*.*

Proof. (i) This is due to Nakamura. See [Nakamura1], §3 and [Nakamura3], 2.1. (See also [Tamagawa1], §7, C.) Strictly speaking, Nakamura only treats the case over number fields, but his proof relies on Frobenius weights and the same proof works over finite fields.
(ii) This follows from (i), together with Corollary 1.12(ii). □

Next, we shall treat decomposition groups at points of $\tilde{U}^{\mathrm{cl}}$. This is done along the lines of [Tamagawa1], §2, but slightly more subtle than the case of [Tamagawa1], due to the existence of the exceptional set $E_{\tilde{U}}$.

Definition 1.19. (i) We denote by $\mathcal{S}(\Pi_U)$ ($\subset \mathrm{Sub}(\Pi_U)$) the set of closed subgroups Z of Π_U such that G_Z is open in G_k and that $\mathrm{pr}_U|_Z : Z \to G_Z$ is an isomorphism.
(ii) For each open subgroup G of G_k, we set

$$\mathcal{S}(\Pi_U)_G \overset{\mathrm{def}}{=} \{Z \in \mathcal{S}(\Pi_U) \mid G_Z = G\}.$$

Namely, $\mathcal{S}(\Pi_U)_G$ can be identified with the set of group-theoretic sections of the surjection $\mathrm{pr}_U|_{(\Pi_U)_G} : (\Pi_U)_G \to G$.

Definition 1.20. Let Z be an element of $\mathcal{S}(\Pi_U)$.
(i) We define $\mathcal{U}(Z)$ to be the set of open subgroups of $(\Pi_U)_{G_Z}$ that contain Z.
(ii) For each $H \in \mathcal{U}(Z)$, we define $m(H, Z)$ to be the number of elements s of (a complete system of representatives of) $(\Pi_U)_{G_Z}/H$ such that $s^{-1}Zs \subset H$. Note that this is a group-theoretic invariant.

(iii) We denote by $\nu_\infty(Z)$ the cardinality of $U_Z(k_Z)$. (Note that $U_Z(k_Z)$ can be identified with the project limit of $\{U_H(k_Z)\}_{H\in\mathcal{U}(Z)}$.)
(iv) We denote by $U_Z(k_Z)^*$ the set of points x of $U_Z(k_Z)$ such that the residue field of the image of x in U coincides with k_Z. (Observe that this residue field is included in k_Z in general.) We denote by $\nu_\infty^*(Z)$ the cardinality of $U_Z(k_Z)^*$.
(v) We define $U_Z(\overline{k})^{\mathrm{fin}}$ to be the union of $U_{Z_G}(k_G) = U_Z(k_G)$ for all open subgroups G of G_Z. (N.B. Since U_Z is not of finite type over k_Z, we have $U_Z(\overline{k})^{\mathrm{fin}} \subsetneq U_Z(\overline{k})$.) We denote by $\overline{\nu}_\infty(Z)$ the cardinality ($\in \mathbb{Z}_{\geq 0}\cup\{\infty\}$) of $U_Z(\overline{k})^{\mathrm{fin}}$. Moreover, we define $(U_Z)^{\mathrm{cl,fin}}$ to be the image of $U_Z(\overline{k})^{\mathrm{fin}}$ in $(U_Z)^{\mathrm{cl}}$.

Proposition 1.21. *Let Z be an element of $\mathcal{S}(\Pi_U)$.*
(i) *Let G be an open subgroup of G_Z and x a point of $U_{Z_G}(k_G) \subset (U_{Z_G})^{\mathrm{cl}}$. Then there exists a unique point $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ above x. Moreover, $D_{\tilde{x}}$ contains Z_G, and, in particular, $D_{\tilde{x}}$ is commensurate to Z.*
(ii) *Let $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ and x the image of $\tilde{x}$ in $(U_Z)^{\mathrm{cl}}$. Then we have*

$$x \in U_Z(k_Z) \iff Z \subset D_{\tilde{x}},$$

$$x \in U_Z(k_Z)^* \iff Z = D_{\tilde{x}},$$

and

$$x \in (U_Z)^{\mathrm{cl,fin}} \iff Z \text{ and } D_{\tilde{x}} \text{ are commensurate.}$$

(iii) *We have $\nu_\infty^*(Z) \leq \nu_\infty(Z) \leq \overline{\nu}_\infty(Z)$ and $\nu_\infty(Z) \leq \nu_U((\Pi_U)_{G_Z}) < \infty$.*
(iv) *Assume, moreover, that Σ is cofinite. Then we have $\overline{\nu}_\infty(Z) < \infty$.*

Proof. (i) Take any point $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ above x. First note that $D_{\tilde{x}} \cap Z_G$ is the decomposition group at $\tilde{x}$ in Z_G. Thus, since x is k_G-rational, the image of $D_{\tilde{x}} \cap Z_G$ by pr_U must coincide with G. Since pr_U induces an isomorphism $Z_G \xrightarrow{\sim} G$, this implies that $D_{\tilde{x}} \cap Z_G$ coincides with Z_G. It follows from this that $D_{\tilde{x}}$ contains Z_G and that there exists only one point (i.e., $\tilde{x}$) of $\tilde{U}$ above x. Finally, since Z_G is open both in Z and in $D_{\tilde{x}}$, $D_{\tilde{x}}$ is commensurate to Z. (For the latter openness, observe that pr_U induces an isomorphism $D_{\tilde{x}} \xrightarrow{\sim} \mathrm{pr}_U(D_{\tilde{x}})$ and that $\mathrm{pr}_U(Z_G) = G$ is open in $\mathrm{pr}_U(D_{\tilde{x}})$.)
(ii) First, suppose $x \in U_Z(k_Z)$. Then, by (i), $Z \subset D_{\tilde{x}}$. Conversely, suppose $Z \subset D_{\tilde{x}}$, Then the decomposition group $D_{\tilde{x}} \cap Z$ at $\tilde{x}$ in Z coincides with Z, which implies $x \in U_Z(k_Z)$.

Next, we define x_U to be the image of x in U^{cl}. Suppose $x \in U_Z(k_Z)^*$. Then, by (i), $Z \subset D_{\tilde{x}}$. By the definition of $U_Z(k_Z)^*$, we must have $k(x_U) = k_Z$, or, equivalently, $\mathrm{pr}_U(D_{\tilde{x}}) = \mathrm{pr}_U(Z)$. This implies $D_{\tilde{x}} = Z$. Conversely, suppose

$Z = D_{\tilde{x}}$. Then $\mathrm{pr}_U(D_{\tilde{x}}) = \mathrm{pr}_U(Z)$, or, equivalently, $k(x_U) = k_Z$. This implies $x \in U_Z(k_Z)^*$.

Finally, for each open subgroup G of G_Z, denote by x_G the image of $\tilde{x}$ in $(U_{Z_G})^{\mathrm{cl}}$. Then

$$\begin{aligned} & x \in (U_Z)^{\mathrm{cl,fin}} \\ \Longleftrightarrow\ & x_G \in U_{Z_G}(k_{Z_G}) \text{ for some open subgroup } G \text{ of } G_Z \\ \Longleftrightarrow\ & Z_G \subset D_{\tilde{x}} \text{ for some open subgroup } G \text{ of } G_Z \\ \Longleftrightarrow\ & Z \text{ and } D_{\tilde{x}} \text{ are commensurate,} \end{aligned}$$

where the second equivalence follows from the first equivalence in the statement of (ii).
(iii) The first two inequalities are clear. To see the third inequality, it suffices to prove that the natural map $U_Z(k_Z) \to U_{(\Pi_U)_{G_Z}}(k_Z)$ is injective. For this, take $x, x' \in U_Z(k_Z)$ and suppose that the images of x, x' in $U_{(\Pi_U)_{G_Z}}(k_Z)$ coincide with each other. Take the unique points $\tilde{x}, \tilde{x}' \in \tilde{U}^{\mathrm{cl}}$ above x, x', respectively. Then, by (i), $D_{\tilde{x}}$ and $D_{\tilde{x}'}$ are commensurate to each other. On the other hand, since the images of $\tilde{x}, \tilde{x}'$ in $(U_{(\Pi_U)_{G_Z}})^{\mathrm{cl}}$ coincide with each other and are k_Z-rational, we see that their images in $\overline{U}^{\mathrm{cl}}$ must coincide with each other. It follows from these observations and Proposition 1.8(iii) that $\tilde{x} = \tilde{x}'$, hence that $x = x'$, as desired.
(iv) This follows from (ii) and Proposition 1.8(vii). (Observe that the natural surjective map $U_Z(\overline{k})^{\mathrm{fin}} \to (U_Z)^{\mathrm{cl,fin}}$ is quasi-finite.) □

Corollary 1.22. *Let Z be an element of $\mathcal{S}(\Pi_U)$. Then we have*
(i) *There exists an $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ such that $Z = D_{\tilde{x}}$ (respectively, $Z \subset D_{\tilde{x}}$, respectively, Z is commensurate to $D_{\tilde{x}}$), if and only if $\nu^*_\infty(Z) > 0$ (respectively, $\nu_\infty(Z) > 0$, respectively, $\overline{\nu}_\infty(Z) > 0$).*
(ii) *There exist more than one $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ such that Z is commensurate to $D_{\tilde{x}}$, if and only if $\overline{\nu}_\infty(Z) > 1$.*
(iii) *There exists an $\tilde{x} \in \tilde{U}^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}$ (respectively, $\tilde{x} \in E_{\tilde{U}}$) such that $Z = D_{\tilde{x}}$ if and only if $\overline{\nu}_\infty(Z) = \nu^*_\infty(Z) = 1$ (respectively, $\nu^*_\infty(Z) > 0$ and $\overline{\nu}_\infty(Z) > 1$).*

Proof. (i) This is immediate from Proposition 1.21(ii).
(ii) By definition, $\overline{\nu}_\infty(Z) > 1$ if and only if $\nu_\infty(Z_G) > 1$ for some open subgroup G of G_Z. Thus, the assertion follows from (the first statement of) Proposition 1.21(ii) and (the uniqueness statement of) Proposition 1.21(i).

(iii) It follows formally from (i) and (ii) that $\nu_\infty^*(Z) > 0$ and $\overline{\nu}_\infty(Z) > 1$ (respectively, ≤ 1) if and only if $Z = D_{\tilde{x}}$ for some $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ and Z is commensurate to $D_{\tilde{x}}$ for more than (respectively, at most) one $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$. This last statement is equivalent to saying that $Z = D_{\tilde{x}}$ for some $\tilde{x} \in E_{\tilde{U}}$ (respectively, $\tilde{x} \in \tilde{U}^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}$). This, together with Proposition 1.21(iii) (or, more specifically, the fact $\nu_\infty^*(Z) \leq \overline{\nu}_\infty(Z)$), completes the proof. □

Proposition 1.23. *Let Z be an element of $\mathcal{S}(\Pi_U)$.*
(i) *We have*

$$\nu_\infty(Z) = \lim_{\substack{H \in \mathcal{U}(Z) \\ H \to Z}} \frac{\nu_U(H)}{m(H,Z)}.$$

More precisely, there exists an $H_0 \in \mathcal{U}(Z)$ such that, for any $H \in \mathcal{U}(Z)$ with $H \subset H_0$, we have

$$\nu_\infty(Z) = \frac{\nu_U(H)}{m(H,Z)}.$$

In particular, $\nu_\infty(Z)$ is a φ-group-theoretic invariant.
(ii) *Set $C \stackrel{\mathrm{def}}{=} C_{\Pi_U}(Z)$, which is isomorphic to $\hat{\mathbb{Z}}$. Then we have*

$$\nu_\infty^*(Z) = \sum_{d|N} \mu(N/d)\nu_\infty(C^d),$$

where $N \stackrel{\mathrm{def}}{=} (C : Z)$, $C^d \stackrel{\mathrm{def}}{=} \{\sigma^d \mid \sigma \in C\}$, and μ stands for Möbius' function.

In particular, $\nu_\infty^*(Z)$ is a φ-group-theoretic invariant.
(iii) *We have*

$$\overline{\nu}_\infty(Z) = \sup_{G \in \mathrm{OSub}(G_Z)} \nu_\infty(Z_G).$$

In particular, $\overline{\nu}_\infty(Z)$ is a φ-group-theoretic invariant.

Proof. (i) We define $U_{(\Pi_U)_{G_Z}}(k_Z)^\infty$ to be the image of $U_Z(k_Z)$ in $U_{(\Pi_U)_{G_Z}}(k_Z)(= U(k_Z))$. On the one hand, the proof of (the third inequality of) Proposition 1.21(iii) shows that the natural surjection $U_Z(k_Z) \to U_{(\Pi_U)_{G_Z}}(k_Z)^\infty$ is a bijection. On the other hand, since $U_Z(k_Z) = \varprojlim_{H \in \mathcal{U}(Z)} U_H(k_Z)$ and $\sharp(U_H(k_Z)) < \infty$ for each $H \in \mathcal{U}(Z)$ (hence, in particular, $\sharp(U(k_Z)) < \infty$), we see that there exists an $H_0 \in \mathcal{U}(Z)$ such that $U_{(\Pi_U)_{G_Z}}(k_Z)^\infty$ coincides with the image of $U_{H_0}(k_Z)$ in $U_{(\Pi_U)_{G_Z}}(k_Z)$.

Take any $H \in \mathcal{U}(Z)$ with $H \subset H_0$. Then each point of $U_H(k_Z)$ lies above some point of $U_{(\Pi_U)_{G_Z}}(k_Z)^\infty$. For each point $x \in U_Z(k_Z)$, write $\tilde{x}$ for the unique point of $\tilde{U}^{\mathrm{cl}}$ that lies above x. Then, by Proposition 1.21(i), the decomposition group at $\tilde{x}$ in $(\Pi_U)_{G_Z}$ coincides with Z. From this, we see that $m(H, Z)$ is defined so as to coincide with the cardinality of the fiber of the map $U_H(k_Z) \to U_{(\Pi_U)_{G_Z}}(k_Z)$ at $x_{(\Pi_U)_{G_Z}}$, where $x_{(\Pi_U)_{G_Z}}$ is the image of x in $U_{(\Pi_U)_{G_Z}}(k_Z)$. From these, we conclude that the quantity $\nu_U(H)/m(H, Z)$ coincides with the cardinality $\sharp(U_{(\Pi_U)_{G_Z}}(k_Z)^\infty)$, as desired.

