A PRIME-TO-$p$ VERSION OF GROTHENDIECK’S
ANABELIAN CONJECTURE FOR HYPERBOLIC CURVES
OVER FINITE FIELDS OF CHARACTERISTIC $p > 0$

MOHAMED SÄIDI AND AKIO TAMAGAWA

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.

Contents

§0. Introduction
§1. Characterization of Decomposition Groups
§2. Cuspidalizations of Proper Hyperbolic Curves
§3. Kummer Theory and Anabelian Geometry
§4. Recovering the Additive Structure

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

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

Here, $G_k$ is the absolute Galois group $\text{Gal} (\bar{k}/k)$, $\ast$ means a suitable geometric point, and $\pi_1$ 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

$$\alpha : \pi_1(U, \ast) \sim \pi_1(V, \ast)$$

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

$$
\begin{array}{ccc}
\tilde{U} & \sim & \tilde{V} \\
\downarrow & & \downarrow \\
U & \sim & V
\end{array}
$$
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 3.12) 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 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 $\Delta_U$ 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 $\Gamma$, $\Gamma^l$ stands for the maximal pro-$l$ (i.e., pro-$\mathcal{C}^l$) quotient of $\Gamma$. Thus, in particular, $\Delta_U^l \cong \pi_1(U \times_k \bar{k},*)^l$. Here, the structures of $\Delta_U$ and $\Delta_U^l$ are well understood — $\Delta_U$ (respectively, $\Delta_U^l$) 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 $\Pi_U \overset{def}{=} \pi_1(U,*)/\ker(\pi_1(U \times_k \bar{k},*) \twoheadrightarrow \Delta_U)$ (respectively, $\Pi_U^{(l)} \overset{def}{=} \pi_1(U,*)/\ker(\pi_1(U \times_k \bar{k},*) \twoheadrightarrow \Delta_U^l)$ be the corresponding quotients of $\pi_1(U \times_k \bar{k},*)$. We shall refer to $\Pi_U$ as the geometrically pro-$\Sigma_U$ étale fundamental group of $U$, where $\Sigma_U \overset{def}{=} \pi\text{-}\text{Primes} - \{\text{char}(k)\}$, and $\pi\text{-}\text{Primes}$ 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 $\Pi_U$, $\Pi_U^{(l)}$, 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 $\Sigma_U \overset{def}{=} \pi\text{-}\text{Primes} - \{\text{char}(k_U)\}$, $\Sigma_V \overset{def}{=} \pi\text{-}\text{Primes} - \{\text{char}(k_V)\}$, and write $\Pi_U$, $\Pi_V$ for the geometrically pro-$\Sigma_U$ étale fundamental group of $U$, and the geometrically pro-$\Sigma_V$ étale fundamental group of $V$, respectively. Let

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

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

\[ \tilde{U} \sim \longrightarrow \tilde{V} \]
\[ \downarrow \hspace{1cm} \downarrow \]
\[ U \sim \longrightarrow V \]

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups \( \Pi_U, \Pi_V \), 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 \( G'_{K_X}, G'_{K_Y} \) be their geometrically pro-prime-to-characteristic quotients (cf. discussion before Corollary 3.11). Let

\[ \alpha : G'_{K_X} \sim \longrightarrow G'_{K_Y} \]

be an isomorphism of profinite groups. Then \( \alpha \) arises from a uniquely determined commutative diagram of field extensions:

\[ (K_X)\sim \sim \longrightarrow (K_Y)\sim \]
\[ \uparrow \hspace{1cm} \uparrow \]
\[ K_X \sim \longrightarrow K_Y \]

in which the horizontal arrows are isomorphisms and the vertical arrows are the extensions corresponding to the Galois groups \( G'_{K_X}, G'_{K_Y} \), 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 \( \Pi_X \), Tamagawa’s method characterizes group-theoretically the decomposition groups at points of \( X \) in \( \Pi_X \). The problem of recovering the points of \( X \) from the corresponding decomposition groups is related to the question of whether the natural map

\[ X^{\text{cl}} \rightarrow \text{Sub}(\Pi_X)_{\Pi_X} \]

from the set of closed points of \( X \) to the set of conjugacy classes of closed subgroups of \( \Pi_X \), 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 \( \pi_1(X, \ast) \) instead of \( \Pi_X \). In our case we are only able to prove that the above map is almost injective, i.e., injective outside a finite set \( E_X \subset X^{\text{cl}} \).

Thus, we can only recover from \( \Pi_X \) the set of points in a nonempty open subset \( X - E_X \).
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 $\Pi_X$, one can recover in a functorial way the Kummer theory of open affine subsets $U_S^{\text{def}} = X - S$, where $S$ is a finite set of closed points contained in $X - E_X$. 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 a support disjoint from $E_X$. Thus, starting from an isomorphism

$$\Pi_X \sim \Pi_Y$$

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 — the minimal elements, i.e., functions with a minimal pole. The arguments 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. In our situation the fact that we can only evaluate functions at all but finitely many points of $X$ (or, more precisely, all points of $X - E_X$) 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 $\Pi_X$. 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.

**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.

**§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 $U = U_S \overset{\text{def}}{=} X - S$. 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 $K^{\text{sep}}$. Write

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

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

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 $K^{\text{sep}}$ (where “tame” is with respect to the complement of $U$ in $X$) can be naturally identified with a quotient of $G_K$. Write $\text{Gal}(K^t_U/K)$ for this quotient. (In case $S = \emptyset$, we also write $K^t_U$ for $K^t$.) It is easy to see that $K^t_U$ contains $K^t_k$.

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

$$\Sigma^\ddagger \overset{\text{def}}{=} \Sigma - \{p\}.$$  

Thus, $\Sigma^\ddagger \neq \emptyset$ by our assumption. Denote by $\hat{Z}^{\Sigma^\ddagger}$ the maximal pro-$\Sigma^\ddagger$ quotient of $\hat{Z}$. Set $\Sigma' = \Sigma_X = \text{Primes} - \Sigma_X$. We say that $\Sigma$ is cofinite if $\#(\Sigma') < \infty$.

We define $\hat{K}_U$ to be the maximal pro-$\Sigma$ subextension of $K^t_k$ in $K^t_U$. Now, set

$$\Pi_U = \text{Gal}(\hat{K}_U/K),$$

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

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

Here, $\Delta_U$ is the maximal pro-$\Sigma$ quotient of $\pi_1^t(U)$, where, for a $k$-scheme $Z$, we set

$$\hat{Z} \overset{\text{def}}{=} Z \times_k \overline{k}.$$  

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

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

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

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

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

For each $\tilde{x} \in (\hat{X}_U)^{\text{cl}}$, 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 $\Pi_U$ on $(\hat{X}_U)^{\text{cl}}$ (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:

$$
\begin{array}{cccccc}
1 & \to & I_{\tilde{x}} & \to & D_{\tilde{x}} & \to & G_{k(x)} & \to & 1 \\
\cap & & \cap & & \cap & & & & \\
1 & \to & \Delta_U & \to & \Pi_U & \to & G_k & \to & 1
\end{array}
$$
Moreover, \( I_{\tilde{x}} = \{1\} \) (respectively, \( I_{\tilde{x}} \) is (non-canonically) isomorphic to \( \hat{\mathbb{Z}}^\Sigma \)), if \( \tilde{x} \in \hat{U}^{\text{cl}} \) (respectively, \( \tilde{x} \in \hat{S}_U \)). 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 \( \tilde{x} \in \hat{S}_U \). Then:

(i) The subgroup \( I^G_{k(x)} \) of \( I_{\tilde{x}} \) that consists of elements fixed by the \( G_{k(x)} \)-action is trivial.

(ii) Assume moreover that \( \Sigma \) is cofinite. Then the kernel of the action \( G_{k(x)} \to \text{Aut}(I_{\tilde{x}}) \) is trivial.

**Proof.** By assumption, \( I_{\tilde{x}} \simeq \hat{\mathbb{Z}}^\Sigma \), and it is well-known that the map \( G_{k(x)} \to \text{Aut}(I_{\tilde{x}}) = (\hat{\mathbb{Z}}^\Sigma)^x \) 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 \( \sharp(k(x)) \in (\hat{\mathbb{Z}}^\Sigma)^x \). The assertion of (i) follows from this, since \( \sharp(k(x)) - 1 \) is not a zero divisor of the ring \( \hat{\mathbb{Z}}^\Sigma \). The assertion of (ii) also follows from this, together with a theorem of Chevalley ([Chevalley], Théorème 1). □

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

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

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

\[
\text{Sub}(G) \overset{\text{def}}{=} \lim_{H \in \text{OSub}(G)} \text{Sub}(H).
\]

Observe that \( \overline{\text{Sub}}(G) \) 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 \( J_1 \cap J_2 \) is open both in \( J_1 \) and in \( J_2 \).)

With these notations, we obtain natural maps

\[
D = D[U] : (X_U)^{\text{cl}} \to \text{Sub}(\Pi_U), \tilde{x} \mapsto D_{\tilde{x}} ,
\]

\[
I = I[U] : (X_U)^{\text{cl}} \to \text{Sub}(\Delta_U) \subset \text{Sub}(\Pi_U), \tilde{x} \mapsto I_{\tilde{x}},
\]

which fit into the commutative diagram

\[
\begin{array}{ccc}
(X_U)^{\text{cl}} & \xrightarrow{D} & \text{Sub}(\Pi_U) \\
\parallel & & \downarrow \\
(X_U)^{\text{cl}} & \xrightarrow{I} & \text{Sub}(\Delta_U),
\end{array}
\]

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

\[
\overline{D} = \overline{D[U]} : (X_U)^{\text{cl}} \to \overline{\text{Sub}}(\Pi_U), \\
\overline{I} = \overline{I[U]} : (X_U)^{\text{cl}} \to \overline{\text{Sub}}(\Delta_U) \subset \overline{\text{Sub}}(\Pi_U).
\]
Remark 1.2. Unlike the case of $D, I$, the maps $\overline{D, 7}$ are essentially unchanged if we replace $U$ by any covering corresponding to an open subgroup of $\Pi_U$.