The last assertion follows from the first assertion and Corollary 1.17.

(ii) First, by Lemma 1.7, we see that $C \in \mathcal{S}(\Pi_U)$ and that C is isomorphic to $\hat{\mathbb{Z}}$. Let x be a point of $U_Z(k_Z)$. We claim that $x \notin U_Z(k_Z)^*$ if and only if there exists $Z' \in \mathcal{S}(\Pi_U)$ with $Z' \supsetneqq Z$, such that the image in $(U_{Z'})^{\mathrm{cl}}$ of $x \in U_Z(k_Z) \subset (U_Z)^{\mathrm{cl}}$ is $k_{Z'}$-rational. Indeed, to see the 'if' part, observe that the natural morphism $U_Z \to U$ factors through $U_Z \to U_{Z'}$. Thus, if the image of x in $(U_{Z'})^{\mathrm{cl}}$ is $k_{Z'}$-rational, so is the image of x in U^{cl}, hence $x \notin U_Z(k_Z)^*$. Conversely, suppose $x \notin U_Z(k_Z)^*$ and take the unique point $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ above x. As the residue field of the image of x in U is strictly smaller than k_Z, the image of $D_{\tilde{x}}$ in G_k must be strictly larger than G_Z. Now, it is easy to see from this that $Z' \overset{\mathrm{def}}{=} D_{\tilde{x}}$ has the desired property.

Now, consider $Z' \in \mathcal{S}(\Pi_U)$ with $Z' \supset Z$. Then we have $Z \subset Z' \subset C$, which implies that $Z' = C^d$ for some (unique) d dividing N. We see $U_{Z'} = U_C \times_{k_C} k_{Z'}$, and, in particular, $U_Z = U_C \times_{k_C} k_Z$. Thus, the image of x in $(U_{Z'})^{\mathrm{cl}}$ is $k_{Z'}$-rational if and only if $x \in U_Z(k_Z) = U_C(k_Z)$ lies in $U_{Z'}(k_{Z'}) = U_C(k_{Z'})$.

These observations, together with the so-called inclusion-exclusion principle (see, e.g., [Hall], Chapter 2), imply the desired formula.

(iii) Immediate from the definitions. □

Theorem 1.24. *The set of decomposition groups at points of* $\tilde{U}^{\mathrm{cl}}$ *(respectively,* $\tilde{U}^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}$*, respectively,* $E_{\tilde{U}}$*) (i.e., the image of the map* $D|_{\tilde{U}^{\mathrm{cl}}} : \tilde{U}^{\mathrm{cl}} \to \mathrm{Sub}(\Pi_U)$ *(respectively,* $D|_{\tilde{U}^{\mathrm{cl}} \smallsetminus E_{\tilde{U}}} : \tilde{U}^{\mathrm{cl}} \smallsetminus E_{\tilde{U}} \to \mathrm{Sub}(\Pi_U)$*, respectively,* $D|_{E_{\tilde{U}}} : E_{\tilde{U}} \to \mathrm{Sub}(\Pi_U)$*)) can be recovered* φ*-group-theoretically from* Π_U*.*

Proof. This follows formally from Corollary 1.22 and Proposition 1.23. □

Corollary 1.25. *The set of decomposition groups at points of* $(\tilde{X}_U)^{\mathrm{cl}}$ *(i.e., the image of the map* $D : (\tilde{X}_U)^{\mathrm{cl}} \to \mathrm{Sub}(\Pi_U)$*) can be recovered* φ*-group-theoretically from* Π_U*.*

Proof. This is immediate from Theorem 1.18(ii) and Theorem 1.24. (See also [Mochizuki2], Remark 10.) □

§2. Cuspidalizations of Proper Hyperbolic Curves

In this §, we review the main results of Mochizuki's theory of cuspidalizations of fundamental groups of proper hyperbolic curves, developed in [Mochizuki2], which plays an important role in this paper. We maintain the notations of §1 and further assume $X = U$. (Thus, the finite set S in §1 is empty, and, in this §, we save the symbol S for another finite set of closed points of X.) Accordingly, X is a proper hyperbolic curve over a finite field $k = k_X$.

Recall that Δ_X stands for the maximal pro-Σ quotient of $\pi_1(\overline{X})$, that Π_X stands for $\pi_1(X)/\operatorname{Ker}(\pi_1(\overline{X}) \twoheadrightarrow \Delta_X)$, and that they fit into the following exact sequence:

$$1 \to \Delta_X \to \Pi_X \overset{\mathrm{pr}_X}{\to} G_k \to 1.$$

Similarly, if we write $X \times X \overset{\mathrm{def}}{=} X \times_k X$, then we obtain (by considering the maximal pro-Σ quotient $\Delta_{X \times X}$ of $\pi_1(\overline{X \times X})$) an exact sequence:

$$1 \to \Delta_{X\times X} \to \Pi_{X\times X} \to G_k \to 1,$$

where $\Pi_{X\times X}$ (respectively, $\Delta_{X\times X}$) may be identified with $\Pi_X \times_{G_k} \Pi_X$ (respectively, $\Delta_X \times \Delta_X$).

Definition 2.1 (cf. [Mochizuki2], Definition 1.1(i).)**.** Let H be a profinite group equipped with a homomorphism $H \to \Pi_X$. Then we shall refer to the kernel I_H of $H \to \Pi_X$ as the cuspidal subgroup of H (relative to $H \to \Pi_X$). We shall refer to an inner automorphism of H by an element of I_H as a cuspidally inner automorphism. We shall say that H is cuspidally abelian (respectively, cuspidally pro-Σ^*, where Σ^* is a set of prime numbers) (relative to $H \to \Pi_X$) if I_H is abelian (respectively, if I_H is a pro-Σ^* group). If H is cuspidally abelian, then observe that H/I_H acts naturally (by conjugation) on I_H. We shall say that H is cuspidally central (relative to $H \to \Pi_X$) if this action of H/I_H on I_H is trivial. Also, we shall use the same terminology for $H \to \Pi_X$ when Π_X is replaced by Δ_X, $\Pi_{X\times X}$, or $\Delta_{X\times X}$.

For a finite subset $S \subset X^{\mathrm{cl}}$ write $U_S \overset{\mathrm{def}}{=} X \setminus S$. Let Δ_{U_S} be the maximal cuspidally (relative to the natural map to Δ_X) pro-$\Sigma^\dagger$ quotient of the maximal pro-Σ quotient of the tame fundamental group of $\overline{U_S}$ (where "tame" is with respect to the complement of U_S in X), and let Π_{U_S} be the corresponding quotient $\pi_1(U_S)/\operatorname{Ker}(\pi_1(\overline{U_S}) \twoheadrightarrow \Delta_{U_S})$ of $\pi_1(U_S)$. Thus, we have an exact sequence:

$$1 \to \Delta_{U_S} \to \Pi_{U_S} \to G_k \to 1,$$

which fits into the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \Delta_{U_S} \arrow[r] \arrow[d] & \Pi_{U_S} \arrow[r] \arrow[d] & G_k \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \Delta_X \arrow[r] & \Pi_X \arrow[r] & G_k \arrow[r] & 1.
\end{tikzcd}$$

Further, let $\iota : X \to X \times X$ be the diagonal morphism, and write

$$U_{X\times X} \overset{\mathrm{def}}{=} X \times X \setminus \iota(X).$$

We shall denote by $\Delta_{U_{X\times X}}$ the maximal cuspidally (relative to the natural map to $\Delta_{X\times X}$) pro-$\Sigma^\dagger$ quotient of the maximal pro-Σ quotient of the tame fundamental group of $(U_{X\times X})_{\bar{k}}$ (where "tame" is with respect to the divisor $\iota(X) \subset X \times X$), and by $\Pi_{U_{X\times X}}$ the corresponding quotient $\pi_1(U_{X\times X})/\operatorname{Ker}(\pi_1(\overline{U_{X\times X}}) \twoheadrightarrow \Delta_{U_{X\times X}})$ of $\pi_1(U_{X\times X})$. Thus, we have an exact sequence:

$$1 \to \Delta_{U_{X\times X}} \to \Pi_{U_{X\times X}} \to G_k \to 1,$$

which fits into the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \Delta_{U_{X\times X}} \arrow[r] \arrow[d] & \Pi_{U_{X\times X}} \arrow[r] \arrow[d] & G_k \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \Delta_{X\times X} \arrow[r] & \Pi_{X\times X} \arrow[r] & G_k \arrow[r] & 1.
\end{tikzcd}$$

Finally, set

$$M_X \overset{\mathrm{def}}{=} \operatorname{Hom}_{\hat{\mathbb{Z}}^{\Sigma^\dagger}}(H^2(\Delta_X, \hat{\mathbb{Z}}^{\Sigma^\dagger}), \hat{\mathbb{Z}}^{\Sigma^\dagger}).$$

Thus, M_X is a free $\hat{\mathbb{Z}}^{\Sigma^\dagger}$-module of rank 1, and M_X is isomorphic to $\hat{\mathbb{Z}}^{\Sigma^\dagger}(1)$ as a G_k-module (where the "(1)" denotes a "Tate twist", i.e., G_k acts on $\hat{\mathbb{Z}}^{\Sigma^\dagger}(1)$ via the cyclotomic character) (cf. [Mochizuki2], the discussion following Proposition 1.1).

For the rest of this §, let X, Y be proper hyperbolic curves over finite fields k_X, k_Y of characteristic p_X, p_Y, respectively. Let Σ_X (respectively, Σ_Y) be a set of prime numbers that contains at least one prime number different from p_X (respectively, p_Y). Write Δ_X (respectively, Δ_Y) for the maximal pro-Σ_X quotient of $\pi_1(\overline{X})$ (respectively, the maximal pro-Σ_Y quotient of $\pi_1(\overline{Y})$), and Π_X (respectively, Π_Y) for the quotient $\pi_1(X)/\operatorname{Ker}(\pi_1(\overline{X}) \twoheadrightarrow \Delta_X)$ of $\pi_1(X)$ (respectively, the quotient $\pi_1(Y)/\operatorname{Ker}(\pi_1(\overline{Y}) \twoheadrightarrow \Delta_Y)$ of $\pi_1(Y)$).

Let

$$\alpha : \Pi_X \xrightarrow{\sim} \Pi_Y$$

be an isomorphism of profinite groups.

The following is one of the main results of Mochizuki's theory.

Theorem 2.2 (Reconstruction of Maximal Cuspidally Abelian Extensions). *Let $\iota_X : X \to X \times X$ (respectively, $\iota_Y : Y \to Y \times Y$) be the diagonal morphism, and write $U_{X\times X} \overset{\mathrm{def}}{=} X \times X \smallsetminus \iota(X)$ (respectively, $U_{Y\times Y} \overset{\mathrm{def}}{=} Y \times Y \smallsetminus \iota(Y)$). Denote by $\Pi_{U_{X\times X}} \twoheadrightarrow \Pi^{\text{c-ab}}_{U_{X\times X}}$, $\Pi_{U_{Y\times Y}} \twoheadrightarrow \Pi^{\text{c-ab}}_{U_{Y\times Y}}$ the maximal cuspidally (relative to the natural surjections $\Pi_{U_{X\times X}} \twoheadrightarrow \Pi_{X\times X}$, $\Pi_{U_{Y\times Y}} \twoheadrightarrow \Pi_{Y\times Y}$, respectively) abelian quotients. Then there is a commutative diagram:*

$$\begin{tikzcd}
\Pi^{\text{c-ab}}_{U_{X\times X}} \arrow[r, "\alpha^{\text{c-ab}}"] \arrow[d] & \Pi^{\text{c-ab}}_{U_{Y\times Y}} \arrow[d] \\
\Pi_{X\times X} \arrow[r, "\alpha\times\alpha"] & \Pi_{Y\times Y}
\end{tikzcd}$$

where $\alpha^{\text{c-ab}}$ is an isomorphism which is well-defined up to cuspidally inner automorphism (i.e., an inner automorphism of $\Pi^{\text{c-ab}}_{U_{Y\times Y}}$ by an element of the cuspidal subgroup $\mathrm{Ker}(\Pi^{\text{c-ab}}_{U_{Y\times Y}} \twoheadrightarrow \Pi_{Y\times Y})$). Moreover, the correspondence

$$\alpha \mapsto \alpha^{\text{c-ab}}$$

is functorial (up to cuspidally inner automorphism) with respect to α.

Proof. See [Mochizuki2], Theorem 1.1(iii). □

Let $\tilde{x} \in \tilde{X}^{\mathrm{cl}}$ and x the image of $\tilde{x}$ in X^{cl}. In this and the next §§, we sometimes refer to the decomposition group $D_{\tilde{x}}$ as the decomposition group of Π_X at x, and denote it simply by D_x. Thus, D_x is well-defined only up to conjugation by an element of Π_X.

For the rest of this §, we shall assume that α is Frobenius-preserving (cf. Definition 1.14). (Note that this assumption is automatically satisfied in the case where Σ_X and Σ_Y are of density 1 by Proposition 1.15(viii).) Thus, by Theorem 1.24, one deduces naturally from α a bijection

$$\phi : X^{\mathrm{cl}} \smallsetminus E_X \xrightarrow{\sim} Y^{\mathrm{cl}} \smallsetminus E_Y$$

such that

$$\alpha(D_x) = D_{\phi(x)}$$

holds (up to conjugation) for any $x \in X^{\mathrm{cl}} \smallsetminus E_X$. (Note that E_X (respectively, E_Y) is a finite set by Proposition 1.8(vi), if Σ_X (respectively, Σ_Y) is cofinite.)