Since the maps $D, I$ are $\Pi_U$-equivariant, they induce natural maps

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

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

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. \qed

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

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,

$$Z_G(H) = \{g \in G \mid ghg^{-1} = h \text{ for any } h \in H\},$$

$$N_G(H) = \{g \in G \mid ghg^{-1} = H\} \supset H,$$

$$C_G(H) = \{g \in G \mid ghg^{-1} \text{ and } H \text{ are commensurate}\}.$$

Lemma 1.7. Let $Z$ be a closed subgroup of $\Pi_U$ such that $\text{pr}_U(Z)$ is open in $G_k$ and that $\text{pr}_U|Z$ is injective. Then $\text{pr}_U$ 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, $Z_0 \overset{\text{def}}{=} Z \cap \sigma Z \sigma^{-1}$ is open both in $Z$ and in $\sigma Z \sigma^{-1}$. We claim that $\sigma$ commutes with any element $\tau$ of $Z_0$. Indeed, first, observe that $\tau \in Z_0 \subset \sigma Z \sigma^{-1}$ and $\sigma \tau \sigma^{-1} = Z_0 \sigma^{-1} \subset \sigma Z \sigma^{-1}$ hold. Or,
equivalently, $\sigma^{-1}\tau\sigma, \tau \in Z$. Second, observe that $\text{pr}_U(\sigma^{-1}\tau\sigma) = \text{pr}_U(\tau)$ holds, since $\text{pr}_U(\sigma) = 1$. Now since $\text{pr}_U|_Z$ is injective, the equality $\text{pr}_U(\sigma^{-1}\tau\sigma) = \text{pr}_U(\tau)$ 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 $\Delta_U$ such that $\sigma \not\in \overline{N}$. Set $\mathcal{H} \overset{\text{def}}{=} \langle \overline{N}, \sigma \rangle \subset \Delta_U$. Then the image of $\sigma$ in $\mathcal{H}^{ab}$ is nontrivial. (Indeed, the image of $\sigma$ in $\mathcal{H}/\overline{N}$ is nontrivial by definition. Since $\mathcal{H}/\overline{N}$ is cyclic, the surjection $\mathcal{H} \to \mathcal{H}^{ab}$ factors through the surjection $\mathcal{H} \to \mathcal{H}^{ab}$.) Observe that $Z_0$ normalizes $\mathcal{H}$, since $\overline{N}$ is characteristic in $\Delta_U$ and $\sigma$ commutes with $Z_0$. So, the open subgroup $H \overset{\text{def}}{=} \langle \mathcal{H}, Z_0 \rangle$ of $\Pi_U$ can be regarded as a semidirect-product extension of $Z_0$ by $\mathcal{H}$ and satisfies $H \cap \Delta_U = \mathcal{H}$. Now, the image of $\sigma$ in $\mathcal{H}^{ab}$ 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 $\text{pr}_U(Z_0)$, 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 $\text{pr}_U$ induces an isomorphism $C_{\Pi_U}(Z) \sim \text{pr}_U(C_{\Pi_U}(Z))$ and $\text{pr}_U(Z)$ is open in $G_k$, the third assertion holds. \(\square\)

The first main result in this § is:

**Proposition 1.8.** (i) $\mathcal{T}|_{\tilde{\mathcal{S}}_U} : \tilde{\mathcal{S}}_U \to \overline{\text{Sub}}(\Pi_U)$ is injective.
(ii) $E_{\tilde{U}}$ is disjoint from $\tilde{\mathcal{S}}_U$. (Or, equivalently, $E_{\tilde{U}} \subset \tilde{U}^{\text{cl}}$.)
(iii) Let $\overline{\mathcal{P}}$ denote the natural morphism $\tilde{X}_U \to \overline{X}$. Then, for each $x \in \overline{X}^{\text{cl}}$, $\overline{\mathcal{D}}|_{\overline{\mathcal{P}}^{-1}(x)}$ is injective.
(iv) Let $\rho$ denote the natural morphism $\tilde{X}_U \to X$. Then, for each $x \in X^{\text{cl}}$, $\overline{\mathcal{D}}|_{\rho^{-1}(x)}$ is quasi-finite. If, moreover, $k(x) = k$ holds (i.e., $x$ is a $k$-rational point of $X$), $\overline{\mathcal{D}}|_{\rho^{-1}(x)}$ is injective.
(v) $E_{\tilde{U}}$ is $\Pi_U$-stable.

Assume, moreover, that $\Sigma$ is cofinite. Then:
(vi) The quotient $E_{\tilde{U}}/\Pi_U$ is finite.
(vii) $\overline{\mathcal{D}} : (\tilde{X}_U)^{\text{cl}} \to \overline{\text{Sub}}(\Pi_U)$ is quasi-finite.

**Proof.** (i) Take any $\tilde{x}, \tilde{x}' \in \tilde{\mathcal{S}}_U$, and assume $\tilde{x} \neq \tilde{x}'$. Then there exists an open subgroup $H_0$ of $\Pi_U$, 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 $X_0 - \overline{U}_0$ is $\geq 3$ (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 $\overline{\mathcal{S}}_1 \overset{\text{def}}{=} \overline{X}_1 - \overline{U}_1$ are distinct from each other and that the cardinality of $\overline{\mathcal{S}}_1$ is $\geq 3$. Then it is easy to see that the images of $I_{\tilde{x}} \cap H_1, I_{\tilde{x}'} \cap H_1$ in $H_1^{ab}$ 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 $\tilde{x}' \in (\tilde{X}_U)^{cl}$, 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 $\Pi_U$, 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 $\tilde{x}' \in \tilde{U}^{cl}$, the last assertion follows from the fact $I_{\tilde{x}} \simeq \hat{\hat{\mathcal{X}}}_{\Sigma}^1, I_{\tilde{x}'} = \{1\}$.

(iii) If $\overline{\sigma} \in \overline{\Sigma} \overset{\text{def}}{=} (\overline{X} - \overline{U})$, the assertion follows from (ii). So, we may and shall assume $\overline{\sigma} \in \overline{U}^{cl}$. Take any $\tilde{x}, \tilde{x}' \in \overline{U}^{-1}(\overline{\sigma})$. Then there exists $\sigma \in \Delta_U$ such that $\tilde{x}' = \sigma \tilde{x}$ holds. (Such $\sigma$ is unique by the assumption $\overline{\sigma} \in \overline{U}^{cl}$, 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, $\sigma \in \mathcal{C}_{\Pi_U}(D_{\tilde{x}}) \cap \Delta_U$, and it follows from Lemma 1.7 that $\sigma = 1$ holds, hence $\tilde{x}' = \sigma \tilde{x} = \tilde{x}$. Namely, $\overline{D}(\overline{\sigma}^{-1}(\overline{\sigma}))$ is injective, as desired.

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

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

(vi) To prove this (assuming that $\Sigma$ is cofinite), we may replace $U$ by any covering corresponding to an open subgroup of $\Pi_U$. 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 [Mochizuki], Lemma 10.4(4) for the latter.) We shall prove that $\rho(E_U)$, which can be identified with $E_U/\Pi_U$, is finite, or, more strongly, that $\mathcal{P}(E_U)$, which can be identified with $E_U/\Delta_U$, is finite.

Take any pair of elements $\tilde{x}, \tilde{x}' \in \tilde{U}^{cl}$, and denote by $\overline{r}, \overline{r}'$ the images of $\tilde{x}, \tilde{x}'$ in $\overline{U}^{cl}$, 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 $\Delta_U$ via the section $s'$). Thus, $\phi$ defines a cohomology class in $H^1(G_0, \Delta_U)$. We denote by $\phi_{0, X}^{ab} = \phi_{0, X}(\tilde{x}, \tilde{x}')$ the image of this class in $H^1(G_0, \Delta_X^{ab})$. (Note that the $G_0$-action on $\Delta_X^{ab}$ induced by that on $\Delta_U$ extends to a canonical $G_k$-action, hence, in particular, is independent of the choice of $\tilde{x}'$.) Moreover, we set

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

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

On the other hand, it is well-known that $\Delta_X^{ab}$ is canonically isomorphic as a $G_k$-module to the pro-$\Sigma$ 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 $J(k_G)/(J(k_G)\{\Sigma'\}) \to H^1(G, \Delta_X^{ab})$, 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 \( \Sigma' \). (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 \( J(\overline{k})/(J(\overline{k})\{\Sigma'\}) \to H_X \).

Now, it is widely known that the image in \( H_X \) of the class of \( \overline{x} - \overline{x}' \) in \( J[1] = J(\overline{k}) \) coincides with \( \phi_{ab}^{\overline{x}} \). For this, see [NT], Lemma (4.14). (See also [Nakamura2], 2.2 and [Tamagawa1], Lemma (2.6).)

Suppose moreover that \((\overline{x}, \overline{x}')\) is an exceptional pair of \( \overline{\Delta} \). Then it follows from the various definitions that \( \phi_{ab}^{\overline{x}} \in H_X \) 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 \( J(\overline{k}) \) falls in \( J(\overline{k})\{\Sigma'\} \). On the other hand, by (iii), \( \overline{x} \neq \overline{x}' \) hold, 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 \( \delta \) does not contain any translate of positive-dimensional abelian subvariety of \( J \).

   Indeed, for (i), suppose that \((P, Q), (P', Q') \in (X \times X - \iota(X))(\overline{k}) \) have the same image under \( \delta \). 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 irreducible of dimension \( \leq 2 \) as the image of \( X \times X \). 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 \( \delta \) induces a bijective morphism \( X \times X - \Delta(X) \to W - \{0\} \). From this, we deduce that there exists a finite radical 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 \( S \) of \((X \times X)(\overline{k})\) that contains any pair \((\overline{x}, \overline{x}')\) as above. This implies the desired assertion that \( \overline{\rho}(E_{\overline{G}}) \) is a finite set.

   (vii) Note that \( \rho(E_{\overline{G}}) \) can be identified with \( E_{\overline{G}}/\Pi_U \) by (v). Thus, the assertion of (vii) directly follows from (vi) and the first part of (iv). \( \square \)

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

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

(ii) \( E_U \) is disjoint from \( S \). (Or, equivalently, \( E_U \subset U^{\text{cl}} \).)
Assume, moreover, that $\Sigma$ is cofinite. Then:

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

**Proof.** (i) As $D|_{(\tilde{X}_U)^\text{cl} - E_U}: (\tilde{X}_U)^\text{cl} - E_U \to \text{Sub}(\Pi_U)$ is injective by definition and $\Pi_U$-equivariant, its quotient by $\Pi_U$, which is naturally identified with $D_{\Pi_U}|_{X^\text{cl} - E_U}: X^\text{cl} - E_U \to \text{Sub}(\Pi_U)_{\Pi_U}$, 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)). \qed

**Corollary 1.12.** (i) For each $\tilde{x} \in \tilde{U}^\text{cl}$, $\text{pr}_U$ 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

$$\left(\text{pr}_U(D_{\tilde{x}}) : D_{\tilde{x}}\right) < \infty.$$

If, moreover, $\tilde{x} \in \tilde{U}^\text{cl} - E_U$, 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

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

(Note that, if $\Sigma$ is cofinite, then $Z_{D_{\tilde{x}}}(D_{\tilde{x}}) = 1$ and $Z_{D_{\tilde{x}}}(I_{\tilde{x}}) = I_{\tilde{x}}$ by Lemma 1.1.)

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

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

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

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

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

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

**Proof.** First, since $\overline{D}|_{(\tilde{X}_U)^\text{cl} - E_U}: (\tilde{X}_U)^\text{cl} - E_U \to \overline{\text{Sub}(\Pi_U)}$ is injective and $\Pi_U$-equivariant, we see that $C_{\Pi_U}(D_{\tilde{x}}) = D_{\tilde{x}}$ holds for any $\tilde{x} \in (\tilde{X}_U)^\text{cl} - E_U$.

(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 \( \bar{x} \in \tilde{S}_U \). Then, \( \bar{x} \notin E_U \) by Proposition 1.8(ii). Thus, we have \( C_{\Pi_U}(\bar{x}) = N_{\Pi_U}(D_{\bar{x}}) = D_{\bar{x}} \). From this, we also have \( Z_{\Pi_U}(\bar{x}) = Z_{D_{\bar{x}}}(D_{\bar{x}}) \).

Next, by Proposition 1.8(i), the map \( \overline{T}|_{\tilde{S}_U} : \tilde{S}_U \rightarrow \text{Sub}(\Pi_U) \) is injective. Since this map is also \( \Pi_U \)-equivariant, we see that \( C_{\Pi_U}(I_{\bar{x}}) = D_{\bar{x}} \). As \( C_{\Pi_U}(I_{\bar{x}}) \supset N_{\Pi_U}(I_{\bar{x}}) \supset D_{\bar{x}} \), we have \( N_{\Pi_U}(I_{\bar{x}}) = D_{\bar{x}}. \) From this, we also have \( Z_{\Pi_U}(I_{\bar{x}}) = Z_{D_{\bar{x}}}(I_{\bar{x}}) \). But this last group coincides with \( I_{\bar{x}} \) by Lemma 1.1(ii).

(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. \( \square \)

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

**Definition 1.13.** (i) We say that \( \Pi = (\Pi, \Delta, \varphi) \) is a \( \varphi \)-(profinite) group, if \( \Pi \) is a profinite group, \( \Delta \) is a closed normal subgroup of \( \Pi \) and \( \varphi \) is an element of \( \Pi/\Delta \).