As an important consequence of Theorem 2.2, we deduce the following:

Corollary 2.3. *With the above assumptions, let $S \subset X^{\mathrm{cl}} \smallsetminus E_X$, $T \subset Y^{\mathrm{cl}} \smallsetminus E_Y$ be finite subsets that correspond to each other via ϕ. Then α, $\alpha^{\text{c-ab}}$ induce isomorphisms* (*well-defined up to cuspidally inner automorphisms, i.e., inner automorphisms by elements of* $\mathrm{Ker}(\Pi_{V_T}^{\text{c-ab}} \to \Pi_Y)$)

$$\alpha_{S,T}^{\text{c-ab}} : \Pi_{U_S}^{\text{c-ab}} \xrightarrow{\sim} \Pi_{V_T}^{\text{c-ab}}$$

lying over α, where $U_S \overset{\mathrm{def}}{=} X \smallsetminus S$, $V_T \overset{\mathrm{def}}{=} Y \smallsetminus T$, and $\Pi_{U_S} \twoheadrightarrow \Pi_{U_S}^{\text{c-ab}}$, $\Pi_{V_T} \twoheadrightarrow \Pi_{V_T}^{\text{c-ab}}$, are the maximal cuspidally abelian quotients (*relative to the maps $\Pi_{U_S} \twoheadrightarrow \Pi_X$, $\Pi_{V_T} \twoheadrightarrow \Pi_Y$, respectively*). *These isomorphisms are functorial with respect to α, S, T, as well as with respect to passing to connected finite étale coverings of X, Y, which arise from open subgroups of Π_X, Π_Y, in the following sense*: *Let $\xi : X' \to X$* (*respectively, $\eta : Y' \to Y$*) *be a finite étale covering which arises from the open subgroup $\Pi_{X'} \subseteq \Pi_X$* (*respectively, $\Pi_{Y'} \subseteq \Pi_Y$*), *such that $\alpha(\Pi_{X'}) = \Pi_{Y'}$; set $U'_{S'} \overset{\mathrm{def}}{=} X' \smallsetminus S'$, $V'_{T'} \overset{\mathrm{def}}{=} Y' \smallsetminus T'$, $S' \overset{\mathrm{def}}{=} \xi^{-1}(S)$, $T' \overset{\mathrm{def}}{=} \eta^{-1}(T)$; and denote by α' the isomorphism $\Pi_{X'} \xrightarrow{\sim} \Pi_{Y'}$ induced by α. Then we have the following commutative diagram*:

$$\begin{tikzcd}
\Pi_{U'_{S'}}^{\text{c-ab}} \arrow[r, "(\alpha')_{S',T'}^{\text{c-ab}}"] \arrow[d] & \Pi_{V'_{T'}}^{\text{c-ab}} \arrow[d] \\
\Pi_{U_S}^{\text{c-ab}} \arrow[r, "\alpha_{S,T}^{\text{c-ab}}"] & \Pi_{V_T}^{\text{c-ab}}
\end{tikzcd}$$

where the vertical arrows are the natural maps.

Proof. The proof of [Mochizuki2], Theorem 2.1(i) (where $E_X = E_Y = \emptyset$ is assumed) works as it is. □

Next, let

$$1 \to M_X \to \mathcal{D} \to \Pi_{X \times X} \to 1$$

be a fundamental extension, i.e., an extension whose corresponding extension class in $H^2_{\mathrm{et}}(X \times X, M_X)$ (via the natural identification $H^2(\Pi_{X\times X}, M_X) \xrightarrow{\sim} H^2_{\mathrm{et}}(X \times X, M_X)$ (cf. [Mochizuki2], Proposition 1.1)) coincides with the first (étale) Chern class of the diagonal $\iota(X)$ (cf. [Mochizuki2], Proposition 1.5). Let

$x, y \in X(k)$ and write $D_x, D_y \subset \Pi_X$ for the associated decomposition groups (which are well-defined up to conjugation). Set

$$\mathcal{D}_x \stackrel{\text{def}}{=} \mathcal{D}|D_x \times_{G_k} \Pi_X, \quad \mathcal{D}_{x,y} \stackrel{\text{def}}{=} \mathcal{D}|D_x \times_{G_k} D_y.$$

Thus, $\mathcal{D}_x$ (respectively, $\mathcal{D}_{x,y}$) is an extension of Π_X (respectively, G_k) by M_X. Similarly, if $D = \sum_i m_i.x_i$, $E = \sum_j n_j.y_j$ are divisors on X supported on k-rational points, then set

$$\mathcal{D}_D \stackrel{\text{def}}{=} \sum_i m_i.\mathcal{D}_{x_i}, \ \mathcal{D}_{D,E} \stackrel{\text{def}}{=} \sum_{i,j} m_i.n_j.\mathcal{D}_{x_i,y_j}$$

where the sums are to be understood as sums of extensions of Π_X, G_k, respectively, by M_X, i.e., the sums are induced by the additive structure of M_X.

For a finite subset $S \subset X(k)$, we shall write

$$\mathcal{D}_S \stackrel{\text{def}}{=} \prod_{x \in S} \mathcal{D}_x$$

where the product is to be understood as a fiber product over Π_X. Thus, $\mathcal{D}_S$ is an extension of Π_X by a product of copies of M_X indexed by the points of S. We shall refer to $\mathcal{D}_S$ as the S-cuspidalization of Π_X. Observe that if $S' \subset X(k)$ is a finite subset containing S, then we obtain a natural projection morphism $\mathcal{D}_{S'} \to \mathcal{D}_S$. More generally, for a finite subset $S \subset X^{\mathrm{cl}}$ which does not necessarily consist of k-rational points, one can still construct the object $\mathcal{D}_S$ by passing to a finite extension k_S of k over which the points of S are rational, performing the above construction over k_S, and then descending to k. (See [Mochizuki2], Remark 5 for more details.)

Proposition 2.4 (Maximal Geometrically Cuspidally Central Quotients)**.** (i) *For $S \subset X^{\mathrm{cl}}$ a finite subset, the S-cuspidalization $\mathcal{D}_S$ of Π_X may be identified with the quotient $\Pi_{U_S} \twoheadrightarrow \Pi_{U_S}^{\text{c-cn}} \stackrel{\text{def}}{=} \Pi_{U_S} / \operatorname{Ker}(\Delta_{U_S} \twoheadrightarrow \Delta_{U_S}^{\text{c-cn}})$ of Π_{U_S}, where $\Delta_{U_S}^{\text{c-cn}}$ is the maximal cuspidally central quotient of Δ_{U_S} relative to the natural map $\Delta_{U_S} \twoheadrightarrow \Delta_X$.*
(ii) *The fundamental extension $\mathcal{D}$ may be identified with the quotient $\Pi_{X \times X} \twoheadrightarrow \Pi_{U_{X \times X}}^{\text{c-cn}} \stackrel{\text{def}}{=} \Pi_{U_{X \times X}} / \operatorname{Ker}(\Delta_{U_{X \times X}} \twoheadrightarrow \Delta_{U_{X \times X}}^{\text{c-cn}})$ of $\Pi_{U_{X \times X}}$, where $\Delta_{U_{X \times X}}^{\text{c-cn}}$ is the maximal cuspidally central quotient of $\Delta_{U_{X \times X}}$ relative to the natural map $\Delta_{U_{X \times X}} \twoheadrightarrow \Delta_{X \times X}$.*

Proof. See [Mochizuki2], Proposition 1.6(iii)(iv). (Precisely speaking, Proposition 1.6(iii) loc. cit. only treats the special case where $S \subset X(k)$

holds. However, the proof for the general case is easily reduced to this special case by passing to a finite extension of k. cf. Remark 5 loc. cit.) □

Remark 2.5. Let $\mathcal{D}$ (respectively, $\mathcal{E}$) be a fundamental extension of X (respectively, Y). The isomorphism $\alpha : \Pi_X \xrightarrow{\sim} \Pi_Y$ induces an isomorphism:

$$\mathcal{D} \xrightarrow{\sim} \mathcal{E}$$

up to cyclotomically inner automorphisms (i.e., inner automorphisms by elements of M_X, M_Y) and the actions of $(k_X^\times)^{\Sigma_X^\dagger}, (k_Y^\times)^{\Sigma_Y^\dagger}$, where $(k_X^\times)^{\Sigma_X^\dagger}$ (respectively, $(k_Y^\times)^{\Sigma_Y^\dagger}$) is the maximal $\Sigma_X^\dagger$- (respectively, $\Sigma_Y^\dagger$-) quotient of $k_X^\times$ (respectively, $k_Y^\times$) (cf. [Mochizuki2], Proposition 1.4(ii)). Moreover, let $S \subset X^{\mathrm{cl}} \setminus E_X$ and $T \subset Y^{\mathrm{cl}} \setminus E_Y$ be as in Corollary 2.3 and write $\mathcal{D}_S$ (respectively, $\mathcal{E}_T$) for the S-cuspidalization of Π_X (respectively, the T-cuspidalization of Π_Y). Then the isomorphism $\mathcal{D} \xrightarrow{\sim} \mathcal{E}$ induces an isomorphism

$$\mathcal{D}_S \xrightarrow{\sim} \mathcal{E}_T$$

lying over α.

On the other hand, let $\Pi_{U_S} \twoheadrightarrow \Pi_{U_S}^{\text{c-cn}}$ and $\Pi_{V_T} \twoheadrightarrow \Pi_{V_T}^{\text{c-cn}}$ be the maximal geometrically cuspidally central quotients (here, $U_S \overset{\text{def}}{=} X \setminus S$, $V_T \overset{\text{def}}{=} Y \setminus T$) (cf. Proposition 2.4). Note that the isomorphism $\alpha_{S,T}^{\text{c-ab}} : \Pi_{U_S}^{\text{c-ab}} \xrightarrow{\sim} \Pi_{V_T}^{\text{c-ab}}$ in Corollary 2.3 naturally induces an isomorphism

$$\Pi_{U_S}^{\text{c-cn}} \xrightarrow{\sim} \Pi_{V_T}^{\text{c-cn}}$$

lying over α, which is well-defined up to cuspidally inner automorphism. Now, by Proposition 2.4(i), $\Pi_{U_S}^{\text{c-cn}}$ (respectively, $\Pi_{V_T}^{\text{c-cn}}$) may be identified with $\mathcal{D}_S$ (respectively, $\mathcal{E}_T$). Thus, we deduce another isomorphism

$$\mathcal{D}_S \xrightarrow{\sim} \mathcal{E}_T$$

lying over α.

Now, the above two isomorphisms between $\mathcal{D}_S$ and $\mathcal{E}_T$ coincide with each other up to cyclotomically inner automorphisms and the actions of $(k_X^\times)^{\Sigma_X^\dagger}$, $(k_Y^\times)^{\Sigma_Y^\dagger}$.

Another main result of Mochizuki's theory is the following, which allows us to recover φ-group-theoretically the maximal cuspidally pro-l extension of Π_X, in the case where the set of cusps consists of a single rational point.

Theorem 2.6 (Reconstruction of Maximal Cuspidally Pro-l Extensions)**.** *Let $x_* \in X(k_X)$, $y_* \in Y(k_Y)$, and set $S \overset{\text{def}}{=} \{x_*\}$, $T \overset{\text{def}}{=} \{y_*\}$, $U_S \overset{\text{def}}{=} X \smallsetminus S$, $V_T \overset{\text{def}}{=} Y \smallsetminus T$. Assume that the Frobenius-preserving isomorphism $\alpha : \Pi_X \overset{\sim}{\to} \Pi_Y$ maps the decomposition group of x_* in Π_X (which is well-defined up to conjugation) to the decomposition group of y_* in Π_Y (which is well-defined up to conjugation). Set $\Sigma \overset{\text{def}}{=} \Sigma_X = \Sigma_Y$ and $p \overset{\text{def}}{=} p_X = p_Y$. Then, for each prime $l \in \Sigma^\dagger$ (thus, $l \neq p$), there exists a commutative diagram:*

$$\begin{tikzcd}
\Pi_{U_S}^{\text{c-}l} \arrow[r, "\alpha^{\text{c-}l}"] \arrow[d] & \Pi_{V_T}^{\text{c-}l} \arrow[d] \\
\Pi_X \arrow[r, "\alpha"] & \Pi_Y
\end{tikzcd}$$

in which $\Pi_{U_S} \twoheadrightarrow \Pi_{U_S}^{\text{c-}l}$, $\Pi_{V_T} \twoheadrightarrow \Pi_{V_T}^{\text{c-}l}$ are the maximal cuspidally pro-l quotients (relative to the maps $\Pi_{U_S} \twoheadrightarrow \Pi_X$, $\Pi_{V_T} \twoheadrightarrow \Pi_Y$, respectively), the vertical arrows are the natural surjections, and $\alpha^{\text{c-}l}$ is an isomorphism well-defined up to composition with a cuspidally inner automorphism (i.e., an inner automorphism by an element of $\text{Ker}(\Pi_{V_T}^{\text{c-}l} \to \Pi_Y)$*), which is compatible relative to the natural surjections*

$$\Pi_{U_S}^{\text{c-}l} \twoheadrightarrow \Pi_{U_S}^{\text{c-ab},l}, \qquad \Pi_{V_T}^{\text{c-}l} \twoheadrightarrow \Pi_{V_T}^{\text{c-ab},l},$$

*where the subscript "*c-ab*, l" denotes the maximal cuspidally pro-l abelian quotient, with the isomorphism*

$$\alpha_{S,T}^{\text{c-ab}} : \Pi_{U_S}^{\text{c-ab}} \overset{\sim}{\to} \Pi_{V_T}^{\text{c-ab}}$$

in Corollary 2.3*. Moreover, $\alpha^{\text{c-}l}$ is compatible, up to cuspidally inner automorphisms, with the decomposition groups of x_*, y_* in $\Pi_{U_S}^{\text{c-}l}$, $\Pi_{V_T}^{\text{c-}l}$.*

Proof. See [Mochizuki2], Theorem 3.1. □

§3. Kummer Theory and Anabelian Geometry

We maintain the notations of §2. If n is an integer all of whose prime factors belong to $\Sigma^\dagger$, then we have the Kummer exact sequence

$$1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1,$$

where $\mathbb{G}_m \to \mathbb{G}_m$ is the n-th power map. We shall identify μ_n with M_X/nM_X according to the identification in [Mochizuki2], the discussion at the beginning of §2.

Consider a subset

$$E \subset X^{\mathrm{cl}}.$$

(We will set $E = E_X$ eventually, but E is arbitrary for the present.) Let $S \subset X^{\mathrm{cl}} \smallsetminus E$ be a finite set. If we consider the above Kummer exact sequence on the étale site of $U_S \overset{\mathrm{def}}{=} X \smallsetminus S$ and pass to the inverse limit with respect to n, then we obtain a natural homomorphism

$$\Gamma(U_S, \mathcal{O}_{U_S}^{\times}) \to H^1(\Pi_{U_S}, M_X)$$

(cf. loc. cit.). (Note that here it suffices to consider the group cohomology of Π_{U_S} (i.e., as opposed to the étale cohomology of U_S), since the extraction of n-th roots of an element of $\Gamma(U_S, \mathcal{O}_{U_S}^{\times})$ yields finite étale coverings of U_S that correspond to open subgroups of Π_{U_S}.) Observe that this homomorphism is injective if $\Sigma^{\dagger} = \mathfrak{Primes} \smallsetminus \{p\}$, since the abelian group $\Gamma(U_S, \mathcal{O}_{U_S}^{\times})$ is finitely generated and free of p-torsion, hence injects into its pro-prime-to-p completion.

In particular, by allowing S to vary among all finite subsets of $X^{\mathrm{cl}} \smallsetminus E$, we obtain a natural homomorphism

$$\mathcal{O}_E^{\times} \to \varinjlim_{S} H^1(\Pi_{U_S}, M_X),$$

where

$$\mathcal{O}_E^{\times} \overset{\mathrm{def}}{=} \{f \in K_X^{\times} \mid \mathrm{supp}(\mathrm{div}(f)) \cap E = \emptyset\}$$

is the multiplicative group of the units in the ring $\mathcal{O}_E$ of functions on X which are regular at all points of E. (Here, K_X denotes the function field of X.) Observe that this homomorphism is injective if $\Sigma^{\dagger} = \mathfrak{Primes} \smallsetminus \{p\}$.

Proposition 3.1 (Kummer Classes of Functions)**.** *Suppose that $S \subset X^{\mathrm{cl}} \smallsetminus E$ is a finite subset. Write*

$$\Delta_{U_S} \twoheadrightarrow \Delta_{U_S}^{\text{c-ab}} \twoheadrightarrow \Delta_{U_S}^{\text{c-cn}}$$

for the maximal cuspidally abelian and the maximal cuspidally central quotients, respectively, relative to the map $\Delta_{U_S} \twoheadrightarrow \Delta_X$, and

$$\Pi_{U_S} \twoheadrightarrow \Pi_{U_S}^{\text{c-ab}} \twoheadrightarrow \Pi_{U_S}^{\text{c-cn}}$$

for the corresponding quotients of Π_{U_S} (i.e., $\Pi_{U_S}^{\text{c-ab}} \overset{\mathrm{def}}{=} \Pi_{U_S}/\operatorname{Ker}(\Delta_{U_S} \twoheadrightarrow \Delta_{U_S}^{\text{c-ab}})$, $\Pi_{U_S}^{\text{c-cn}} \overset{\mathrm{def}}{=} \Pi_{U_S}/\operatorname{Ker}(\Delta_{U_S} \twoheadrightarrow \Delta_{U_S}^{\text{c-cn}})$). If $x \in X^{\mathrm{cl}}$, then we shall write

$$D_x[U_S] \subset \Pi_{U_S}$$

for the decomposition group at x *in* Π_{U_S} (*which is well-defined up to conjugation*), *and* $I_x[U_S] \overset{\text{def}}{=} D_x[U_S] \cap \Delta_{U_S}$ *for the inertia subgroup of* $D_x[U_S]$. *Thus, when* $x \in S$ *we have a natural isomorphism of* M_X *with* $I_x[U_S]$ (*cf.* [Mochizuki2], *Proposition* 1.5(ii)(iii)). *Then*:

(i) *The natural surjections induce the following isomorphisms*:

$$H^1(\Pi_{U_S}^{\text{c-cn}}, M_X) \xrightarrow{\sim} H^1(\Pi_{U_S}^{\text{c-ab}}, M_X) \xrightarrow{\sim} H^1(\Pi_{U_S}, M_X)$$

In particular, we obtain the following natural homomorphisms:

$$\Gamma(U_S, \mathcal{O}_{U_S}^\times) \to H^1(\Pi_{U_S}^{\text{c-cn}}, M_X) \xrightarrow{\sim} H^1(\Pi_{U_S}^{\text{c-ab}}, M_X) \xrightarrow{\sim} H^1(\Pi_{U_S}, M_X),$$

$$\mathcal{O}_E^\times \to \varinjlim_S H^1(\Pi_{U_S}^{\text{c-cn}}, M_X) \xrightarrow{\sim} \varinjlim_S H^1(\Pi_{U_S}^{\text{c-ab}}, M_X) \xrightarrow{\sim} \varinjlim_S H^1(\Pi_{U_S}, M_X),$$

where S *varies among all finite subsets of* $X \smallsetminus E$.

These natural homomorphisms are injective, if, moreover, $\Sigma^\dagger = \mathfrak{Primes} \smallsetminus \{p\}$.

(ii) *Restricting cohomology classes of* Π_{U_S} *to the various* $I_x[U_S]$ *for* $x \in S$ *yields a natural exact sequence*:

$$1 \to (k^\times)^{\Sigma^\dagger} \to H^1(\Pi_{U_S}, M_X) \to (\bigoplus_{s \in S} \hat{\mathbb{Z}}^{\Sigma^\dagger})$$

(*where we identify* $\operatorname{Hom}_{\hat{\mathbb{Z}}^{\Sigma^\dagger}}(I_x[U_S], M_X)$ *with* $\hat{\mathbb{Z}}^{\Sigma^\dagger}$). *Moreover, the image* (*via the natural homomorphism given in* (i)) *of* $\Gamma(U_S, \mathcal{O}_{U_S}^\times)$ *in* $H^1(\Pi_{U_S}, M_X)$ *is equal to the inverse image in* $H^1(\Pi_{U_S}, M_X)$ *of the submodule of*

$$(\bigoplus_{s \in S} \mathbb{Z}) \subset (\bigoplus_{s \in S} \hat{\mathbb{Z}}^{\Sigma^\dagger})$$

determined by the principal divisors (*with support in* S). *A similar statement holds when* Π_{U_S} *is replaced by* $\Pi_{U_S}^{\text{c-cn}}$ *or* $\Pi_{U_S}^{\text{c-ab}}$.

(iii) *If* $f \in \Gamma(U_S, \mathcal{O}_{U_S}^\times)$, *write*

$$\kappa_f^{\text{c-cn}} \in H^1(\Pi_{U_S}^{\text{c-cn}}, M_X), \quad \kappa_f^{\text{c-ab}} \in H^1(\Pi_{U_S}^{\text{c-ab}}, M_X), \quad \kappa_f \in H^1(\Pi_{U_S}, M_X)$$

for the associated Kummer classes. If $x \in (X^{\text{cl}} \smallsetminus E) \smallsetminus S$, *then* $D_x[U_S]$ *maps, via the natural surjection* $\Pi_{U_S} \twoheadrightarrow G_k$, *isomorphically onto the open subgroup* $G_{k(x)} \subseteq G_k$ (*where* $k(x)$ *is the residue field of* X *at* x). *Moreover, the images of the pulled back classes*

$$\kappa_f^{\text{c-cn}}|_{D_x[U_S]} = \kappa_f^{\text{c-ab}}|_{D_x[U_S]} = \kappa_f|_{D_x[U_S]} \in H^1(D_x[U_S], M_X) \simeq H^1(G_{k(x)}, M_X) \simeq (k(x)^\times)^{\Sigma^\dagger}$$

in $(k(x)^{\times})^{\Sigma^{\dagger}}$ *are equal to the image in* $(k(x)^{\times})^{\Sigma^{\dagger}}$ *of the value* $f(x) \in k(x)^{\times}$ *of* f *at* x*.*

Proof. See [Mochizuki2], Proposition 2.1. (Strictly speaking, Proposition 2.1(ii) loc. cit. only treats the case where $S \subset X(k)$, but the same proof works well for the general case.) □

Remark 3.2 (cf. [Mochizuki2], Remark 12). In the situation of Proposition 3.1(iii), assume $x \in X(k)$ and $S \subset X(k)$ for simplicity. If we think of the extension $\Pi_{U_S}^{\text{c-cn}}$ of Π_X as being given by the extension $\mathcal{D}_S$, where $\mathcal{D}$ is a fundamental extension of $\Pi_{X\times X}$ (cf. Proposition 2.4(i)), then it follows that the image of $D_x[U_S]$ in $\Pi_{U_S}^{\text{c-cn}}$ may be thought of as the image of $D_x[U_S]$ in $\mathcal{D}_S$. This image of $D_x[U_S]$ in $\mathcal{D}_S$ amounts to a section of $\mathcal{D}_S \twoheadrightarrow \Pi_X \twoheadrightarrow G_k$ lying over the section $s_x : G_k \to \Pi_X$ corresponding to the rational point x (which is well-defined up to conjugation). Since $\mathcal{D}_S$ is defined as a certain fiber product, this section is equivalent to a collection of sections (regarded as "cyclotomically outer homomorphisms", i.e., well-defined up to composition with an inner automorphism of $\mathcal{D}_{y,x}$ by an element of $\mathrm{Ker}(\mathcal{D}_{y,x} \twoheadrightarrow G_k)$)

$$\gamma_{y,x} : G_k \to \mathcal{D}_{y,x},$$

where y ranges over all points of S. Namely, from this point of view, Proposition 3.1(iii) may be regarded as saying that the image in $(k(x)^{\times})^{\Sigma^{\dagger}} = (k^{\times})^{\Sigma^{\dagger}}$ of the value $f(x)$ of the function $f \in \Gamma(U_S, \mathcal{O}_{U_S}^{\times})$ at $x \in X(k)$ may be computed from its Kummer class, as soon as one knows the sections $\gamma_{y,x} : G_k \to \mathcal{D}_{y,x}$ for $y \in S$. Observe that $\gamma_{y,x}$ depends only on x, y, and not on the choice of S.

Definition 3.3 (cf. [Mochizuki2], Definition 2.1)**.** For $x, y \in X(k)$ with $x \neq y$, we shall refer to the above section (regarded as a cyclotomically outer homomorphism)

$$\gamma_{y,x} : G_k \to \mathcal{D}_{y,x}$$

as the Green's trivialization of $\mathcal{D}$ at (y, x). If D is a divisor on X supported on k-rational points $\neq x$, then multiplication of the various Green's trivializations for the points in the support of D yields a section (regarded as a cyclotomically outer homomorphism)

$$\gamma_{D,x} : G_k \to \mathcal{D}_{D,x}$$

which we shall refer to as the Green's trivialization of $\mathcal{D}$ at (D, x).

Definition 3.4 (cf. [Mochizuki2], Definition 2.2)**.** Let the notations and the assumptions as in Corollary 2.3.
(i) Write $\mathcal{D}$ (respectively, $\mathcal{E}$) for the fundamental extension of $\Pi_{X\times X}$ (respectively, $\Pi_{Y\times Y}$) that arises as the quotient of $\Pi^{\text{c-ab}}_{U_{X\times X}}$ (respectively, $\Pi^{\text{c-ab}}_{U_{Y\times Y}}$) by the kernel of the maximal cuspidally central quotient $\Delta^{\text{c-ab}}_{U_{X\times X}} \twoheadrightarrow \Delta^{\text{c-cn}}_{U_{X\times X}}$ (respectively, $\Delta^{\text{c-ab}}_{U_{Y\times Y}} \twoheadrightarrow \Delta^{\text{c-cn}}_{U_{Y\times Y}}$) (cf. Proposition 2.4(ii)). The isomorphism $\alpha^{\text{c-ab}}$ induces naturally an isomorphism:

$$\alpha^{\text{c-cn}} : \mathcal{D} \xrightarrow{\sim} \mathcal{E}$$

We shall say that α is (S,T)-locally Green-compatible outside exceptional sets if, for every pair of points $(x_1,x_2) \in X(k_X) \times X(k_X)$ corresponding via ϕ to a pair of points $(y_1,y_2) \in Y(k_Y) \times Y(k_Y)$, such that $x_1 \in (X^{\text{cl}} \smallsetminus E_X) \smallsetminus S$, $y_1 \in (Y^{\text{cl}} \smallsetminus E_Y) \smallsetminus T$, $x_2 \in S$, $y_2 \in T$, the isomorphism

$$\mathcal{D}_{x_1,x_2} \xrightarrow{\sim} \mathcal{E}_{y_1,y_2}$$

(obtained by restricting $\alpha^{\text{c-cn}}$ to the various decomposition groups) is compatible with the Green's trivializations. We shall say that α is (S,T)-locally principally Green-compatible outside exceptional sets if, for every point $x \in X(k_X) \cap S$ and every principal divisor D supported on k_X-rational points $\neq x$ contained in $X^{\text{cl}} \smallsetminus E_X$, corresponding via ϕ to a pair (y,E) (so $y \in Y(k_Y) \cap T$), the isomorphism

$$\mathcal{D}_{D,x} \xrightarrow{\sim} \mathcal{E}_{E,y}$$

obtained from $\alpha^{\text{c-cn}}$ is compatible with the Green's trivializations.
(ii) We shall say that α is totally globally Green-compatible (respectively, totally globally principally Green-compatible) outside exceptional sets if, for all pair of connected finite étale coverings $\xi : X' \to X$, $\eta : Y' \to Y$ that arise from open subgroups $\Pi_{X'} \subseteq \Pi_X$, $\Pi_{Y'} \subseteq \Pi_Y$, corresponding to each other via α, then for any subset $S \subset X^{\text{cl}} \smallsetminus E_X$ that corresponds, via ϕ, to $T \subset Y \smallsetminus E_Y$ the isomorphism

$$\Pi_{X'} \xrightarrow{\sim} \Pi_{Y'}$$

induced by α is (S',T')-locally Green-compatible (respectively, (S',T')-locally principally Green-compatible) outside exceptional sets, where $S' \overset{\text{def}}{=} \xi^{-1}(S) \subset X'^{\text{cl}}$, $T' \overset{\text{def}}{=} \eta^{-1}(T) \subset Y'^{\text{cl}}$ are the inverse images of S, T, respectively.