(ii) An isomorphism from a \( \varphi \)-group \( \Pi = (\Pi, \Delta, \varphi) \) to another \( \varphi \)-group \( \Pi' = (\Pi', \Delta', \varphi') \) is an isomorphism \( \Pi \cong \Pi' \) as profinite groups that induces \( \Delta \cong \Delta' \), hence also \( \Pi/\Delta \cong \Pi'/\Delta' \), such that the last isomorphism sends \( \varphi \) to \( \varphi' \).

From now on, we regard \( \Pi_U \) as a \( \varphi \)-group by \( \Pi_U = (\Pi_U, \Delta_U, \varphi_k) \), where \( \varphi_k \) stands for the \( k \)-th power Frobenius element in \( G_k = \Pi_U/\Delta_U \). We shall say that an isomorphism \( \alpha : \Pi_U \cong \Pi_{U'} \) as profinite groups is Frobenius-preserving, if \( \alpha \) is an isomorphism as \( \varphi \)-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, \( \varphi \)-group-theoretically) from \( \Pi_U \), if any isomorphism (respectively, any Frobenius-preserving isomorphism) \( \Pi_U \cong \Pi_V \) 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 \( \Pi_U \) 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 \( \Pi_U \cong \Pi_V \) induced by this isomorphism \( U \cong V \) (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, \( \varphi \)-group-theoretically) from \( \Pi_U \), if any isomorphism (respectively, any Frobenius-preserving isomorphism) \( \Pi_U \cong \Pi_V \) 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 \( \Pi_U \):

(i) The subgroup \( \Delta_U \) of \( \Pi_U \), hence the quotient \( G_k = \Pi_U/\Delta_U \).

(ii) The subsets \( \Sigma \) and \( \Sigma^\dagger \) of \( \mathfrak{P} \) primes.

II. The following invariants and structures can be recovered \( \varphi \)-group-theoretically from \( \Pi_U \):

(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 \( r = r_U = \sharp(\overline{S}) \), where \( \overline{S} = \overline{X - U} \).
(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 $\Sigma$ is cofinite. Then the following structure (hence also (iii)-(vii) above) can be recovered group-theoretically from $\Pi_U$:

(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 1.16(ii).)

(ii) Note that $\Delta_{ab}^{ab}U$ 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 $\Pi_U$ 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 $\Sigma$ and $\Sigma^\dagger$ can be recovered group-theoretically from $\Pi_U$. (See also [Mochizuki2], Theorem 1.16(i).)

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

$$\rho_{\text{det}} : G_k \to \text{Aut}(\bigwedge_{\hat{\mathbb{Z}}^{\Sigma^\dagger}}^{\text{max}}((\Delta_{ab}^{ab})^{\Sigma^\dagger})) = (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times.$$

As in the proof of [Tamagawa1], Proposition (3.4)(i), we have $\rho_{\text{det}} = \epsilon x_{\Sigma^\dagger}^{2g+n+b-1}$, where $x_{\Sigma^\dagger}$ is the pro-$\Sigma^\dagger$ cyclotomic character and $\epsilon$ is a certain character (depending on $U$) with values in $\{\pm 1\}$. Now, $p$ can be characterized by $\rho_{\text{det}}(\varphi_k) \in \pm p^2$ ($\subset (\hat{\mathbb{Z}}^{\Sigma^\dagger})^\times$). (See also [Mochizuki2], Remark 1.18.3.)

(iv) Similar to [Tamagawa1], Proposition (3.4)(iii). (See also [Mochizuki2], Remark 1.18.3.)

(v) Similar to [Tamagawa1], Proposition (3.5). (See also [Mochizuki2], Theorem 1.16(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 $l \in \Sigma^\dagger$,

$$\sharp(X(k)) = \sum_{i=0}^{2} (-1)^i \text{tr}(\varphi_k^{-1} | H^i_{\text{et}}(X, \mathbb{Q}_l))$$

$$= \begin{cases} 
1 + \sharp(k), & g = 0, \\
\sum_{i=0}^{2} (-1)^i \text{tr}(\varphi_k^{-1} | H^i(\Delta_X, \mathbb{Q}_l)), & g > 0,
\end{cases}$$
and

\[ \sharp(U(k)) = \sum_{i=0}^{2} (-1)^i \text{tr}(\varphi_k^{-1} \mid H_c^i(U_l, \mathbb{Q}_l)) \]

\[ = \sum_{i=0}^{2} (-1)^i \text{tr}(\varphi_k \mid H_{\text{et}}^i(U_l, \mathbb{Q}_l(1))) \]

\[ = \sharp(k) \sum_{i=0}^{2} (-1)^i \text{tr}(\varphi_k \mid H^i(U_l, \mathbb{Q}_l)) \]

\[ = \sharp(k) \sum_{i=0}^{2} (-1)^i \text{tr}(\varphi_k \mid H^i(\Delta_U, \mathbb{Q}_l)). \]

Here, for a profinite group \( \Gamma \), we define

\[ H^i(\Gamma, \mathbb{Q}_l) \overset{\text{def}}{=} (\lim_{\leftarrow} H^i(\Gamma, \mathbb{Z}/l^n\mathbb{Z})) \otimes_{\mathbb{Z}/l^n} \mathbb{Q}_l, \]

as usual. Thus, \( \sharp(X(k)) \) and \( \sharp(U(k)) \) can be recovered \( \varphi \)-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 \( (\rho^\text{det})^2 = \chi^{2(g+n+b-1)} \) is an open subgroup of the subgroup \( \overline{(p)} \) of \( (\hat{\mathbb{Z}} \Sigma')^\times \) (topologically) generated by \( p \). This characterizes group-theoretically the prime number \( p \) (in \( (\Sigma')' = \Sigma' \cup \{p\} \)), by a theorem of Chevalley ([Chevalley], Théorème 1). Next, define \( m \) to be the minimal positive integer with \( p^m \in (\rho^\text{det})^2(G_k) \) \( \subset (\hat{\mathbb{Z}} \Sigma')^\times \). Then \( \varphi_k \) can be characterized by \( (\rho^\text{det})^2(\varphi_k) = p^m \). (See also [Mochizuki2], Remark 1.18.1.) \( \square \)

**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 \( \Pi_U \), we set \( G_H = \text{pr}_U(H) \) and \( k_H \overset{\text{def}}{=} k_{G_H} \). We denote by \( U_H \) the (pro-finite, pro-tame, geometrically pro-\( \Sigma \)) 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 \( \Pi_{U_H} \).

(iii) Let \( H \) be a closed subgroup of \( \Pi_U \) and \( G \) a closed subgroup of \( G_H \). Then we set \( H_G \overset{\text{def}}{=} H \cap \text{pr}_U^{-1}(G) \). Observe that \( U_{H_G} \) can be identified with \( U_H \times_{k_H} k_G \).

(iv) For each open subgroup \( H \) of \( \Pi_U \), we set

\[ \nu_U(H) \overset{\text{def}}{=} \sharp(U(H(k_H))). \]

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

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

Finally, we shall prove that the set of decomposition groups in \( \Pi_U \) can be recovered group-theoretically from \( \Pi_U \). First, we shall treat decomposition groups at points of \( S_U \).
Theorem 1.18. (i) The set of inertia groups at points of \( \tilde{S}_U \) (i.e., the image of the injective map \( I|_{\tilde{S}_U} : \tilde{S}_U \to \text{Sub}(\Delta_U) \subset \text{Sub}(\Pi_U) \)) can be recovered \( \varphi \)-group-theoretically from \( \Pi_U \).
(ii) The set of decomposition groups at points of \( \tilde{S}_U \) (i.e., the image of the injective map \( D|_{\tilde{S}_U} : \tilde{S}_U \to \text{Sub}(\Pi_U) \)) can be recovered \( \varphi \)-group-theoretically from \( \Pi_U \).

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 goes well over finite fields.
(ii) This follows from (i), together with Corollary 1.12(ii). \(\Box\)

Next, we shall treat decomposition groups at points of \( \tilde{U}^{cl} \). 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 \( S(\Pi_U) \subset \text{Sub}(\Pi_U) \) the set of closed subgroups \( Z \) of \( \Pi_U \) such that \( \tilde{G}_Z \) is open in \( \tilde{G}_k \) and that \( \text{pr}_U|_Z : Z \to G_Z \) is an isomorphism.
(ii) For each open subgroup \( G \) of \( G_k \), we set

\[
S(\Pi_U)_G \overset{\text{def}}{=} \{ Z \in S(\Pi_U) \mid G_Z = G \}.
\]

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

Definition 1.20. Let \( Z \) be an element of \( S(\Pi_U) \).
(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 \( (\Pi_U)_G_Z/H \) 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 \( U_Z(\overline{k})^{\text{fin}} \) 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 \( U_Z(\overline{k})^{\text{fin}} \subset U_Z(\overline{k}) \).)
We denote by \( \overline{\nu}_\infty(Z) \) the cardinality of \( U_Z(\overline{k})^{\text{fin}} \). Moreover, we define \( (U_Z)^{cl, fin} \) to be the image of \( U_Z(\overline{k})^{\text{fin}} \) in \( U_Z^{cl} \).

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

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

15
(iii) We have $\nu^\ast_\infty(Z) \leq \nu_\infty(Z) \leq \nu_\infty(\Pi_U G_Z) < \infty$.
(iv) Assume, moreover, that $\Sigma$ is cofinite. Then we have $\nu_\infty(Z) < \infty$.

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 $\text{pr}_U$ must coincide with $G$. Since $\text{pr}_U$ induces an isomorphism $Z_G \rightarrow G$, 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 $\text{pr}_U$ induces an isomorphism $D_{\tilde{x}} \sim \text{pr}_U(D_{\tilde{x}})$ and that $\text{pr}_U(Z_G) = G$ is open in $\text{pr}_U(D_{\tilde{x}})$.)

(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 $Z$ coincide with $Z$, which implies $x \in U_Z(k_Z)$.

Next, we define $x_U$ to be the image of $x$ in $U^{\mathrm{cl}}$. 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, $\text{pr}_U(D_{\tilde{x}}) = \text{pr}_U(Z)$. This implies $D_{\tilde{x}} = Z$. Conversely, suppose $Z = D_{\tilde{x}}$. Then $\text{pr}_U(D_{\tilde{x}}) = \text{pr}_U(Z)$, 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 $(U_Z)_{\tilde{G}_Z}^{\mathrm{cl}}$. Then

$$x \in (U_Z)^{\mathrm{cl}, \mathrm{fin}} \quad \iff \quad x_G \in U_{Z_G}(k_{Z_G}) \text{ for some open subgroup } G \text{ of } G_Z$$

$$\iff Z_G \subset D_{\tilde{x}} \text{ for some open subgroup } G \text{ of } G_Z$$

$$\iff Z \text{ and } D_{\tilde{x}} \text{ are commensurate.}$$

(iii) The first two inequalities are clear. To see the third inequality, it suffices to prove that the natural map $U_Z(k_Z) \twoheadrightarrow U_{(\Pi_U)G_Z}(k_Z)$ 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 $\tilde{U}^{\mathrm{cl}}$ must coincide with each other. It follows from these and Proposition 1.8(iii) that $\tilde{x} = \tilde{x}'$ holds. Thus, $x = x'$ holds, as desired. Finally, the fourth equality is clear.

(iv) This follows from (ii) and Proposition 1.8(vii). (Observe that the natural surjective map $U_Z(k_Z)^{\mathrm{fin}} \twoheadrightarrow (U_Z)^{\mathrm{cl}, \mathrm{fin}}$ is quasi-finite.) □

Corollary 1.22. Let $Z$ be an element of $\mathcal{S}(\Pi_U)$. Then we have

(i) There exists $\tilde{x} \in \tilde{U}^{\mathrm{cl}}$ 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, $\nu^*_\infty(Z) > 0$).