Remark/Definition 3.5. Let $J = J_X$ be the Jacobian variety of X. Let $\text{Div}^0_{X\smallsetminus E_X}$ be the group of degree zero divisors on X which are supported on points in $X \smallsetminus E_X$. Write $D_{X \smallsetminus E_X}$ for the kernel of the natural homomorphism $\mathrm{Div}^0_{X \smallsetminus E_X} \to J(k)^{\Sigma}$. Here, $J(k)^{\Sigma}$ stands for the maximal Σ-quotient $J(k)/(J(k)\{\Sigma'\})$ of $J(k)$, where, for an abelian group M, $M\{\Sigma'\}$ stands for the subgroup of torsion elements a of M such that every prime divisor of the order of a belongs to Σ'. Then $D_{X \smallsetminus E_X}$ sits naturally in the following exact sequence:

$$0 \to \mathrm{Pri}_{X \smallsetminus E_X} \to D_{X \smallsetminus E_X} \to J(k)\{\Sigma'\} \to 0,$$

where $\mathrm{Pri}_{X \smallsetminus E_X} \overset{\mathrm{def}}{=} \mathcal{O}^{\times}_{E_X}/k^{\times}$ stands for the group of principal divisors supported in $X \smallsetminus E_X$.

Theorem 3.6 (Reconstruction of Functions). *In the situation of Theorem* 2.2, *assume that α is Frobenius-preserving. Write $\Sigma \overset{\mathrm{def}}{=} \Sigma_X = \Sigma_Y$ and $p \overset{\mathrm{def}}{=} p_X = p_Y$* (*cf. Proposition* 1.15(ii)(iii)). *Then*:
(i) *The bijection $\phi : X^{\mathrm{cl}} \smallsetminus E_X \xrightarrow{\sim} Y^{\mathrm{cl}} \smallsetminus E_Y$ induced by α* (*where E_X and E_Y are the exceptional sets*) *induces a natural bijection between the groups $D_{X \smallsetminus E_X}$, $D_{Y \smallsetminus E_Y}$.*
(ii) *Assume, moreover, $\Sigma^{\dagger} = \mathfrak{Primes} \smallsetminus \{p\}$. Then the bijection in* (*i*), *together with the isomorphisms in Corollary* 2.3, *induces naturally an injective homomorphism*

$$\mathcal{O}^{\times}_{E_X} \hookrightarrow (\mathcal{O}^{\times}_{E_Y})^{p^{-n}},$$

where p^n is the exponent of the p-primary finite abelian group $J_Y(k_Y)\{\Sigma'\}$. The image $\mathrm{Im}(\mathcal{O}^{\times}_{E_X})$ of $\mathcal{O}^{\times}_{E_X}$ in $(\mathcal{O}^{\times}_{E_Y})^{p^{-n}}$ is "commensurate" to $\mathcal{O}^{\times}_{E_Y}$, i.e., the intersection $\mathrm{Im}(\mathcal{O}^{\times}_{E_X}) \cap \mathcal{O}^{\times}_{E_Y}$ has finite indices both in $\mathrm{Im}(\mathcal{O}^{\times}_{E_X})$ and in $\mathcal{O}^{\times}_{E_Y}$.

Moreover, this injective homomorphism $\mathcal{O}^{\times}_{E_X} \hookrightarrow (\mathcal{O}^{\times}_{E_Y})^{p^{-n}}$ is functorial in X, Y, in the following sense: if $\xi : X' \to X$ is a finite étale covering, arising from an open subgroup $\Pi_{X'} \subseteq \Pi_X$, which corresponds to a finite étale covering $\eta : Y' \to Y$ via α (*thus, $\Pi_{Y'} = \alpha(\Pi_{X'})$*), *then we have a commutative diagram*:

$$\begin{tikzcd}
\mathcal{O}^{\times}_{E_{X'}} \arrow[r] & (\mathcal{O}^{\times}_{E_{Y'}})^{p^{-n'}} \\
\mathcal{O}^{\times}_{E_X} \arrow[r] \arrow[u] & (\mathcal{O}^{\times}_{E_Y})^{p^{-n}} \arrow[u]
\end{tikzcd}$$

where $E_{X'} \overset{\mathrm{def}}{=} \xi^{-1}(E_X)$, $E_{Y'} \overset{\mathrm{def}}{=} \eta^{-1}(E_Y)$, $p^{n'} \geq p^n$ is the exponent of the p-primary finite abelian group $J_{Y'}(k_{Y'})\{\Sigma'\}$, and the vertical arrows are the natural embeddings.

Proof. (cf. [Mochizuki2], Theorem 2.1(ii).)

(i) First, ϕ induces naturally a bijection $\mathrm{Div}^0_{X\smallsetminus E_X} \xrightarrow{\sim} \mathrm{Div}^0_{Y\smallsetminus E_Y}$. Second, the natural homomorphism $\mathrm{Div}^0_{X\smallsetminus E_X} \to J(k_X)^{\Sigma}$ can be recovered φ-group-theoretically from Π_X. (Observe the pro-Σ version of [Mochizuki2], Proposition 2.2(i). See also the discussion before Proposition 2.2 loc. cit.) Thus, α induces naturally a commutative diagram:

$$\begin{tikzcd}
\mathrm{Div}^0_{X\smallsetminus E_X} \arrow[r] \arrow[d, "\wr"] & J_X(k_X)^{\Sigma} \arrow[d, "\wr"] \\
\mathrm{Div}^0_{Y\smallsetminus E_Y} \arrow[r] & J_Y(k_Y)^{\Sigma}
\end{tikzcd}$$

where the vertical arrows are the isomorphisms induced by α. From this diagram we deduce naturally an isomorphism $D_{X\smallsetminus E_X} \xrightarrow{\sim} D_{Y\smallsetminus E_Y}$ between the kernels of the horizontal arrows.

(ii) From the isomorphism $D_{X\smallsetminus E_X} \xrightarrow{\sim} D_{Y\smallsetminus E_Y}$, we deduce naturally an embedding $(\mathrm{Pri}_{X\smallsetminus E_X})^{p^n} (\subset \mathrm{Ker}(\mathrm{Pri}_{X\smallsetminus E_X} \to J_Y(k_Y)\{\Sigma'\})) \hookrightarrow \mathrm{Pri}_{Y\smallsetminus E_Y}$, from which we deduce an embedding $(\mathcal{O}^{\times}_{E_X})^{p^n} \hookrightarrow (\mathcal{O}^{\times}_{E_Y})$, or, equivalently, an embedding $\mathcal{O}^{\times}_{E_X} \hookrightarrow (\mathcal{O}^{\times}_{E_Y})^{p^{-n}}$, by Corollary 2.3 and Proposition 3.1(i)(ii). The desired commensurabilty follows from the fact that both $J_X(k_X)\{\Sigma'\}$ and $J_Y(k_Y)\{\Sigma'\}$ are finite. Finally, the desired commutativity of diagram follows easily from the functoriality of Kummer theory. □

Theorem 3.7 (Totally Globally Principally Green-Compatible Isomorphisms Outside Exceptional Sets)**.** *In the situation of Theorem* 3.6, *assume further that* $\Sigma^{\dagger} = \mathfrak{Primes} \smallsetminus \{p\}$, *and that* α *is totally globally principally Green-compatible outside exceptional sets. Then* α *arises from a uniquely determined commutative diagram of schemes*:

$$\begin{tikzcd}
\tilde{X} \arrow[r, "\sim"] \arrow[d] & \tilde{Y} \arrow[d] \\
X \arrow[r, "\sim"] & Y
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings determined by the groups Π_X, Π_Y.

Proof. (cf. [Mochizuki2], Corollary 2.1, Remark 22.) Let $l \neq p$ be a prime number and let k^l_X, k^l_Y be the (unique) $\mathbb{Z}_l$-extensions of k_X, k_Y, respectively. Let X^l, Y^l be the normalizations of X, Y in $K_X k^l_X$, $K_Y k^l_Y$, respectively. Then the p-primary abelian subgroups $J_X(k^l_X)\{\Sigma'\}$, $J_Y(k^l_Y)\{\Sigma'\}$ of $J_X(k^l_X)$, $J_Y(k^l_Y)$, respectively, are finite. (See, e.g., [Rosen], Theorem 11.6. Alternatively, this finiteness, say, for X follows from the fact that the profinite group $GL_N(\mathbb{Z}_p)$ is almost pro-p, i.e., admits a pro-p open subgroup. Indeed, the action of G_{k_X} on $J_X(\overline{k_X})\{\Sigma'\}$ factors through the image $\rho(G_{k_X})$ of the natural Galois representation $\rho : G_{k_X} \to \operatorname{Aut}(T_p(J_X)) \simeq GL_N(\mathbb{Z}_p)$, where $T_p(J_X)$ is the p-adic Tate module of J_X and N is the $\mathbb{Z}_p$-rank of $T_p(J_X)$. Now, since $G_{k_X}/G_{k_X^l} \simeq \mathbb{Z}_l$ and $l \neq p$, the image $\rho(G_{k_X^l})$ is open in $\rho(G_{k_X})$. Write k_X' for the finite extension of k_X corresponding to the finite quotient $G_{k_X} \twoheadrightarrow \rho(G_{k_X})/\rho(G_{k_X^l})$. Then, it is easy to see that $J_X(k_X^l)\{\Sigma'\}$ coincides with $J_X(k_X')\{\Sigma'\}$ ($\subset J_X(k_X')$), which is clearly finite.) So, write p^{n_0} for the exponent of $J_Y(k_Y^l)\{\Sigma'\}$. By passing to the limit over the finite extensions of k_X, k_Y contained in k_X^l, k_Y^l, respectively, we obtain a natural embedding $\mathcal{O}^\times_{E_{X^l}} \hookrightarrow (\mathcal{O}^\times_{E_{Y^l}})^{p^{-n_0}}$, where $\mathcal{O}^\times_{E_{X^l}}$, $\mathcal{O}^\times_{E_{Y^l}}$ are the multiplicative groups of functions on X^l, Y^l, whose divisor has support disjoint from $E_{X^l} \overset{\text{def}}{=} E_X \times_{k_X} k_X^l$, $E_{Y^l} \overset{\text{def}}{=} E_Y \times_{k_Y} k_Y^l$, respectively (cf. Theorem 3.6(ii)). (Recall that $E_X \subset X^{\text{cl}}$, $E_Y \subset Y^{\text{cl}}$ are finite by Proposition 1.8(vi).)

Now, we shall apply a result of §4. (Observe that there are no vicious circles since the discussion of §4 does not depend on the contents of earlier §§.) More specifically, by Proposition 4.4, the above embedding $\mathcal{O}^\times_{E_{X^l}} \hookrightarrow (\mathcal{O}^\times_{E_{Y^l}})^{p^{-n_0}}$ arises from a uniquely determined embedding $K_{X^l} \hookrightarrow K_{Y^l}^{p^{-n_0}}$ of function fields, where K_{X^l}, K_{Y^l} are the function fields of X^l, Y^l, respectively. (Observe that the value-preserving assumption in Proposition 4.4 is equivalent to the Green-compatibility assumption. See Remark 3.2. Observe also that $X^l(k_X^l)$ is an infinite set by the Weil estimate on numbers of rational points of curves over finite fields.) This embedding of fields restricts to the original embedding of multiplicative groups $\mathcal{O}^\times_{E_X} \hookrightarrow (\mathcal{O}^\times_{E_Y})^{p^{-n_0}}$ (i.e., the restriction of $\mathcal{O}^\times_{E_{X^l}} \hookrightarrow (\mathcal{O}^\times_{E_{Y^l}})^{p^{-n_0}}$). It also restricts to an embedding of fields $K_X \hookrightarrow K_Y^{p^{-n_0}}$. Indeed, the embedding $K_{X^l} \hookrightarrow K_{Y^l}^{p^{-n_0}}$ is Galois-equivariant with respect to the given isomorphism $\alpha : \Pi_X \overset{\sim}{\to} \Pi_Y$, hence one obtains an embedding $K_X \hookrightarrow K_Y^{p^{-n_0}}$ by taking Galois invariants. Now, by applying these arguments to $\alpha^{-1} : \Pi_Y \overset{\sim}{\to} \Pi_X$, we see that the image of the embedding $K_X \hookrightarrow K_Y^{p^{-n_0}}$ contains $K_Y^{p^{m_0}}$, where p^{m_0} is the exponent of $J_X(k_X^l)\{\Sigma'\}$. From this, we deduce that the embedding $K_X \hookrightarrow K_Y^{p^{-n_0}}$ is radicial and maps K_X isomorphically onto $K_Y^{p^s}$ for some integer $-n_0 \leq s \leq m_0$. Thus, in particular, the original embedding $\mathcal{O}^\times_{E_X} \hookrightarrow (\mathcal{O}^\times_{E_Y})^{p^{-n_0}}$ induces an isomorphism $\mathcal{O}^\times_{E_X} \overset{\sim}{\to} (\mathcal{O}^\times_{E_Y})^{p^s}$. Now, by Theorem 3.6, the image $\operatorname{Im}(\mathcal{O}^\times_{E_X})$ of $\mathcal{O}^\times_{E_X}$ in $(\mathcal{O}^\times_{E_Y})^{p^{-n_0}}$ (i.e., $(\mathcal{O}^\times_{E_Y})^{p^s}$) is commensurate to $\mathcal{O}^\times_{E_Y}$. This implies $s = 0$. That is to say, the embedding $K_X \hookrightarrow K_Y^{p^{-n_0}}$ maps K_X isomorphically onto K_Y.

If $\xi : X' \to X$ is a finite étale covering, arising from an open subgroup

$\Pi_{X'} \subseteq \Pi_X$, which corresponds to a finite étale covering $\eta : Y' \to Y$ via α (thus, $\Pi_{Y'} = \alpha(\Pi_{X'})$), then the commutative diagram in Theorem 3.6(ii), together with the above argument, induces a commutative diagram of embeddings of fields:

$$\begin{tikzcd}
K_{X'} \arrow[r, "\tau'"] & K_{Y'}^{p^{-{n_0}'}} \\
K_X \arrow[u] \arrow[r, "\tau"] & K_Y^{p^{-n_0}} \arrow[u]
\end{tikzcd}$$

where the vertical arrows are the natural embeddings, $p^{{n_0}'}$, p^{n_0} stand for the exponents of the p-primary abelian groups $J_{Y'}(k^l_{Y'})\{\Sigma'\}$, $J_Y(k^l_Y)\{\Sigma'\}$, respectively (note that $n'_0 \geq n_0$), and the horizontal arrows are the embeddings obtained above. Applying the above arguments to $\Pi_X \xrightarrow{\sim} \Pi_Y$ and $\Pi_{X'} \xrightarrow{\sim} \Pi_{Y'}$, we obtain $\tau(K_X) = K_Y$, $\tau'(K_{X'}) = K_{Y'}$. Thus, this diagram induces naturally a commutative diagram:

$$\begin{tikzcd}
K_{X'} \arrow[r, "\sim"] & K_{Y'} \\
K_X \arrow[u] \arrow[r, "\sim"] & K_Y \arrow[u]
\end{tikzcd}$$

where the vertical arrows are the natural embeddings and the horizontal arrows are isomorphisms of fields. By passing to the limit over all open subgroups of Π_X we obtain a natural commutative diagram:

$$\begin{tikzcd}
K_{\tilde{X}} \arrow[r, "\sim"] & K_{\tilde{Y}} \\
K_X \arrow[u] \arrow[r, "\sim"] & K_Y \arrow[u]
\end{tikzcd}$$

where $K_{\tilde{X}}$, $K_{\tilde{Y}}$ stand for the function fields of $\tilde{X}$, $\tilde{Y}$, respectively, the vertical arrows are the natural embeddings, and the horizontal arrows are isomorphisms of fields. This commutative diagram yields a commutative diagram of schemes as in the statement of Theorem 3.7 with the desired properties. (cf. the proof of [Tamagawa1], Theorem (6.3).) □

Proposition 3.8 (Total Global Green-Compatibility Outside Exceptional Sets). *In the situation of Theorem* 2.2, *assume further that α is Frobenius-preserving. Then the isomorphism α is totally globally Green-compatible outside* *exceptional sets. In particular, if* Σ *is of density* 1*, then* α *is totally globally Green-compatible outside exceptional sets.*

Proof. For the first assertion, the proof of [Mochizuki2], Corollary 3.1 (where $\Sigma^\dagger = \mathfrak{Primes}^\dagger$ and $E_X = E_Y = \emptyset$ are assumed) also works well in this case. (Thus, the main ingredient of the proof is Theorem 2.6.) The second assertion follows from the first, together with Proposition 1.15(viii). □

Theorem 3.9 (A Prime-to-p Version of Grothendieck's Anabelian Conjecture for Proper Hyperbolic Curves over Finite Fields). *Let* X *and* Y *be proper hyperbolic curves over finite fields* k_X, k_Y*, respectively. Let* Σ_X, Σ_Y *be subsets of* $\mathfrak{Primes}$*, and assume* $\Sigma_X^\dagger \overset{\text{def}}{=} \Sigma_X \setminus \{\text{char}(k_X)\} = \mathfrak{Primes} \setminus \{\text{char}(k_X)\}$, $\Sigma_Y^\dagger \overset{\text{def}}{=} \Sigma_Y \setminus \{\text{char}(k_Y)\} = \mathfrak{Primes} \setminus \{\text{char}(k_Y)\}$*. Write* Π_X, Π_Y *for the geometrically pro-*Σ_X *étale fundamental group of* X*, the geometrically pro-*Σ_Y *étale fundamental group of* Y*, respectively. Let*

$$\alpha : \Pi_X \xrightarrow{\sim} \Pi_Y$$

be an isomorphism of profinite groups. Then α *arises from a uniquely determined commutative diagram of schemes*:

$$\begin{tikzcd}
\tilde{X} \arrow[r, "\sim"] \arrow[d] & \tilde{Y} \arrow[d] \\
X \arrow[r, "\sim"] & Y
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups Π_X, Π_Y.

Proof. Follows formally from Theorem 3.7 and Proposition 3.8. □

As a consequence of Theorem 3.9, we deduce the following:

Corollary 3.10 (A Prime-to-p Version of Grothendieck's Anabelian Conjecture for (Not Necessarily Proper) Hyperbolic Curves over Finite Fields). *Let* U, V *be* (*not necessarily proper*) *hyperbolic curves over finite fields* k_U, k_V*, respectively. Let* Σ_U, Σ_V *be subsets of* $\mathfrak{Primes}$*, and assume* $\Sigma_U^\dagger \overset{\text{def}}{=} \Sigma_U \setminus \{\text{char}(k_U)\} = \mathfrak{Primes} \setminus \{\text{char}(k_U)\}$, $\Sigma_V^\dagger \overset{\text{def}}{=} \Sigma_V \setminus \{\text{char}(k_V)\} = \mathfrak{Primes} \setminus \{\text{char}(k_V)\}$*. Write* Π_U, Π_V *for the geometrically pro-*Σ_U *tame fundamental group of* U*, the geometrically pro-*Σ_V *tame fundamental group of* V*, respectively. Let*

$$\alpha : \Pi_U \xrightarrow{\sim} \Pi_V$$

be an isomorphism of profinite groups. Then α arises from a uniquely determined commutative diagram of schemes:

$$\begin{tikzcd}
\tilde{U} \arrow[r, "\sim"] \arrow[d] & \tilde{V} \arrow[d] \\
U \arrow[r, "\sim"] & V
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups Π_U, Π_V.

Proof. Let $U' \to U$, $V' \to V$ be any finite étale Galois coverings arising from the open normal subgroups $\Pi_{U'} \subseteq \Pi_U$, $\Pi_{V'} \subseteq \Pi_V$, which correspond to each other via α, such that the smooth compactifications X', Y' of U', V', respectively, are hyperbolic, and that the coverings $\xi : X' \to X$, $\eta : Y' \to Y$, where X, Y are the smooth compactifications of U, V, respectively, are ramified above all the points of $S \overset{\text{def}}{=} X \smallsetminus U$, $T \overset{\text{def}}{=} Y \smallsetminus V$, respectively. (Observe that such $U' \to U$, $V' \to V$ are cofinal in the finite étale coverings arising from open subgroups of Π_U, Π_V, respectively.) Thus, the isomorphism $\alpha : \Pi_U \overset{\sim}{\to} \Pi_V$ restricts to an isomorphism $\alpha' : \Pi_{U'} \overset{\sim}{\to} \Pi_{V'}$. By Proposition 1.15(vi)(viii), α' induces naturally an isomorphism $\tilde{\alpha}' : \Pi_{X'} \overset{\sim}{\to} \Pi_{Y'}$, which fits into the following commutative diagram:

$$\begin{tikzcd}
\Pi_{U'} \arrow[r, "\alpha'"] \arrow[d] & \Pi_{V'} \arrow[d] \\
\Pi_{X'} \arrow[r, "\tilde{\alpha}'"] & \Pi_{Y'}
\end{tikzcd}$$

in which the vertical maps are the natural surjections.

By Theorem 3.9, the isomorphism $\tilde{\alpha}'$ arises from a uniquely determined commutative diagram of schemes:

$$\begin{tikzcd}
\tilde{X}' \arrow[r, "\sim"] \arrow[d] & \tilde{Y}' \arrow[d] \\
X' \arrow[r, "\sim"] & Y'
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups $\Pi_{X'}$, $\Pi_{Y'}$. Since $\tilde{\alpha}' : \Pi_{X'} \overset{\sim}{\to} \Pi_{Y'}$ is equivariant with respect to $\alpha : \Pi_U \overset{\sim}{\to} \Pi_V$, this last diagram is also equivariant with respect to $\alpha : \Pi_U \overset{\sim}{\to} \Pi_V$. Thus, by dividing by the actions of Π_U, Π_V, we see that it induces naturally a commutative diagram of schemes:

$$\begin{tikzcd}
X' \arrow[r, "\sim"] \arrow[d, "\xi"] & Y' \arrow[d, "\eta"] \\
X \arrow[r, "\sim"] & Y
\end{tikzcd}$$

The commutativity of this diagram forces the isomorphisms $X' \xrightarrow{\sim} Y'$ and $X \xrightarrow{\sim} Y$ to preserve the sets of ramified points of ξ, η. Thus, by the choice of ξ, η, this diagram induces a commutative diagram of schemes:

$$\begin{tikzcd}
U' \arrow[r, "\sim"] \arrow[d, "\xi"] & V' \arrow[d, "\eta"] \\
U \arrow[r, "\sim"] & V
\end{tikzcd}$$

Finally, by considering this last commutative diagram for any coverings $U' \to U$, $V' \to V$ as above, we obtain a commutative diagram of schemes in the assertion of Corollary 3.10, with desired properties. (cf. the proof of [Tamagawa1], Theorem (6.3).) □

Finally, we deduce from our main result a prime-to-p birational version of Grothendieck's anabelian conjecture for (function fields of) curves over finite fields (see Corollary 3.11 below).

Let X be a proper, smooth, geometrically connected curve over a finite field $k = k_X$ of characteristic $p = p_X > 0$. Let K_X be the function field of X. Let $G_{K_X} \overset{\text{def}}{=} \mathrm{Gal}(K_X^{\mathrm{sep}}/K_X)$ be the absolute Galois group of K_X (where K_X^{sep} is a separable closure of K_X), which sits naturally in the following exact sequence:

$$1 \to G_{K_{\overline{X}}} \to G_{K_X} \to G_k \overset{\text{def}}{=} \mathrm{Gal}(\overline{k}/k) \to 1,$$

where $G_{K_{\overline{X}}} \overset{\text{def}}{=} \mathrm{Gal}(K_X^{\mathrm{sep}}/K_{\overline{X}})$ is the absolute Galois group of the function field $K_{\overline{X}}$ of $\overline{X} \overset{\text{def}}{=} X \times_k \overline{k}$, and $G_k \overset{\text{def}}{=} \mathrm{Gal}(\overline{k}/k)$ is the absolute Galois group of k (here, $\overline{k}$ is the algebraic closure of k in K_X^{sep}). Let $\Gamma_{K_{\overline{X}}}$ be the maximal prime-to-p quotient of $G_{K_{\overline{X}}}$, and let $\Gamma_{K_X} \overset{\text{def}}{=} G_{K_X} / \mathrm{Ker}(G_{K_{\overline{X}}} \twoheadrightarrow \Gamma_{K_{\overline{X}}})$ be the corresponding quotient of G_{K_X}. We shall refer to Γ_{K_X} as the geometrically pro-prime-to-characteristic quotient of G_{K_X}. As an important consequence of Corollary 3.10, we deduce the following prime-to-p version of Uchida's Theorem on isomorphisms between absolute Galois groups of function fields (cf. [Uchida]).

Corollary 3.11 (A Prime-to-p Version of Uchida's Theorem)**.** *Let X, Y be proper, smooth, geometrically connected curves over finite fields k_X, k_Y, respectively. Let K_X, K_Y be the function fields of X, Y, respectively. Let G_{K_X}, G_{K_Y} be the absolute Galois groups of K_X, K_Y, respectively, and let Γ_{K_X}, Γ_{K_Y} be their geometrically prime-to-characteristic quotients, respectively. Let*

$$\alpha : \Gamma_{K_X} \xrightarrow{\sim} \Gamma_{K_Y}$$

be an isomorphism of profinite groups. Then α arises from a uniquely determined commutative diagram:

$$\begin{tikzcd}
(K_X)^\sim \arrow[r, "\sim"] & (K_Y)^\sim \\
K_X \arrow[u] \arrow[r, "\sim"] & K_Y \arrow[u]
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms and the vertical arrows are the extensions corresponding to the groups Γ_{K_X}, Γ_{K_Y}, respectively.

Proof. Following the arguments of [Uchida], Lemma 3 (involving Brauer groups), one can establish a bijection $\phi : X^{\mathrm{cl}} \xrightarrow{\sim} Y^{\mathrm{cl}}$ such that $\alpha(D_x) = D_{\phi(x)}$ holds for each $x \in X^{\mathrm{cl}}$, where D_x stands for the decomposition group of Γ_{K_X} at x (which is well-defined up to conjugation). Further, $\alpha(I_x) = I_{\phi(x)}$ also holds for each $x \in X^{\mathrm{cl}}$, where I_x stands for the inertia subgroup of D_x by the same argument (involving local class field theory) as in the proof of Lemma 4 loc. cit. Let $S \subset X^{\mathrm{cl}}$ be a finite subset such that $U \overset{\mathrm{def}}{=} X \smallsetminus S$ is hyperbolic. Let $T \overset{\mathrm{def}}{=} \phi(S)$ and $V \overset{\mathrm{def}}{=} Y \smallsetminus T$. Then α induces naturally an isomorphism $\Pi_U \xrightarrow{\sim} \Pi_V$ between the geometrically prime-to-characteristic quotients of $\pi_1(U)$, $\pi_1(V)$, respectively. The latter arises, by Corollary 3.10, from a uniquely determined commutative diagram of schemes:

$$\begin{tikzcd}
\tilde{U} \arrow[r, "\sim"] \arrow[d] & \tilde{V} \arrow[d] \\
U \arrow[r, "\sim"] & V
\end{tikzcd}$$

By considering this commutative diagram for all finite subsets $S \subset X^{\mathrm{cl}}$, $T \subset Y^{\mathrm{cl}}$ as above, we obtain a commutative diagram of field extensions in the assertion of Corollary 3.11 with desired properties. □

Remark 3.12. As was communicated to the authors by the referee, in the above proof of Corollary 3.11, one may also recover the decomposition groups of points, say, for X, as follows: First, one recovers the quotient G_{k_X} of Γ_{K_X} by abelianizing and dividing by the closure of torsion. In particular, one recovers the characteristic $p = p_X$ of k_X as the unique prime number l such that the maximal pro-l quotient $\Gamma^l_{K_{\overline{X}}}$ of the geometric part $\Gamma_{K_{\overline{X}}} \overset{\text{def}}{=} \operatorname{Ker}(\Gamma_{K_X} \twoheadrightarrow G_{k_X})$ is topologically finitely generated. Next, for any prime number $l \neq p$, one recovers the pro-l cyclotomic character up to multiplication by a character of finite order as a character χ such that the action of G_{k_X} on the abelianization $\Gamma^{l,\mathrm{ab}}_{K_{\overline{X}}}$ of $\Gamma^l_{K_{\overline{X}}}$ has the property that the closure of the union of the χ-eigenspaces for open subgroups of G_{k_X} is not topologically finitely generated. Then one recovers the genus of X as the $\mathbb{Z}_l$-rank of the quotient of $\Gamma^{l,\mathrm{ab}}_{K_{\overline{X}}}$ by this closure. Once one has the genus, the rest of the reconstruction of the decomposition groups of points is "standard" (cf. Proposition 1.15 and Theorem 1.18).