(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 $\nu_\infty(Z) > 1$.

(iii) There exists $\tilde{x} \in \tilde{U}^{\mathrm{cl}} - E_{\tilde{U}}$ (respectively, $\tilde{x} \in E_{\tilde{U}}$) such that $Z = D_{\tilde{x}}$ if and only if $\nu_\infty(Z) = \nu^*_\infty(Z) = 1$ (respectively, $\nu^*_\infty(Z) > 0$ and $\nu_\infty(Z) > 1$).

Proof. (i) This is immediate from Proposition 1.21(ii).
(ii) By definition, \( \varpi_{\infty}(Z) > 1 \) 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 \( \varpi_{\infty}(Z) > 1 \) (respectively, \( \leq 1 \)) if and only if \( Z = D_{\tilde{x}} \) for some \( \tilde{x} \in \hat{U}^{\text{cl}} \) and \( Z \) is commensurate to \( D_{\tilde{x}} \) for more than (respectively, at most) one \( \tilde{x} \in \hat{U}^{\text{cl}} \). This last statement is equivalent to saying that \( Z = D_{\tilde{x}} \) for some \( \tilde{x} \in E_{\hat{U}} \) (respectively, \( \tilde{x} \in \hat{U}^{\text{cl}} - E_{\hat{U}} \)). This, together with Proposition 1.21(iii) (or, more specifically, the fact \( \nu^*_\infty(Z) \leq \varpi_{\infty}(Z) \)), completes the proof. \( \square \)

**Proposition 1.23.** Let \( Z \) be an element of \( S(\Pi_U) \).

(i) We have

\[
\lim_{H \in \mathcal{U}(Z)} \frac{\nu_U(H)}{m(H, Z)} = \nu_{\infty}(Z).
\]

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

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

In particular, \( \nu_{\infty}(Z) \) is a \( \varphi \)-group-theoretic invariant.

(ii) Set \( C \overset{\text{def}}{=} C_{\Pi_U}(Z) \), which is isomorphic to \( \hat{\mathbb{Z}} \). Then we have

\[
\nu^*_\infty(Z) = \sum_{d \mid N} \mu(N/d) \nu_{\infty}(C^d),
\]

where \( N \overset{\text{def}}{=} (C : Z) \), \( C^d \overset{\text{def}}{=} \{ \sigma^d \mid \sigma \in C \} \), and \( \mu \) stands for Möbius’ function.

In particular, \( \nu^*_\infty(Z) \) is a \( \varphi \)-group-theoretic invariant.

(iii) We have

\[
\sup_{G \in \text{OSub}(G_Z)} \nu_{\infty}(Z_G) = \varpi_{\infty}(Z).
\]

In particular, \( \varpi_{\infty}(Z) \) is a \( \varphi \)-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 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 \( U_Z(k_Z) = \lim_{H \in \mathcal{U}(Z)} U_H(k_Z) \) and \( \sharp(U_H(k_Z)) < \infty \) for each \( H \in \mathcal{U}(Z) \), we see that there exists \( H_0 \in \mathcal{U}(Z) \) 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 \( U_H(k_Z) \) is above some point of \( U_{(\Pi_U)G_Z}(k_Z)^{\infty} \). Moreover, for each point \( x \in U_Z(k_Z) \), take the unique point \( \tilde{x} \in \hat{U}^{\text{cl}} \) 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.

(ii) First, by Lemma 1.7, we see that \( C \in S(\Pi_U) \) and that \( C \) is isomorphic to \( \hat{\mathbb{Z}} \).
Let \( x \) be a point of \( U_Z(k_Z) \). We claim that \( x \not\in U_Z(k_Z)^* \) if and only if there exists \( Z' \in \mathcal{S}(\Pi_U) \) with \( Z' \supset Z \), such that the image in \((U_{Z'})^{cl}\) of \( x \in U_Z(k_Z) \subset (U_Z)^{cl} \) 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 \((U_{Z'})^{cl}\) is \( k_{Z'} \)-rational, so is the image of \( x \) in \( U^{cl} \), hence \( x \not\in U_Z(k_Z)^* \). Conversely, suppose \( x \not\in U_Z(k_Z)^* \) and take the unique point \( \tilde{x} \in U^{cl} \) 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 \( Z' \overset{\text{def}}{=} D_{\tilde{x}} \) 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 \((U_{Z'})^{cl}\) is \( k_{Z'} \)-rational if and only if \( x \in U_Z(k_Z) = U_C(k_Z) \) falls in \((U_{Z'})^{cl}(k_{Z'}) = U_C(k_{Z'}) \).

These, together with the so-called inclusion-exclusion principle, imply the desired formula.

(iii) Immediate from the definitions. \( \square \)

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

**Proof.** This follows formally from Corollary 1.22 and Proposition 1.23. \( \square \)

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

**Proof.** This is immediate from Theorem 1.18(ii) and Theorem 1.24. (See also [Mochizuki2], Remark 1.18.2.) \( \square \)

**§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 \( \Delta_X \) stands for the maximal pro-\( \Sigma \) quotient of \( \pi_1(\overline{X}) \), that \( \Pi_X \) stands for \( \pi_1(X)/\Ker(\pi_1(\overline{X}) \to \Delta_X) \), and that they fit into the following exact sequence:

\[
1 \to \Delta_X \to \Pi_X \overset{\text{pr}_X}{\to} G_k \to 1.
\]

Similarly, if we write \( X \times X \overset{\text{def}}{=} X \times_k X \), then we obtain (by considering the maximal pro-\( \Sigma \) 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 1.5(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-$\Sigma^*$, where $\Sigma^*$ is a set of prime numbers) (relative to $H \to \Pi_X$) if $I_H$ is abelian (respectively, if $I_H$ is a pro-$\Sigma^*$ group). If $H$ is cuspidally abelian, then observe that $H/I_H$ acts naturally (by conjugation) on $I_H$. 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 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 $\Pi_X$ is replaced by $\Delta_X$, $\Pi_{X \times X}$, or $\Delta_{X \times X}$.

For a finite subset $S \subset X^{cl}$ write $U_S \overset{\text{def}}{=} X - S$. Let $\Delta_{U_S}$ be the maximal cuspidally (relative to the natural map to $\Delta_X$) pro-$\Sigma^*$ quotient of the maximal pro-$\Sigma$ 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 $\Pi_{U_S}$ be the corresponding quotient $\pi_1(U_S)/\text{Ker}(\pi_1(\overline{U_S}) \twoheadrightarrow \Delta_{U_S})$ 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:

$$
\begin{array}{ccc}
1 & \to & \Delta_{U_S} \\
\downarrow & & \downarrow \\
1 & \to & \Delta_X
\end{array}
\quad
\begin{array}{ccc}
\Pi_{U_S} & \to & G_k \\
\downarrow & & \downarrow \\
\Pi_X & \to & G_k \\
\downarrow & & \downarrow \\
1 & \to & 1
\end{array}
$$

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

$$U_{X \times X} \overset{\text{def}}{=} X \times X - \iota(X).$$

We shall denote by $\Delta_{U_{X \times X}}$ the maximal cuspidally (relative to the natural map to $\Delta_{X \times X}$) pro-$\Sigma^*$ quotient of the maximal pro-$\Sigma$ quotient of the tame fundamental group of $(U_{X \times X})_\kbar$ (where “tame” is with respect to the divisor $\iota(X) \subset X \times X$), and by $\Pi_{U_{X \times X}}$ the corresponding quotient $\pi_1(U_{X \times X})/\text{Ker}(\pi_1(U_{X \times X}) \twoheadrightarrow \Delta_{U_{X \times X}})$ 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:

$$
\begin{array}{ccc}
1 & \to & \Delta_{U_{X \times X}} \\
\downarrow & & \downarrow \\
1 & \to & \Delta_{X \times X}
\end{array}
\quad
\begin{array}{ccc}
\Pi_{U_{X \times X}} & \to & G_k \\
\downarrow & & \downarrow \\
\Pi_{X \times X} & \to & G_k \\
\downarrow & & \downarrow \\
1 & \to & 1
\end{array}
$$

Finally, set

$$M_X \overset{\text{def}}{=} \text{Hom}_{2\Sigma^*}(H^2(\Delta_X, \hat{\mathbb{Z}}^{\Sigma^*}), \hat{\mathbb{Z}}^{\Sigma^*}).$$
Thus, $M_X$ is a free $\hat{\mathbb{Z}}^{\Sigma}$-module of rank 1, and $M_X$ is isomorphic to $\hat{\mathbb{Z}}^{\Sigma}(1)$ as a $G_k$-module (where the “(1)” denotes a “Tate twist”, i.e., $G_k$ acts on $\hat{\mathbb{Z}}^{\Sigma}(1)$ 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 $\Sigma_X$ (respectively, $\Sigma_Y$) be a set of prime numbers that contains at least one prime number different from $p_X$ (respectively, $p_Y$). Write $\Delta_X$ (respectively, $\Delta_Y$) for the maximal pro-$\Sigma_X$ quotient of $\pi_1(\overline{X})$ (respectively, the maximal pro-$\Sigma_Y$ quotient of $\pi_1(\overline{Y})$), and $\Pi_X$ (respectively, $\Pi_Y$) for the quotient $\pi_1(X)/\text{Ker}(\pi_1(\overline{X}) \rightarrow \Delta_X)$ of $\pi_1(X)$ (respectively, the quotient $\pi_1(Y)/\text{Ker}(\pi_1(\overline{Y}) \rightarrow \Delta_Y)$ of $\pi_1(Y)$).

Let

$$\alpha : \Pi_X \sim \Pi_Y$$

be an isomorphism of profinite groups.

The following is one of the main results of Mochizuki’s theory (cf. [Mochizuki2], Theorem 1.16(iii)).

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

$$\begin{array}{ccc}
\Pi_{U_{X\times X}^c}^{c-ab} & \rightarrow & \Pi_{U_{Y\times Y}^c}^{c-ab} \\
\downarrow & & \downarrow \\
\Pi_{X\times X} & \overset{\alpha \times \alpha}{\rightarrow} & \Pi_{Y\times Y}
\end{array}$$

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

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

is functorial (up to cuspidally inner automorphism) with respect to $\alpha$.