Remark 3.13. In [Stix1], [Stix 2], Stix proved a certain relative version of Grothendieck's anabelian conjecture for hyperbolic curves over finitely generated fields in positive characteristics. His proof relies on (the absolute version of) Grothendieck's anabelian conjecture for affine hyperbolic curves over the prime field, proved by Tamagawa in [Tamagawa1]. Using the same arguments as in [Stix1], one should be able to prove a "prime-to-characteristic" relative version of Grothendieck's anabelian conjecture for hyperbolic curves over finitely generated fields in positive characteristics, by reducing it to our main results in Theorem 3.9 and Corollary 3.10.

Remark 3.14. Even after Theorem 3.9 and Corollary 3.10 are established, it is still unclear to the authors, at the time of writing, whether or not $E_X = \emptyset$ for $\Sigma_X = \mathfrak{Primes} \smallsetminus \{\mathrm{char}(k)\}$.

Indeed, following a standard way in anabelian geometry of approaching this kind of problem, let us consider the following tautological family of hyperbolic curves of type $(g_X, 1)$:

$$f : U_{X\times X} \overset{\text{def}}{=} X \times X \smallsetminus \iota(X) \to X.$$

Then f induces a right exact sequence:

$$\Delta_F \to \Delta_{U_{X\times X}} \to \Delta_X \to 1,$$

where F is a geometric fiber of f (which is a hyperbolic curve of type $(g_X, 1)$), and Δ stands for the maximal pro-Σ_X quotient of the geometric fundamental group. Suppose that this right exact sequence is also left exact:

$$1 \to \Delta_F \to \Delta_{U_{X\times X}} \to \Delta_X \to 1.$$

Then the sequence

$$1 \to \Delta_F \to \Pi_{U_{X\times X}} \to \Pi_X \to 1$$

is also exact, where Π stands for the maximal geometrically pro-Σ_X quotient of the arithmetic fundamental group. Now, take $x, x' \in X(k)$ and suppose that $D_x, D_{x'} \subset \Pi_X$ coincide with each other (up to conjugation). Then, by pulling back the last exact sequence by $D_x, D_{x'} \subset \Pi_X$, we can easily obtain the following commutative diagram:

$$\begin{tikzcd} \Pi_{X\smallsetminus\{x\}} \arrow[r, "\sim"] \arrow[d] & \Pi_{X\smallsetminus\{x'\}} \arrow[d] \\ \Pi_X \arrow[r, equal] & \Pi_X \end{tikzcd}$$

Then, by Theorem 3.9 and Corollary 3.10, we obtain the following commutative diagram:

$$\begin{tikzcd} X\smallsetminus\{x\} \arrow[r, "\sim"] \arrow[d] & X\smallsetminus\{x'\} \arrow[d] \\ X \arrow[r, equal] & X. \end{tikzcd}$$

(Observe that the commutativity follows from the uniqueness assertion in Theorem 3.9.) This implies $x = x'$, as desired.

However, it is unclear to the authors, at the time of writing, whether or not the above left exactness (i.e., the injectivity of $\Delta_F \to \Delta_{U_{X\times X}}$) is valid. (Note that this is a purely topological (or even purely group-theoretical) problem.)

§4. Recovering the Additive Structure

In this §, we complete the proofs of the results of §3 by investigating the problem of recovering the additive structure of function fields of curves.

Let X, Y be proper, smooth, geometrically connected curves over fields k_X, k_Y, respectively. Let X^{cl}, Y^{cl} be the set of closed points of X, Y, respectively. Let $E_X \subset X^{\mathrm{cl}}$, $E_Y \subset Y^{\mathrm{cl}}$ be finite subsets, and let

$$\phi : X^{\mathrm{cl}} \smallsetminus E_X \overset{\sim}{\to} Y^{\mathrm{cl}} \smallsetminus E_Y$$

be a (set-theoretic) bijection. Write

$$\mathcal{O}_{E_X} \overset{\mathrm{def}}{=} \{f \in K_X \mid \forall x \in E_X,\ \mathrm{ord}_x(f) \geq 0\},$$

$$\mathcal{O}_{E_Y} \overset{\mathrm{def}}{=} \{g \in K_Y \mid \forall y \in E_Y,\ \mathrm{ord}_y(g) \geq 0\},$$

where K_X, K_Y denote the function fields of X, Y, respectively. These are the semi-local rings of functions on X, Y that are regular at all points of E_X, E_Y, respectively. Then we have

$$\mathcal{O}_{E_X}^{\times} = \{f \in K_X^{\times} \mid \operatorname{supp}(\operatorname{div}(f)) \cap E_X = \emptyset\},$$

$$\mathcal{O}_{E_Y}^{\times} = \{g \in K_Y^{\times} \mid \operatorname{supp}(\operatorname{div}(g)) \cap E_Y = \emptyset\}.$$

Let

$$\iota : \mathcal{O}_{E_X}^{\times} \hookrightarrow \mathcal{O}_{E_Y}^{\times}$$

be an embedding of multiplicative groups.

Definition 4.1. The map $\iota : \mathcal{O}_{E_X}^{\times} \hookrightarrow \mathcal{O}_{E_Y}^{\times}$ is called order-preserving, relative to the bijection ϕ, if, for each $x \in X^{\mathrm{cl}} \smallsetminus E_X$, we have a commutative diagram:

$$\begin{tikzcd}
\mathcal{O}_{E_Y}^{\times} \arrow[r, "\operatorname{ord}_{\phi(x)}"] & \mathbb{Z} \\
\mathcal{O}_{E_X}^{\times} \arrow[u, "\iota"] \arrow[r, "\operatorname{ord}_x"] & \mathbb{Z} \arrow[u, "e_x"']
\end{tikzcd}$$

where the right vertical map is the multiplication by a positive integer e_x on $\mathbb{Z}$.

Definition 4.2. The map $\iota : \mathcal{O}_{E_X}^{\times} \hookrightarrow \mathcal{O}_{E_Y}^{\times}$ is called value-preserving, relative to the bijection ϕ, if, for each $x \in X^{\mathrm{cl}} \smallsetminus E_X$, there exists an embedding of multiplicative groups

$$\iota_x : k(x)^{\times} \hookrightarrow k(\phi(x))^{\times},$$

where $k(x)$, $k(\phi(x))$ are the residue fields of X, Y at x, $\phi(x)$, respectively, such that, for any $f \in \mathcal{O}_{E_X}^{\times}$ with $\operatorname{ord}_x(f) = 0$, the equalities

$$\operatorname{ord}_{\phi(x)}(\iota(f)) = 0, \ \iota_x(f(x)) = \iota(f)(\phi(x))$$

hold.

Remark 4.3. (i) Assume that the map ι is order-preserving relative to ϕ. Then ι induces naturally an embedding $k_X^{\times} \hookrightarrow k_Y^{\times}$ of the multiplicative groups $k_X^{\times}$, $k_Y^{\times}$ of k_X, k_Y, respectively. We extend this embedding to an embedding $k_X \hookrightarrow k_Y$ (of multiplicative monoids) by letting $0 \mapsto 0$. We denote this last embedding also by ι.

(ii) Assume that the map ι is order-preserving and value-preserving relative to ϕ. For each $x \in X^{\mathrm{cl}} \smallsetminus E_X$, we extend ι_x to an embedding $k(x) \cup \{\infty\} \hookrightarrow k(\phi(x)) \cup \{\infty\}$ by letting $0 \mapsto 0$, $\infty \mapsto \infty$, and denote this last embedding also by ι_x. Then the equality

$$\iota_x(f(x)) = \iota(f)(\phi(x))$$

holds for any $x \in X^{\mathrm{cl}} \smallsetminus E_X$ and any $f \in \mathcal{O}_{E_X}^{\times}$.

Our aim in this § is to prove the following:

Proposition 4.4 (Recovering the Additive Structure). *Let $\iota : \mathcal{O}_{E_X}^{\times} \hookrightarrow \mathcal{O}_{E_Y}^{\times}$ be an embedding of multiplicative groups which is order-preserving and value-preserving relative to a bijection $\phi : X^{\mathrm{cl}} \smallsetminus E_X \xrightarrow{\sim} Y^{\mathrm{cl}} \smallsetminus E_Y$, where $E_X \subset X^{\mathrm{cl}}$, $E_Y \subset Y^{\mathrm{cl}}$ are finite subsets. Assume further that $X(k_X)$ is an infinite set. Then ι arises from a uniquely determined embedding $K_X \hookrightarrow K_Y$ of function fields.*

The rest of this § will be devoted to the proof of Proposition 4.4. Thus, we shall assume that the embedding

$$\iota : \mathcal{O}_{E_X}^{\times} \hookrightarrow \mathcal{O}_{E_Y}^{\times}$$

is order-preserving and value-preserving relative to a bijection

$$\phi : X^{\mathrm{cl}} \smallsetminus E_X \xrightarrow{\sim} Y^{\mathrm{cl}} \smallsetminus E_Y,$$

and that $X(k_X)$ is an infinite set, hence, in particular, that k_X is an infinite field.

Lemma 4.5 (Recovering the Additive Structure of Constants). *The map ι preserves the additive structure of the constant fields k_X, k_Y, respectively, i.e.,*

$$\iota(\lambda + \mu) = \iota(\lambda) + \iota(\mu)$$

holds for any $\lambda, \mu \in k_X$ (cf. Remark 4.3(i)).

Proof. Fix a point $x_0 \in X^{\mathrm{cl}} \smallsetminus E_X$. Then, by the Riemann-Roch theorem, we can find a non-constant function $f \in \mathcal{O}_{E_X}^{\times}$ such that the pole divisor $\mathrm{div}(f)_\infty$ is of the form $n \cdot x_0$ for some integer $n > 0$. Next, observe that $f + \alpha \in \mathcal{O}_{E_X}^{\times}$ holds for infinitely many $\alpha \in k_X^{\times}$ (namely, for any $\alpha \in k_X^{\times} \smallsetminus (\{-f(x) \mid x \in E_X\} \cap k_X^{\times})$). For $\alpha \in k_X^{\times}$ with $f + \alpha \in \mathcal{O}_{E_X}^{\times}$, we shall analyze the divisor of the function

$\iota(f+\alpha)-\iota(f)$. (Observe that $\iota(f+\alpha)-\iota(f)\neq 0$, since ι is injective.) We claim: (i) the support of the divisor $\operatorname{div}(\iota(f+\alpha)-\iota(f))$ is contained in $\{\phi(x_0)\}\cup E_Y$, and (ii) the support of the pole divisor $\operatorname{div}(\iota(f+\alpha)-\iota(f))_\infty$ is contained in $\{\phi(x_0)\}$. Indeed, let $x\in X^{\mathrm{cl}}\smallsetminus(E_X\cup\{x_0\})$, and let $y=\phi(x)$. Then, $\operatorname{ord}_y(\iota(f+\alpha))=e_x\operatorname{ord}_x(f+\alpha)\geq 0$ and $\operatorname{ord}_y(\iota(f))=e_x\operatorname{ord}_x(f)\geq 0$. Moreover, $\iota(f+\alpha)(y)\neq\iota(f)(y)$ as follows from the value-preserving assumption, since $(f+\alpha)(x)\neq f(x)$. Thus, y does not belong to the support of $\operatorname{div}(\iota(f+\alpha)-\iota(f))$, hence (i) follows. Next, as $\iota(f),\iota(f+\alpha)\in\mathcal{O}_{E_Y}^\times$, we have $\iota(f+\alpha)-\iota(f)\in\mathcal{O}_{E_Y}$. Thus, $\iota(f+\alpha)-\iota(f)$ has no poles in E_Y, and (ii) follows.

Further, the order of $\iota(f+\alpha)-\iota(f)$ at the possible pole $\phi(x_0)$ is bounded:

$$\operatorname{ord}_{\phi(x_0)}(\iota(f+\alpha)-\iota(f))\geq\min(\operatorname{ord}_{\phi(x_0)}(\iota(f+\alpha)),\operatorname{ord}_{\phi(x_0)}(\iota(f)))=-ne_{x_0}.$$

This implies the boundedness of the zero divisor of $\iota(f+\alpha)-\iota(f)$, hence also that there are only finitely many possibilities for the divisor of zeroes and poles of $\iota(f+\alpha)-\iota(f)$. We deduce from this that there exists an infinite subset $A\subset k_X^\times$, such that $f+\alpha\in\mathcal{O}_{E_X}^\times$ holds for all $\alpha\in A$, and that the divisor $\operatorname{div}(\iota(f+\alpha)-\iota(f))$ is constant for $\alpha\in A$ (i.e., $\operatorname{div}(\iota(f+\alpha)-\iota(f))$ $(\alpha\in A)$ is independent of α).