**Proof.** See [Mochizuki2], Theorem 1.16(iii). \(\square\)

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

For the rest of this §, we shall assume that $\alpha$ is Frobenius-preserving (cf. Definition 1.14). (Note that this assumption is automatically satisfied in the case where $\Sigma_X$ and $\Sigma_Y$ are cofinite by Theorem 1.15(viii).) Thus, by Theorem 1.24, one deduces naturally from $\alpha$ a bijection

$$\phi : X^{\text{cl}} - E_X \sim Y^{\text{cl}} - E_Y$$

such that

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

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

As an important consequence of Theorem 2.2 we deduce the following:
Corollary 2.3. With the above assumptions, let $S \subset X^{cl} = E_X$, $T \subset Y^{cl} = E_Y$ be finite subsets that correspond to each other via $\phi$. Then $\alpha$, $\alpha^{c,ab}$ induce isomorphisms (well-defined up to cuspidally inner automorphisms, i.e., inner automorphisms by elements of $\text{Ker}(\Pi_{V_T}^{c,ab} \rightarrow \Pi_Y^{c,ab})$)

$$\alpha^{c,ab}_{S, T} : \Pi_{U_S}^{c,ab} \sim \Pi_{V_T}^{c,ab}$$

lying over $\alpha$, where $U_S \overset{\text{def}}{=} X - S$, $V_T \overset{\text{def}}{=} Y - T$, and $\Pi_{U_S} \rightarrow \Pi_{U_S}^{c,ab}$, $\Pi_{V_T} \rightarrow \Pi_{V_T}^{c,ab}$, are the maximal cuspidally abelian quotients (relative to the maps $\Pi_{U_S} \rightarrow \Pi_X$, $\Pi_{V_T} \rightarrow \Pi_Y$, respectively). These isomorphisms are functorial with respect to $\alpha$, $S$, $T$, as well as with respect to passing to connected finite étale coverings of $X$, $Y$, which arise from open subgroups of $\Pi_X$, $\Pi_Y$, in the following sense: Let $\xi : X' \rightarrow X$ (respectively, $\eta : Y' \rightarrow Y$) 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 $U'_S \overset{\text{def}}{=} X' - S'$, $V'_T \overset{\text{def}}{=} Y' - T'$, $S' \overset{\text{def}}{=} \xi^{-1}(S)$, $T' \overset{\text{def}}{=} \eta^{-1}(T)$; and denote by $\alpha'$ the isomorphism $\Pi_{X'} \rightarrow \Pi_{Y'}$ induced by $\alpha$. Then we have the following commutative diagram:

$$\begin{array}{ccc}
\Pi_{U'_S}^{c,ab} & \xrightarrow{(\alpha')^{c,ab}_{S', T'}} & \Pi_{V'_T}^{c,ab} \\
\downarrow & & \downarrow \\
\Pi_{U_S}^{c,ab} & \xrightarrow{\alpha^{c,ab}_{S, T}} & \Pi_{V_T}^{c,ab}
\end{array}$$

where the vertical arrows are the natural maps.

Proof. The proof of [Mochizuki2], Theorem 2.5(i) (where $E_X = E_Y = \emptyset$ is assumed) works as it is. □

Next, let

$$1 \rightarrow M_X \rightarrow D \rightarrow \Pi_{X \times X} \rightarrow 1$$

be a fundamental extension, i.e., an extension whose corresponding extension class in $H^2_{\text{et}}(X \times X, M_X)$ (via the natural identification $H^2(\Pi_{X \times X}, M_X) \sim H^2_{\text{et}}(X \times X, M_X)$ (cf. [Mochizuki2], Proposition 1.1)) coincides with the first (étale) Chern class of the diagonal $\iota(X)$ (cf. [Mochizuki2], Proposition 1.6). 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

$$D_x \overset{\text{def}}{=} D|_{D_x \times G_k \Pi_X}, \quad D_{x, y} \overset{\text{def}}{=} D|_{D_x \times G_k D_y}.$$ 

Thus, $D_x$ (respectively, $D_{x, y}$) is an extension of $\Pi_X$ (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

$$D_D \overset{\text{def}}{=} \sum_i m_i D_{x_i}, \quad D_{D, E} \overset{\text{def}}{=} \sum_{i, j} m_i n_j D_{x_i, y_j}$$

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

21
For a finite subset $S \subset X(k)$, we shall write
\[
\mathcal{D}_S \overset{\text{def}}{=} \prod_{x \in S} \mathcal{D}_x
\]
where the product is to be understood as a fiber product over $\Pi_X$. Thus, $\mathcal{D}_S$ is an extension of $\Pi_X$ 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 $\Pi_X$. Observe that if $T \subset X(k)$ is a finite subset containing $S$, then we obtain a natural projection morphism $\mathcal{D}_T \to \mathcal{D}_S$. More generally, for a finite subset $S \subset X^{\text{cl}}$ 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 1.10.1 for more details.)

**Proposition 2.4 (Maximal Geometrically Cuspidally Central Quotients).**
(i) For $S \subset X^{\text{cl}}$ a finite subset, the $S$-cuspidalization $\mathcal{D}_S$ of $\Pi_X$ may be identified with the quotient $\Pi_{U_S} \to \prod_{\Pi_S^{\text{cn}}} \Pi_{U_S}/\text{Ker}(\Delta_{U_S} \to \Delta_{U_S}^{\text{cn}})$ of $\Pi_{U_S}$, where $\Delta_{U_S}^{\text{cn}}$ is the maximal cuspidally central quotient of $\Delta_{U_S}$ relative to the natural map $\Delta_{U_S} \to \Delta_X$.

(ii) The fundamental extension $\mathcal{D}$ may be identified with the quotient $\Pi_{X \times X} \to \Pi_{U_{X \times X}}^{\text{cn}} \overset{\text{def}}{=} \Pi_{U_{X \times X}} / \text{Ker}(\Delta_{U_{X \times X}} \to \Delta_{U_{X \times X}}^{\text{cn}})$ of $\Pi_{U_{X \times X}}$, where $\Delta_{U_{X \times X}}^{\text{cn}}$ is the maximal cuspidally central quotient of $\Delta_{U_{X \times X}}$ relative to the natural map $\Delta_{U_{X \times X}} \to \Delta_{X \times X}$.

**Proof.** See [Mochizuki2], Proposition 1.8(iii)(iv). (Precisely speaking, Proposition 1.8(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 1.10.1 loc. cit.)

**Remark 2.5.** Let $\mathcal{D}$ (respectively, $\mathcal{E}$) be a fundamental extension of $X$ (respectively, $Y$). The isomorphism $\alpha : \Pi_X \sim \Pi_Y$ induces an isomorphism:
\[
\mathcal{D} \sim \mathcal{E}
\]
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 $S \subset X^{\text{cl}} = E_X$ and $T \subset Y^{\text{cl}} = E_Y$ be as in Corollary 2.3 and write $\mathcal{D}_S$ (respectively, $\mathcal{E}_T$) for the $S$-cuspidalization of $\Pi_X$ (respectively, the $T$-cuspidalization of $\Pi_Y$). Then the isomorphism $\mathcal{D} \sim \mathcal{E}$ induces an isomorphism $\mathcal{D}_S \sim \mathcal{E}_T$ lying over $\alpha$.

On the other hand, let $\Pi_{U_S} \to \Pi_{U_S}^{\text{cn}}$ and $\Pi_{U_T} \to \Pi_{U_T}^{\text{cn}}$ be the maximal geometrically cuspidally central quotients (here, $U_S \overset{\text{def}}{=} X - S$, $V_T \overset{\text{def}}{=} Y - T$) (cf. Proposition 2.4). Note that the isomorphism $\alpha_{S,T}^{\text{ab}} : \Pi_{U_S}^{\text{cn}} \sim \Pi_{U_T}^{\text{cn}}$ in Corollary 2.3 naturally induces an isomorphism
\[
\Pi_{U_S}^{\text{cn}} \sim \Pi_{U_T}^{\text{cn}}
\]
lying over $\alpha$, which is well-defined up to cuspidally inner automorphism. Now, by Proposition 2.4(i), $\Pi^{\text{cn}}_{\bar{U}}$ (respectively, $\Pi^{\text{cn}}_{\bar{V}}$) 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 $\alpha$.

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 $(k^\times_X)^{\Sigma^\dagger}$, $(k^\times_Y)^{\Sigma^\dagger}$.

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

**Theorem 2.7 (Reconstruction of Maximal Cuspidally Pro-$l$ Extensions).**

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

$$\begin{array}{ccc}
\Pi^{c-l}_{\bar{U}} & \xrightarrow{\alpha^{c-l}} & \Pi^{c-l}_{\bar{V}} \\
\downarrow & & \downarrow \\
\Pi_X & \xrightarrow{\alpha} & \Pi_Y
\end{array}$$

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

$$\Pi^{c-l}_{\bar{U}} \rightarrow \Pi^{c,\text{ab},l}_{\bar{U}}; \quad \Pi^{c-l}_{\bar{V}} \rightarrow \Pi^{c,\text{ab},l}_{\bar{V}}$$

where the subscript “c-ab, $l$” denotes the maximal cuspidally pro-$l$ abelian quotient, with the isomorphism

$$\alpha^{c,\text{ab}}_{S,T} : \Pi^{c,\text{ab}}_{\bar{U}} \xrightarrow{\sim} \Pi^{c,\text{ab}}_{\bar{V}}$$

in Corollary 2.3. Moreover, $\alpha^{c-l}$ is compatible, up to cuspidally inner automorphisms, with the decomposition groups of $x_*$, $y_*$ in $\Pi^{c-l}_{\bar{U}}$, $\Pi^{c-l}_{\bar{V}}$. □

**Proof.** See [Mochizuki2], Theorem 3.10. □

§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

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

where $\mathbb{G}_m \rightarrow \mathbb{G}_m$ is the $n$-th power map. We shall identify $\mu_n$ with $M_X/nM_X$ according to the identification in [Mochizuki2], the discussion at the beginning of §2.
Consider a subset \( E \subset X \). 

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

\[
\Gamma(U_S, \mathcal{O}_U^X) \to H^1(\Pi_U, M_X)
\]

(cf. loc. cit.). (Note that here it suffices to consider the group cohomology of \( \Pi_U \) (i.e., as opposed to the étale cohomology of \( U_S \)), since the extraction of \( n \)-th roots of an element of \( \Gamma(U_S, \mathcal{O}_U^X) \) yields finite étale coverings of \( U_S \) that correspond to open subgroups of \( \Pi_U \).) Observe that this is injective if \( \Sigma^\dagger = \text{Primes} - \{p\} \), since the abelian group \( \Gamma(U_S, \mathcal{O}_U^X) \) 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 \( X - E \), we obtain a natural homomorphism

\[
\mathcal{O}_E^X \to \lim_{S} H^1(\Pi_U, M_X),
\]

where \( \mathcal{O}_E^X \defeq \{ f \in K_X^X \mid \text{sup}(\text{div}(f)) \cap E = \emptyset \} \) 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 is injective if \( \Sigma^\dagger = \text{Primes} - \{p\} \).

**Proposition 3.1 (Kummer Classes of Functions).** Suppose that \( S \subset X - E \) is a finite subset. Write

\[
\Delta_U \twoheadrightarrow \Delta_{U_S}^{\text{c-ab}} \twoheadrightarrow \Delta_{U_S}^{\text{c-cn}}
\]

for the maximal cuspidally abelian and the maximal cuspidally central quotients, respectively, relative to the map \( \Delta_U \twoheadrightarrow \Delta_X \), and

\[
\Pi_U \twoheadrightarrow \Pi_{U_S}^{\text{c-ab}} \twoheadrightarrow \Pi_{U_S}^{\text{c-cn}}
\]

for the corresponding quotients of \( \Pi_U \) (i.e., \( \Pi_{U_S}^{\text{c-ab}} \defeq \Pi_U / \ker(\Delta_U \twoheadrightarrow \Delta_{U_S}^{\text{c-ab}}) \), \( \Pi_{U_S}^{\text{c-cn}} \defeq \Pi_U / \ker(\Delta_U \twoheadrightarrow \Delta_{U_S}^{\text{c-cn}}) \)). If \( x \in X \), then we shall write

\[
D_x[U_S] \subset \Pi_U
\]

for the decomposition group at \( x \) in \( \Pi_U \) (which is well-defined up to conjugation), and \( I_x[U_S] \defeq D_x[U_S] \cap \Delta_U \) 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 1.6(ii)(iii)). Then:

(i) The natural surjections induce the following isomorphisms:

\[
H^1(\Pi_{U_S}^{\text{c-cn}}, M_X) \sim H^1(\Pi_{U_S}^{\text{c-ab}}, M_X) \sim H^1(\Pi_U, M_X)
\]
In particular, we obtain the following natural homomorphisms:

\[ \Gamma(U_S, \mathcal{O}_{U_S}^\times) \to H^1(\Pi_{U_S}^{c\text{cn}}, M_X) \cong H^1(\Pi_{U_S}^{c\text{ab}}, M_X) \cong H^1(\Pi_{U_S}, M_X), \]

\[ \mathcal{O}_E^\times \to \lim_S H^1(\Pi_{U_S}^{c\text{cn}}, M_X) \cong \lim_S H^1(\Pi_{U_S}^{c\text{ab}}, M_X) \cong \lim_S H^1(\Pi_{U_S}, M_X), \]

where \( S \) varies among all finite subsets of \( X - E \).

These natural homomorphisms are injective, if, moreover, \( \Sigma^\dagger = \text{Primes} - \{p\} \).

(ii) Restricting cohomology classes of \( \Pi_{U_S} \) 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 \( \text{Hom}_{\hat{\mathbb{Z}}^\Sigma^\dagger}(I_x[U_S], M_X) \) 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 \( \Pi_{U_S} \) is replaced by \( \Pi_{U_S}^{c\text{cn}} \) or \( \Pi_{U_S}^{c\text{ab}} \).

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

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

for the associated Kummer classes. If \( x \in (X^\text{cl} - E) - S \), then \( D_x[U_S] \) maps, via the natural surjection \( \Pi_{U_S} \to G_k \), 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

\[ \kappa_f^{c\text{cn}}|_{D_x[U_S]} = \kappa_f^{c\text{ab}}|_{D_x[U_S]} = \kappa_f|_{D_x[U_S]} \in H^1(D_x[U_S], M_X) \cong H^1(G_{k(x)}, M_X) \]

\[ \cong (k(x)^\times)^\Sigma^\dagger \]

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.) \( \square \)

Remark 3.2. (cf. [Mochizuki2], Remark 2.1.1.) 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 \( \Pi_{U_S}^{c\text{cn}} \) of \( \Pi_X \) 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 \( \Pi_{U_S}^{c\text{cn}} \) may be thought of as the image of \( D_x[U_S] \) in \( D_S \). This image of \( D_x[U_S] \) in \( D_S \) amounts to a section of \( D_S \to \Pi_X \to G_k \) 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 \( D_S \)
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 $D_{y,x}$ by an element of $\text{Ker}(D_{y,x} \to G_k)$)

$$\gamma_{y,x} : G_k \to D_{y,x},$$

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 $(k(x)^\times)^\Gamma = (k^\times)^\Gamma$ 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 $\gamma_{y,x} : G_k \to D_{y,x}$ 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 2.2.) For $x, y \in X(k)$ with $x \neq y$, we shall refer to the above section (regarded as a cyclotomically outer homomorphism)

$$\gamma_{y,x} : G_k \to D_{y,x}$$

as the Green’s trivialization of $D$ 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)

$$\gamma_{D,x} : G_k \to D_{D,x}$$

which we shall refer to as the Green’s trivialization of $D$ at $(D, x)$.

**Definition 3.4.** (cf. [Mochizuki2], Definition 2.4.) Let the notations and the assumptions as in Corollary 2.3.

(i) Write $D$ (respectively, $E$) for the fundamental extension of $\Pi_{X \times X}$ (respectively, $\Pi_{Y \times Y}$) that arises as the quotient of $\Pi_{X \times X}^{ab}$ (respectively, $\Pi_{Y \times Y}^{ab}$) by the kernel of the maximal cuspidally central quotient $\Delta_{U_{X \times X}}^{ab} \twoheadrightarrow \Delta_{U_{X \times X}}^{c-cn}$ (respectively, $\Delta_{U_{Y \times Y}}^{ab} \twoheadrightarrow \Delta_{U_{Y \times Y}}^{c-cn}$) (cf. Proposition 2.4(ii)). The isomorphism $\alpha^{c-ab}$ induces naturally an isomorphism:

$$\alpha^{c-cn} : D \sim \to E$$

We shall say that $\alpha$ 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 $\phi$ to a pair of points $(y_1, y_2) \in Y(k_Y) \times Y(k_Y)$, such that $x_1 \in (X^{\text{cl}} - E_X) - S$, $y_1 \in (Y^{\text{cl}} - E_Y) - T$, $x_2 \in S$, $y_2 \in T$, the isomorphism

$$D_{x_1, x_2} \sim \to \mathcal{E}_{y_1, y_2}$$

(obtained by restricting $\alpha^{c-cn}$ to the various decomposition groups) is compatible with the Green’s trivializations. We shall say that $\alpha$ 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 $X^{\text{cl}} - E_X$, corresponding via $\phi$ to a pair $(y, E)$ (so $y \in Y(k_Y) \cap T$), the isomorphism

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

obtained from $\alpha^{c-cn}$ is compatible with the Green’s trivializations.

26
(ii) We shall say that \( \alpha \) 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 \( \alpha \), then for any subset \( S \subset X^{\text{cl}} - E_X \) that corresponds, via \( \phi \), to \( T \subset Y - E_Y \) the isomorphism

\[
\Pi_{X'} \cong \Pi_{Y'}
\]

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

**Remark/Definition 3.5.** Let \( J = J_X \) be the Jacobian variety of \( X \). Let \( \text{Div}^0_{X-E_X} \) be the group of degree zero divisors on \( X \) which are supported on points in \( X - E_X \). Write \( D_{X-E_X} \) for the kernel of the natural homomorphism \( \text{Div}^0_{X-E_X} \to J(k)\Sigma \).

Here, \( J(k)\Sigma \) stands for the maximal \( \Sigma \)-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 \( \Sigma' \). Then \( D_{X-E_X} \) sits naturally in the following exact sequence:

\[
0 \to \text{Pri}_{X-E_X} \to D_{X-E_X} \to J(k)\{\Sigma'\} \to 0,
\]

where \( \text{Pri}_{X-E_X} \defeq \mathcal{O}_{E_X}^\times / k^\times \) stands for the group of principal divisors supported in \( X - E_X \).

**Theorem 3.6 (Reconstruction of Functions).** In the situation of Theorem 2.2, assume that \( \alpha \) is Frobenius-preserving. Write \( \Sigma \defeq \Sigma_X = \Sigma_Y \) and \( p \defeq p_X = p_Y \) (cf. Proposition 1.15(ii)(iii)). Then:

(i) The bijection \( \phi : X^{\text{cl}} - E_X \cong Y^{\text{cl}} - E_Y \) induced by \( \alpha \) (where \( E_X \) and \( E_Y \) are the exceptional sets) induces a natural bijection between the groups \( D_{X-E_X}, D_{Y-E_Y} \).

(ii) Assume, moreover, \( \Sigma = \mathfrak{Primes} - \{p\} \). Then the bijection in (i), together with the isomorphisms in Corollary 2.3, induces naturally an injective homomorphism

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

where \( p^n \) is the exponent of the \( p \)-primary abelian group \( J_Y(k_Y)\{\Sigma'\} \).

Moreover, this injective homomorphism \( \mathcal{O}_{E_X}^\times \hookrightarrow (\mathcal{O}_{E_Y}^\times)^{p^{-n}} \) 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 \( \alpha \) (thus, \( \Pi_{Y'} = \alpha(\Pi_{X'}) \)), then we have a commutative diagram:

\[
\begin{array}{ccc}
\mathcal{O}_{E_{X'}}^\times & \longrightarrow & (\mathcal{O}_{E_{Y'}}^\times)^{p^{-n'}} \\
\uparrow & & \uparrow \\
\mathcal{O}_{E_X}^\times & \longrightarrow & (\mathcal{O}_{E_Y}^\times)^{p^{-n}}
\end{array}
\]

where \( E_{X'} \defeq \xi^{-1}(E_X), E_{Y'} \defeq \eta^{-1}(E_Y) \), \( p^{n'} \geq p^n \) is the exponent of the \( p \)-primary abelian group \( J_Y(k_Y)\{\Sigma'\} \), and the vertical arrows are the natural embeddings.
Proof. (cf. [Mochizuki2], Theorem 2.5(ii).) 
(i) First, \( \phi \) induces naturally a bijection \( \text{Div}^0_{X-E_X} \cong \text{Div}^0_{Y-E_Y} \). Second, the natural homomorphism \( \text{Div}^0_{X-E_X} \to J(k_X) \Sigma \) can be recovered \( \varphi \)-group-theoretically from \( \Pi_X \). (Observe the pro-\( \Sigma \) version of [Mochizuki2], Proposition 2.3(i).) See also the discussion before Proposition 2.3 loc. cit.) Thus, \( \alpha \) induces naturally a commutative diagram:

\[
\begin{array}{ccc}
\text{Div}^0_{X-E_X} & \longrightarrow & J_X(k_X) \Sigma \\
\downarrow & & \downarrow \\
\text{Div}^0_{Y-E_Y} & \longrightarrow & J_Y(k_Y) \Sigma
\end{array}
\]

where the vertical arrows are the isomorphisms induced by \( \alpha \). From this diagram we deduce naturally an isomorphism \( D_{X-E_X} \cong D_{Y-E_Y} \) between the kernels of the horizontal arrows.

(ii) From the isomorphism \( D_{X-E_X} \cong D_{Y-E_Y} \) we deduce naturally an embedding \( (\text{Pri}_{X-E_X})_{\mathfrak{p}^n} \hookrightarrow \text{Pri}_{Y-E_Y} \), from which we deduce an embedding \( (\mathcal{O}_{E_X}^\times)_{\mathfrak{p}^n} \hookrightarrow (\mathcal{O}_{E_Y}^\times) \) by Corollary 2.3 and Proposition 3.1(i)(ii). Finally, the desired commutativity of diagram follows easily from the functoriality of Kummer theory. \( \square \)

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

\[
\begin{array}{ccc}
\tilde{X} & \longrightarrow & \tilde{Y} \\
\downarrow & & \downarrow \\
X & \longrightarrow & Y
\end{array}
\]

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings determined by the groups \( \Pi_X, \Pi_Y \).

Proof. (cf. [Mochizuki2], Corollary 2.7, Remark 2.7.1.) Let \( l \neq p \) be a prime number and let \( k_X^l, k_Y^l \) 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 \( K_Xk_X^l, K_Yk_Y^l \), respectively. The exponents of the \( p \)-primary abelian groups \( J_X(k_X^l)\{\Sigma'\}, J_Y(k_Y^l)\{\Sigma'\} \) of \( J_X(k_X^l), J_Y(k_Y^l) \), respectively, are finite (cf. [Rosen], Theorem 11.6). 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 \( \mathcal{O}_{E_X^l}^\times \hookrightarrow (\mathcal{O}_{E_Y^l}^\times)^{p^{n_0}} \), where \( \mathcal{O}_{E_X^l}^\times, \mathcal{O}_{E_Y^l}^\times \) are the multiplicative groups of functions on \( X^l, Y^l \), whose divisor has a 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(i)). (Recall that \( E_X \subset X^{cl}, E_Y \subset Y^{cl} \) are finite by Proposition 1.8(vi).) The above embedding \( \mathcal{O}_{E_X^l}^\times \hookrightarrow (\mathcal{O}_{E_Y^l}^\times)^{p^{n_0}} \) arises, by Proposition 4.4, 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 $O_{E_X}^\times \hookrightarrow (O_{E_Y}^\times)^{p^{-n_0}}$ (i.e., the restriction of $O_{E_X}^\times \hookrightarrow (O_{E_Y}^\times)^{p^{-n_0}}$), hence to an embedding of fields $K_X \hookrightarrow K_Y^{n_0}$. From the construction in the proof of Theorem 3.6, the image of the embedding $O_{E_X}^\times \hookrightarrow (O_{E_Y}^\times)^{p^{-n_0}}$ contains $(O_{E_Y}^\times)^{p^{m_0}} = ((O_{E_Y}^\times)^{p^{-n_0}})^{p^{(n_0+m_0)}}$, where $p^{m_0}$ is the exponent of $J_X(k_X)^\prime\{\Sigma\}$. Thus, the image of the embedding $K_X \hookrightarrow K_Y^{n_0}$ contains $(K_Y^{n_0})^{p^{n_0+m_0}} = K_Y^{m_0}$. From this, we deduce that the embedding $K_X \hookrightarrow K_Y^{n_0}$ is radicial and maps $K_X$ isomorphically onto $K_Y^{s}$ for some integer $n_0 \leq s \leq m_0$. Thus, in particular, the original embedding $O_{E_X}^\times \hookrightarrow (O_{E_Y}^\times)^{p^{-n_0}}$ induces an isomorphism $O_{E_X}^\times \simeq (O_{E_Y}^\times)^{p^s}$.