Let $\alpha,\beta\in A$ with $\alpha\neq\beta$. Thus,

$$\frac{\iota(f+\beta)-\iota(f)}{\iota(f+\alpha)-\iota(f)}=c\in k_Y^\times.$$

Further, $c=\frac{\iota(\beta)}{\iota(\alpha)}$, as is easily seen by evaluating the function $\frac{\iota(f+\beta)-\iota(f)}{\iota(f+\alpha)-\iota(f)}$ at $\phi(x_1)$, where x_1 is a zero of f. (Observe $x_1\notin E_X$.) Thus, we have the equality

$$\iota(\beta)(\iota(f+\alpha)-\iota(f))=\iota(\alpha)(\iota(f+\beta)-\iota(f))$$

which is equivalent to

$$(*)\qquad \iota(f)(\iota(\alpha)-\iota(\beta))=\iota(\alpha)\iota(f+\beta)-\iota(\beta)\iota(f+\alpha).$$

Let

$$g\overset{\mathrm{def}}{=}g_{\alpha,\beta}\overset{\mathrm{def}}{=}\frac{\beta(f+\alpha)}{(\alpha-\beta)f}\in\mathcal{O}_{E_X}^\times.$$

Note that $g=\frac{\beta(1+\alpha f^{-1})}{(\alpha-\beta)}$ is non-constant, since f is non-constant. Moreover, we have

$$g+1=\frac{\alpha(f+\beta)}{(\alpha-\beta)f}\in\mathcal{O}_{E_X}^\times.$$

We will show the identity $\iota(g+1)=\iota(g)+1$. Indeed,

$$\iota(g+1)-\iota(g)=\frac{\iota(\alpha)\iota(f+\beta)}{\iota(\alpha-\beta)\iota(f)}-\frac{\iota(\beta)\iota(f+\alpha)}{\iota(\alpha-\beta)\iota(f)}\overset{(*)}{=}\frac{\iota(\alpha)-\iota(\beta)}{\iota(\alpha-\beta)}.$$

Moreover,

$$\frac{\iota(\alpha)-\iota(\beta)}{\iota(\alpha-\beta)}=1,$$

as follows by evaluating the function $\iota(g+1)-\iota(g)$ at $\phi(x_2)$, where x_2 is a zero of g. (Observe $x_2 \notin E_X$.) Thus,

$$\iota(g+1)=\iota(g)+1.$$

Next, let $\lambda, \mu \in k_X$, and we shall show the identity $\iota(\lambda+\mu)=\iota(\lambda)+\iota(\mu)$. If one (or both) of λ, μ is 0, this identity clearly holds. So, we may and shall assume $\lambda, \mu \in k_X^\times$ and set $\eta \overset{\text{def}}{=} \lambda/\mu \in k_X^\times$. First, assume that

$$\eta \in k_X \smallsetminus (\{g(x) \mid x \in E_X\} \cap k_X)$$

and let $x_3 \in X^{\text{cl}}$ be a zero of $g-\eta$. Thus, $x_3 \notin E_X$, and, by evaluating the identity $\iota(g+1)=\iota(g)+1$ at $\phi(x_3)$, we obtain $\iota(\eta)+1=\iota(\eta+1)$. To show this equality for general η, we shall fix (f and) $\beta \in A$ and make $\alpha \in A \smallsetminus \{\beta\}$ vary in the expression of $g=g_{\alpha,\beta}$. More precisely, take any $\alpha \in (A \smallsetminus \{\beta\}) \smallsetminus \{\frac{(\eta+1)\beta f(x)}{\eta f(x)-\beta} \mid x \in E_X\}$. Then $g=g_{\alpha,\beta}$ satisfies $\eta \notin k_X \smallsetminus (\{g(x) \mid x \in E_X\} \cap k_X)$. Thus, by the preceding argument, we conclude that

$$\iota(\eta)+1=\iota(\eta+1)$$

holds in general.

Finally, we obtain

$$\iota(\lambda+\mu)=\iota(\mu)\iota(\eta+1)=\iota(\mu)(\iota(\eta)+1)=\iota(\lambda)+\iota(\mu),$$

as desired. □

Corollary 4.6. *The map $\iota : k_X \to k_Y$ is an embedding of fields.*

Proof. ι is multiplicative by definition and additive by Lemma 4.5. □

Corollary 4.7. *For each $x \in X(k_X) \smallsetminus E_X$, the map $\iota_x : k(x) \to k(\phi(x))$ is an embedding of fields.*

Proof. For each $x \in X^{\text{cl}} \smallsetminus E_X$, consider the following diagram

$$\begin{tikzcd} k(x) \arrow[r, "\iota_x"] & k(\phi(x)) \\ k_X \arrow[u] \arrow[r, "\iota"] & k_Y \arrow[u] \end{tikzcd}$$

where the vertical arrows are evaluation maps. By the value-preserving property, this diagram is commutative. If, moreover, $x \in X(k_X)$, we have $k_X \overset{\sim}{\to} k(x)$. Thus, Corollary 4.7 follows from Corollary 4.6. □

Next, let $\mathbb{Z}[\mathcal{O}_{E_X}^\times]$, $\mathbb{Z}[\mathcal{O}_{E_Y}^\times]$ be the group algebras of the multiplicative groups $\mathcal{O}_{E_X}^\times$, $\mathcal{O}_{E_Y}^\times$, respectively, over $\mathbb{Z}$. The group homomorphism $\iota : \mathcal{O}_{E_X}^\times \hookrightarrow \mathcal{O}_{E_Y}^\times$ extends uniquely to a ring homomorphism

$$\iota' : \mathbb{Z}[\mathcal{O}_{E_X}^\times] \to \mathbb{Z}[\mathcal{O}_{E_Y}^\times].$$

Namely,

$$\iota'\left(\sum_i n_i f_i\right) \overset{\text{def}}{=} \sum_i n_i \iota(f_i)$$

where $n_i \in \mathbb{Z}$, $f_i \in \mathcal{O}_{E_X}^\times$. Further, let R_X, R_Y be the $\mathbb{Z}$-subalgebras of K_X, K_Y, respectively, generated by $\mathcal{O}_{E_X}^\times$, $\mathcal{O}_{E_Y}^\times$, respectively. Observe that R_X, R_Y may be naturally regarded as quotient rings of $\mathbb{Z}[\mathcal{O}_{E_X}^\times]$, $\mathbb{Z}[\mathcal{O}_{E_Y}^\times]$, respectively.

Lemma 4.8. *The ring homomorphism $\iota' : \mathbb{Z}[\mathcal{O}_{E_X}^\times] \to \mathbb{Z}[\mathcal{O}_{E_Y}^\times]$ induces a* (*unique*) *ring homomorphism $\iota_R : R_X \to R_Y$. More precisely, The composite of $\iota' : \mathbb{Z}[\mathcal{O}_{E_X}^\times] \to \mathbb{Z}[\mathcal{O}_{E_Y}^\times]$ and the natural surjection $\mathbb{Z}[\mathcal{O}_{E_Y}^\times] \to R_Y$ factors through the natural surjection $\mathbb{Z}[\mathcal{O}_{E_X}^\times] \to R_X$.*

Proof. Take any element

$$F = \sum_i n_i f_i \in \mathbb{Z}[\mathcal{O}_{E_X}^\times],$$

where $n_i \in \mathbb{Z}$, $f_i \in \mathcal{O}_{E_X}^\times$, such that the image F_X of F in R_X is 0. Then we have to show that the image F_Y of F in R_Y is also 0. To avoid confusion, we shall denote a sum in a ring R by means of $\sum_R$. Then the assumption $F_X = 0$ can be expressed as the equality

$$\sum_i {}_{R_X}\ n_i f_i = 0.$$

Let $S_i \subset X^{\mathrm{cl}}$ denote the (finite) set of poles of f_i and consider a point $x \in X(k_X) \smallsetminus (E_X \cup \cup_i S_i)$. By evaluating the above equality at x, we obtain the equality

$$\sum_i {}_{k(x)}\ n_i f_i(x) = 0.$$

By Corollary 4.7 and the value-preserving property at x, this last equality implies the equality

$$\sum_i {}_{k(\phi(x))}\ n_i \iota(f_i)(\phi(x)) = 0,$$

or, equivalently, the equality

$$F_Y(\phi(x)) = 0$$

in $k(\phi(x))$. Since x is an arbitrary point in the infinite set $X(k_X) \setminus (E_X \cup \cup_i S_i)$, this implies $F_Y = 0$ in R_Y, as desired. □

Lemma 4.9. *For each $f \in \mathcal{O}_{E_X}$ (respectively, $f \in \mathcal{O}_{E_Y}$), there exist $g, h \in \mathcal{O}_{E_X}^\times$ (respectively, $g, h \in \mathcal{O}_{E_Y}^\times$), such that $f = g + h$. In particular, we have $R_X = \mathcal{O}_{E_X}$ (respectively, $R_Y = \mathcal{O}_{E_Y}$).*

Proof. It suffices to prove the assertions for X. For each $f \in \mathcal{O}_{E_X}$, consider the subset $A_X \overset{\text{def}}{=} k_X^\times \setminus (\{f(x) \mid x \in E_X\} \cap k_X^\times)$ of $\mathcal{O}_{E_X}^\times$. Since k_X is infinite and E_X is finite, A_X is nonempty, so we can take $\alpha \in A_X \subset \mathcal{O}_{E_X}^\times$. By the definition of A_X, we have $f - \alpha \in \mathcal{O}_{E_X}^\times$. Thus, $g \overset{\text{def}}{=} \alpha$ and $h \overset{\text{def}}{=} f - \alpha$ satisfy the desired conditions. In particular, we have $\mathcal{O}_{E_X} \subset R_X$. Since the other inclusion $R_X \subset \mathcal{O}_{E_X}$ is clear, this completes the proof. □

Lemma 4.10. *The ring homomorphism $\iota_R : R_X \to R_Y$ in Lemma 4.8 is injective.*

Proof. Take any $f \in R_X$ with $\iota_R(f) = 0$. By Lemma 4.9, $f \in R_X = \mathcal{O}_{E_X}$ can be written as $f = g + h$ for some $g, h \in \mathcal{O}_{E_X}^\times$. Now we have

$$\iota(g) = \iota_R(g) = \iota_R(f) + \iota_R(-h) = \iota(-h).$$

Since ι is injective, this shows $g = -h$, hence $f = 0$, as desired. □

Corollary 4.11. *The ring homomorphism $\iota_R : R_X \to R_Y$ extends uniquely to an embedding $K_X \hookrightarrow K_Y$ of fields.*

Proof. This follows from Lemmas 4.9 and 4.10. □

This completes the proof of Proposition 4.4. □

Remark 4.12. The above proof of Proposition 4.4 relies on the value-preserving property at all but finitely many points of X^{cl} (or, more precisely, all points of $X^{\text{cl}} \setminus E_X$). This is in contrast to the proof of [Tamagawa1], Lemma (4.7), which relies on the value-preserving property at only finitely many points. Thus, unlike the case of [Tamagawa1], Theorem (4.3), we need, at least for the time being, to resort to Mochizuki's theory of cuspidalizations to prove Corollary 3.10, even in the affine case.

We should also remark here that the birational version given in Corollary 3.11 is independent of Mochizuki's theory of cuspidalizations, although we resorted to Corollary 3.10 in the present proof of Corollary 3.11 for the sake of simplicity. Indeed, once the bijection $\phi : X^{\mathrm{cl}} \xrightarrow{\sim} Y^{\mathrm{cl}}$ is established so that $\alpha(D_x) = D_{\phi(x)}$ for each $x \in X^{\mathrm{cl}}$, we can construct an embedding $\iota : K_X^\times \hookrightarrow K_Y^\times$ directly from $\alpha : \Gamma_{K_X} \xrightarrow{\sim} \Gamma_{K_Y}$ (via Kummer theory or via class field theory), such that ι is order-preserving and value-preserving relative to ϕ.

Acknowledgment

The authors would like to thank Shinichi Mochizuki very much for various useful discussions on his theory of cuspidalizations. The first author holds an EPSRC advanced research fellowship GR/R75861/02, and would like very much to thank EPSRC for its support. This work was done during a visit of his to the Research Institute for Mathematical Sciences (RIMS) in Kyoto. He would like very much to thank the staff members of RIMS for their hospitality. Finally, the authors would like to thank the referee very much for various useful comments, especially concerning Remark 3.12.

References

[Boxall] J. Boxall, Autour d'un problème de Coleman, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 10, 1063–1066.

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

[Grothendieck] A. Grothendieck, Brief an G. Faltings, in *Geometric Galois actions, 1*, London Math. Soc. Lecture Note Ser., 242, 49–58, Cambridge Univ. Press, Cambridge, 1997; English translation, 285–293.

[GS] F. J. Grunewald and D. Segal, On congruence topologies in number fields, J. Reine Angew. Math. **311/312** (1979), 389–396.

[Hall] M. Hall, Jr., *Combinatorial theory*, Blaisdell Publishing Co. Ginn and Co., Waltham, Mass., 1967.

[Mochizuki1] S. Mochizuki, The local pro-p anabelian geometry of curves, Invent. Math. **138** (1999), no. 2, 319–423.

[Mochizuki2] ———, Absolute anabelian cuspidalizations of proper hyperbolic curves, J. Math. Kyoto Univ. **47** (2007), no. 3, 451–539.

[Nakamura1] H. Nakamura, Galois rigidity of the étale fundamental groups of punctured projective lines, J. Reine Angew. Math. **411** (1990), 205–216.

[Nakamura2] ———, Galois rigidity of algebraic mappings into some hyperbolic varieties, Internat. J. Math. **4** (1993), no. 3, 421–438.

[Nakamura3] ———, Galois rigidity of pure sphere braid groups and profinite calculus, J. Math. Sci. Univ. Tokyo **1** (1994), no. 1, 71–136.

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

[Rosen] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, 210, Springer, New York, 2002.

[Stix1] J. Stix, Affine anabelian curves in positive characteristic, Compositio Math. **134** (2002), no. 1, 75–85.

[Stix2] ———, *Projective anabelian curves in positive characteristic and descent theory for log-étale covers*, Bonner Mathematische Schriften, 354, Univ. Bonn, Bonn, 2002.

[Tamagawa1] A. Tamagawa, The Grothendieck conjecture for affine curves, Compositio Math. **109** (1997), no. 2, 135–194.

[Tamagawa2] ———, On the tame fundamental groups of curves over algebraically closed fields of characteristic > 0, in *Galois groups and fundamental groups*, Math. Sci. Res. Inst. Publ., 41, 47–105, Cambridge Univ. Press, Cambridge, 2003.

[Tamagawa3] ———, Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups, J. Algebraic Geom. **13** (2004), no. 4, 675–724.

[Uchida] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, Ann. Math. (2) **106** (1977), no. 3, 589–598.