Now, it follows from the construction in the proof of Theorem 3.6 that the image $\text{Im}(O_{E_X}^\times)$ of $O_{E_X}^\times$ in $(O_{E_Y}^\times)^{p^{-n_0}}$ (i.e., $(O_{E_Y}^\times)^{p^s}$) must be “commensurate” to $O_{E_Y}^\times$ (that is to say, the intersection $\text{Im}(O_{E_X}^\times) \cap O_{E_Y}^\times$ has finite indices both in $\text{Im}(O_{E_X}^\times)$ and in $O_{E_Y}^\times$). This implies $s = 0$. That is to say, the embedding $K_X \hookrightarrow K_Y^{n_0}$ is radicial and 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 $\alpha$ (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:

$$
\begin{array}{ccc}
K_X & \xrightarrow{\tau} & K_Y \\
\uparrow & & \uparrow \\
K_X' & \xrightarrow{\tau'} & K_Y'
\end{array}
$$

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

$$
\begin{array}{ccc}
K_X' & \xrightarrow{\sim} & K_Y' \\
\uparrow & & \uparrow \\
K_X & \xrightarrow{\sim} & K_Y
\end{array}
$$

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 $\Pi_X$ we obtain a natural commutative diagram:

$$
\begin{array}{ccc}
K_X & \xrightarrow{\sim} & K_Y \\
\uparrow & & \uparrow \\
K_X & \xrightarrow{\sim} & K_Y
\end{array}
$$

where $K_X$, $K_Y$ 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 in the
assertion of Theorem 3.7 with 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 \( \alpha \) is Frobenius-preserving. Then the isomorphism \( \alpha \) is totally globally Green-compatible outside exceptional sets. In particular, if \( \Sigma \) is cofinite, then \( \alpha \) is totally globally Green-compatible outside exceptional sets.

Proof. For the first assertion, the proof of [Mochizuki2], Corollary 3.11 (where \( \Sigma^\dagger = \Primes^\dagger \) and \( E_X = E_Y = \emptyset \) are assumed) also works well in this case. (Thus, the main ingredient of the proof is Theorem 2.7.) 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 \( \Sigma_X, \Sigma_Y \) be subsets of \( \Primes \), and assume \( \Sigma_X^\dagger \overset{\text{def}}{=} \Sigma_X - \{ \text{char}(k_X) \} = \Primes - \{ \text{char}(k_X) \} \), \( \Sigma_Y^\dagger \overset{\text{def}}{=} \Sigma_Y - \{ \text{char}(k_Y) \} = \Primes - \{ \text{char}(k_Y) \} \). Write \( \Pi_X, \Pi_Y \) for the geometrically pro-\( \Sigma_X \) étale fundamental group of \( X \), the geometrically pro-\( \Sigma_Y \) étale fundamental group of \( Y \), respectively. Let

\[ \alpha : \Pi_X \sim \Pi_Y \]

be an isomorphism of profinite groups. Then \( \alpha \) arises from a uniquely determined commutative diagram of schemes:

\[
\begin{array}{ccc}
\tilde{X} & \sim & \tilde{Y} \\
\downarrow & & \downarrow \\
X & \sim & Y
\end{array}
\]

in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups \( \Pi_X, \Pi_Y \).

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 \( \Sigma_U, \Sigma_V \) be subsets of \( \Primes \), and assume \( \Sigma_U^\dagger \overset{\text{def}}{=} \Sigma_U - \{ \text{char}(k_U) \} = \Primes - \{ \text{char}(k_U) \} \), \( \Sigma_V^\dagger \overset{\text{def}}{=} \Sigma_V - \{ \text{char}(k_V) \} = \Primes - \{ \text{char}(k_V) \} \). Write \( \Pi_U, \Pi_V \) for the geometrically pro-\( \Sigma_U \) tame fundamental group of \( U \), the geometrically pro-\( \Sigma_V \) tame fundamental group of \( V \), respectively. Let

\[ \alpha : \Pi_U \sim \Pi_V \]

be an isomorphism of profinite groups. Then \( \alpha \) arises from a uniquely determined commutative diagram of schemes:

\[
\begin{array}{ccc}
\tilde{U} & \sim & \tilde{V} \\
\downarrow & & \downarrow \\
U & \sim & V
\end{array}
\]

30
in which the horizontal arrows are isomorphisms and the vertical arrows are the profinite étale coverings corresponding to the groups $\Pi_U, \Pi_V$.

**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 $\alpha$, 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 $S \coloneqq X - U, T \coloneqq Y - V$, respectively. (Observe that such $U' \to U, V' \to V$ are cofinal in the finite étale coverings arising from open subgroups of $\Pi_U, \Pi_V$, respectively.) Thus, the isomorphism $\alpha : \Pi_U \sim \Pi_V$ restricts to an isomorphism $\alpha' : \Pi_{U'} \sim \Pi_{V'}$. By Proposition 1.15(vi), $\alpha'$ induces naturally an isomorphism $\tilde{\alpha}' : \Pi_{X'} \sim \Pi_{Y'}$, which fits into the following commutative diagram:

$$
\begin{array}{ccc}
\Pi_{U'} & \xrightarrow{\alpha'} & \Pi_{V'} \\
\downarrow & & \downarrow \\
\Pi_{X'} & \xrightarrow{\tilde{\alpha}'} & \Pi_{Y'}
\end{array}
$$

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:

$$
\begin{array}{ccc}
\tilde{X}' & \xrightarrow{\sim} & \tilde{Y}' \\
\downarrow & & \downarrow \\
X' & \xrightarrow{\sim} & Y'
\end{array}
$$

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 $\tilde{\alpha}' : \Pi_{X'} \sim \Pi_{Y'}$ is equivariant with respect to $\alpha : \Pi_U \sim \Pi_V$, this last diagram must be also equivariant with respect to $\alpha : \Pi_U \sim \Pi_V$. Thus, by dividing by the actions of $\Pi_U, \Pi_V$, we see that it induces naturally a commutative diagram of schemes:

$$
\begin{array}{ccc}
X' & \xrightarrow{\sim} & Y' \\
\downarrow{\xi} & & \downarrow{\eta} \\
X & \xrightarrow{\sim} & Y
\end{array}
$$

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

$$
\begin{array}{ccc}
U' & \xrightarrow{\sim} & V' \\
\downarrow{\xi} & & \downarrow{\eta} \\
U & \xrightarrow{\sim} & V
\end{array}
$$

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 $G_{K_X} \overset{\text{def}}{=} \text{Gal}(K_{X}^{\text{sep}}/K_X)$ be the absolute Galois group of $K_X$ (where $K_X^{\text{sep}}$ is a separable closure of $K_X$), which sits naturally in the following exact sequence:

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

where $G_{K_X} \overset{\text{def}}{=} \text{Gal}(K_{X}^{\text{sep}}/K_X)$ is the absolute Galois group of the function field $K_X$ of $\overline{X} \overset{\text{def}}{=} X \times_k \overline{k}$, and $G_k \overset{\text{def}}{=} \text{Gal}(\overline{k}/k)$ is the absolute Galois group of $k$ (here, $\overline{k}$ is the algebraic closure of $k$ in $K_X^{\text{sep}}$). Let $G'_{K_X}$ be the maximal prime-to-$p$ quotient of $G_{K_X}$, and let $G'_{K_X} \overset{\text{def}}{=} G_{K_X}/\text{Ker}(G_{K_X} \to G'_{K_X})$ be the corresponding quotient of $G_{K_X}$. We shall refer to $G'_{K_X}$ 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.

**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 $G'_{K_X}, G'_{K_Y}$ be their geometrically prime-to-characteristic quotients. Let

$$\alpha : G'_{K_X} \overset{\sim}{\to} G'_{K_Y}$$

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

$$\begin{array}{ccc}
(K_X)^\sim & \overset{\sim}{\longrightarrow} & (K_Y)^\sim \\
\uparrow & & \uparrow \\
K_X & \overset{\sim}{\longrightarrow} & K_Y
\end{array}$$

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

**Proof.** Following the arguments of [Uchida], Lemma 3 (involving Brauer groups), one can establish a bijection $\phi : X^{\cl} \overset{\sim}{\to} Y^{\cl}$ such that $\alpha(D_x) = D_{\phi(x)}$ holds for each $x \in X^{\cl}$, where $D_x$ stands for the decomposition group of $G'_{K_X}$ at $x$ (which is well-defined up to conjugation). Further, $\alpha(I_x) = I_{\phi(x)}$ also holds for each $x \in X^{\cl}$, 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 $S \subset X^{\cl}$ be a finite subset such that $U \overset{\text{def}}{=} X - S$ is hyperbolic. Let $T \overset{\text{def}}{=} \phi(S)$ and $V \overset{\text{def}}{=} Y - T$. Then $\alpha$ induces naturally an isomorphism $\Pi_U \overset{\sim}{\to} \Pi_V$ between the geometrically

32
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:

$$
\begin{array}{ccc}
\tilde{U} & \rightarrow & \tilde{V} \\
\downarrow & & \downarrow \\
U & \rightarrow & V
\end{array}
$$

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

**Remark 3.12.** In [Stix1], [Stix 2], Stix proved a certain relative version of Grothendieck’s anabelian conjecture for hyperbolic curves over finitely generated fields. 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 3.13.** 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 $\Sigma_X = \mathcal{P} \text{rimes} - \{\text{char}(k)\}$.

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 $(g_X, 1)$:

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

Then $f$ induces a right exact sequence:

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

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

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

Then the sequence

$$1 \rightarrow \Delta_F \rightarrow \Pi_{U_{X \times X}} \rightarrow \Pi_X \rightarrow 1.
$$

is also exact, where $\Pi$ stands for the maximal geometrically pro-$\Sigma_X$ 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:

$$
\begin{array}{ccc}
\Pi_{X-\{x\}} & \rightarrow & \Pi_{X-\{x'\}} \\
\downarrow & & \downarrow \\
\Pi_X & \rightarrow & \Pi_X
\end{array}
$$
Then, by Theorem 3.9 and Corollary 3.10, we obtain the following commutative diagram:

\[
\begin{array}{ccc}
X - \{x\} & \xrightarrow{\sim} & X - \{x'\} \\
\downarrow & & \downarrow \\
X & \xrightarrow{=} & X.
\end{array}
\]

(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 \(\Delta_F \rightarrow \Delta_{U_X X}\)) is valid. (Note that this is a purely topological (or even purely group-theoretical) problem.)

§4. Recovering the Additive Structure.

In this §, we investigate 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 \(X^{\text{cl}}, Y^{\text{cl}}\) be the set of closed points of \(X, Y,\) respectively. Let \(E_X \subset X^{\text{cl}}, E_Y \subset Y^{\text{cl}},\) be finite subsets, and let

\[
\phi : X^{\text{cl}} - E_X \xrightarrow{\sim} Y^{\text{cl}} - E_Y
\]

be a (set-theoretic) bijection. Write

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

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

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

\[
\mathcal{O}^\times_{E_X} = \{f \in K_X^\times \mid \sup(\text{div}(f)) \cap E_X = \emptyset\},
\]

\[
\mathcal{O}^\times_{E_Y} = \{g \in K_Y^\times \mid \sup(\text{div}(g)) \cap E_Y = \emptyset\}.
\]

Let

\[
\iota : \mathcal{O}^\times_{E_X} \hookrightarrow \mathcal{O}^\times_{E_Y}
\]

be an embedding of multiplicative groups.

**Definition 4.1.** The map \(\iota : \mathcal{O}^\times_{E_X} \hookrightarrow \mathcal{O}^\times_{E_Y}\) is called order-preserving, relative to the bijection \(\phi,\) if, for each \(x \in X^{\text{cl}} - E_X,\) we have a commutative diagram:

\[
\begin{array}{ccc}
\mathcal{O}^\times_{E_Y} & \xrightarrow{\text{ord}_\phi(x)} & \mathbb{Z} \\
\uparrow \iota & & \uparrow e_x \\
\mathcal{O}^\times_{E_X} & \xrightarrow{\text{ord}_x} & \mathbb{Z}
\end{array}
\]

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

34
**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 \( \phi \), if, for each \( x \in X^{cl} - E_X \), 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 \( \text{ord}_x(f) = 0 \),

\[
\text{ord}_{\phi(x)}(\iota(f)) = 0, \quad \iota_x(f(x)) = \iota(f(\phi(x)))
\]

hold.

**Remark 4.3.** (i) Assume that the map \( \iota \) is order-preserving relative to \( \phi \). Then \( \iota \) 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 \( 0 \mapsto 0 \). We denote this last embedding also by \( \iota \).

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

\[
\iota_x(f(x)) = \iota(f(\phi(x)))
\]

holds for any \( x \in X^{cl} - E_X \) 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 \( \phi : X^{cl} - E_X \sim Y^{cl} - E_Y \), where \( E_X \subset X^{cl} \), \( E_Y \subset Y^{cl} \) are finite subsets. Assume further that \( X(k_X) \) is an infinite set. Then \( \iota \) 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

\[
\phi : X^{cl} - E_X \sim Y^{cl} - E_Y,
\]

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

**Lemma 4.5 (Recovering the Additive Structure of Constants).** The map \( \iota \) 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 \( x_0 \in X^{cl} - E_X \). 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 \( \text{div}(f)_\infty \) is in the form of \( n \cdot x_0 \) 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 \( \alpha \in k_X^\times - \{-f(x) \mid x \in E_X \} \cap k_X^\times \)). For
α ∈ k^*_X with f + α ∈ O^*_E_X, we shall analyze the divisor of the function ℱ(f + α) − ℱ(f).
(Observe that ℱ(f + α) − ℱ(f) ≠ 0, since ℱ is injective.) We claim: (i) the support of the
divisor div(ℱ(f + α) − ℱ(f)) is contained in {ϕ(x₀)} ∪ E_Y, and (ii) the support of the pole
divisor div(ℱ(f + α) − ℱ(f))_∞ is contained in {ϕ(x₀)}. Indeed, let
x ∈ X^cl − (E_X ∪ {x₀}), and let y = ϕ(x). Then, ord_y(ℱ(f + α)) = e_x ord_x(f) ≥ 0
and ord_y(ℱ(f)) = e_x ord_x(f) ≥ 0. Moreover, ℱ(f + α)(y) ≠ ℱ(f)(y) as follows from
the value-preserving assumption, since (f + α)(x) ≠ f(x). Thus, y does not belong
to the support of div(ℱ(f + α) − ℱ(f)), hence (i) follows. Next, as ℱ(f), ℱ(f + α) ∈ O^*_E_Y,
we have ℱ(f + α) − ℱ(f) ∈ O_E_Y. Thus, ℱ(f + α) − ℱ(f) has no poles in E_Y, and (ii)
follows.

Further, the order of ℱ(f + α) − ℱ(f) at the possible pole ϕ(x₀) is bounded:

\[ \text{ord}_x(ℱ(f + α) − ℱ(f)) ≥ \min(\text{ord}_x(ℱ(f + α)), \text{ord}_x(ℱ(f))) = -ne_x. \]

We deduce from this that there exists an infinite subset A ⊂ k^*_X, such that f + α ∈
O^*_E_X holds for all α ∈ A, and that the divisor div(ℱ(f + α) − ℱ(f)) is constant for
α ∈ A (i.e., div(ℱ(f + α) − ℱ(f)) (α ∈ A) is independent of α).

Let α, β ∈ A with α ≠ β. Thus,

\[ \frac{ℱ(f + β) − ℱ(f)}{ℱ(f + α) − ℱ(f)} = c ∈ k^*_Y. \]

Further, c = \frac{ℱ(β)}{ℱ(α)}, as is easily seen by evaluating the function \frac{ℱ(f + β) − ℱ(f)}{ℱ(f + α) − ℱ(f)} at ϕ(x₁),
where x₁ is a zero of f. (Observe x₁ ∉ E_X.) Thus, we have the equality

\[ ℱ(β)(ℱ(f + α) − ℱ(f)) = ℱ(α)(ℱ(f + β) − ℱ(f)) \]

which is equivalent to

(*) \[ ℱ(f)(ℱ(α) − ℱ(β)) = ℱ(α)ℱ(f + β) − ℱ(β)ℱ(f + α). \]

Let

\[ g \overset{\text{def}}{=} g_{α, β} \overset{\text{def}}{=} \frac{β(f + α)}{(α − β)f} ∈ O^*_E_X. \]

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

\[ g + 1 = \frac{α(f + β)}{(α − β)f} ∈ O^*_E_X. \]

We will show the identity ℱ(g + 1) = ℱ(g) + 1. Indeed,

\[ ℱ(g + 1) − ℱ(g) = \frac{ℱ(α)ℱ(f + β)}{ℱ(α − β)ℱ(f)} − \frac{ℱ(β)ℱ(f + α)}{ℱ(α − β)ℱ(f)} = (*)& ℱ(α) − ℱ(β). \]

Moreover,

\[ \frac{ℱ(α) − ℱ(β)}{ℱ(α − β)} = 1, \]

as follows by evaluating the function ℱ(g + 1) − ℱ(g) at ϕ(x₂), where x₂ is a zero of
g. (Observe x₂ ∉ E_X.) Thus,

\[ ℱ(g + 1) = ℱ(g) + 1. \]
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 $\lambda, \mu$ is 0, this identity clearly holds. So, we may and shall assume $\lambda, \mu \in k_X^n$ and set $\eta \overset{\text{def}}{=} \lambda/\mu \in k_X^n$. First, assume that 

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

and let $x_3 \in X^{cl}$ 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 $\eta$, we shall fix $(f, \beta) \in A$ and make $\alpha \in A - \{\beta\}$ vary in the expression of $g = g_{\alpha, \beta}$. More precisely, take any $\alpha \in (A - \{\beta\}) - \{(\eta f + 1)/\eta f(x) - \beta \mid x \in E_X\}$. Then $g = g_{\alpha, \beta}$ satisfies $\eta \notin k_X - (\{g(x) \mid x \in E_X \} \cap k_X)$. 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.* $\iota$ is multiplicative by definition and additive by Lemma 4.5. □

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

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

$$
\begin{array}{ccc}
k(x) & \xrightarrow{\iota_x} & k(\phi(x)) \\
\uparrow & & \uparrow \\
k_X & \xrightarrow{\iota} & k_Y
\end{array}
$$

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 $k_X \cong k(x)$. Thus, Corollary 4.7 follows from Corollary 4.6. □

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

$$\iota' : Z[O_{E_X}^\times] \to Z[O_{E_Y}^\times].$$

Namely,

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

where $n_i \in Z, f_i \in O_{E_X}^\times$. Further, let $R_X, R_Y$ be the $Z$-subalgebras of $K_X, K_Y$, respectively, generated by $O_{E_X}^\times, O_{E_Y}^\times$, respectively. Observe that $R_X, R_Y$ may be naturally regarded as factor rings of $Z[O_{E_X}^\times], Z[O_{E_Y}^\times]$, respectively.
Lemma 4.8. The ring homomorphism $\iota': \mathbb{Z}[O_{E_X}^\times] \to \mathbb{Z}[O_{E_Y}^\times]$ induces a (unique) ring homomorphism $\iota_R: R_X \to R_Y$. More precisely, the composite of $\iota': \mathbb{Z}[O_{E_X}^\times] \to \mathbb{Z}[O_{E_Y}^\times]$ and the natural surjection $\mathbb{Z}[O_{E_Y}^\times] \to R_Y$ factors through the natural surjection $\mathbb{Z}[O_{E_X}^\times] \to R_X$.

Proof. Take any element

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

where $n_i \in \mathbb{Z}$, $f_i \in O_{E_X}^\times$, 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

$$\sum_i n_i f_i = 0.$$

Let $S_i \subset X^{\text{cl}}$ denote the (finite) set of poles of $f_i$ and consider a point $x \in X(k_X) - (E_X \cup \cup_i S_i)$. 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

$$\sum_i k(\phi(x)) n_i f_i(\phi(x)) = 0,$$

or, equivalently, the equality

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

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

Lemma 4.9. We have $R_X = O_{E_X}$ and $R_Y = O_{E_Y}$.

Proof. It suffices to prove $R_X = O_{E_X}$. It is clear from the definitions that $R_X \subset O_{E_X}$. We will show the other inclusion $O_{E_X} \subset R_X$. Let $f \in O_{E_X}$, then $(f(x))_{x \in E_X} \in \oplus_{x \in E_X} k(x)$. Fix $\alpha \in k_X^\times - \{1\}$. For each $x \in E_X$, set

$$\epsilon(x) = \begin{cases} f(x) - 1, & \text{if } f(x) \neq 1, \\ 1 - \alpha, & \text{if } f(x) = 1. \end{cases}$$

Thus, we have

$$(\epsilon(x))_{x \in E_X} \in \oplus_{x \in E_X} k(x)^\times.$$

Further, set

$$(\delta(x))_{x \in E_X} \overset{\text{def}}{=} (f(x))_{x \in E_X} - (\epsilon(x))_{x \in E_X},$$

then we have

$$\delta(x) = \begin{cases} 1, & \text{if } f(x) \neq 1, \\ \alpha, & \text{if } f(x) = 1. \end{cases}$$

Thus, in particular, we have

$$(\delta(x))_{x \in E_X} \in \oplus_{x \in E_X} k(x)^\times.$$
Since the evaluation map $\mathcal{O}_{E_X} \to \bigoplus_{x \in E_X} k(x)$ is surjective, we can find a function $g \in \mathcal{O}_{E_X}$, such that $(g(x))_{x \in E_X} = (\epsilon(x))_{x \in E_X}$. Set $h \overset{\text{def}}{=} f - g$. Then we have $(h(x))_{x \in E_X} = (\delta(x))_{x \in E_X}$. Since $g, h \in \mathcal{O}_{E_X}^\times$, the equality $f = g + h$ shows that $f \in R_X$. □

**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 $\iota_R(f) = 0$. As in the proof of 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 $\iota$ 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 $X^{\text{cl}}$ (or, more precisely, all points of $X^{\text{cl}} - E_X$). This is a 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.

References.

[Boxall] Boxall, J., Autour d’un problème de Coleman, C. R. Acad. Sci. Paris 315 (1992), Sér. I, 1063–1066.

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

[Grothendieck] Grothendieck, A., Brief an G. Faltings. (German) [Letter to G. Faltings] With an English translation on pp. 285–293. London Math. Soc. Lecture Note Ser., 242, Geometric Galois actions, 1, 49–58, Cambridge Univ. Press, Cambridge, 1997.

[Mochizuki1] Mochizuki, S., The local pro-$p$ anabelian geometry of curves, Inventiones Mathematicae 138 (1999), 319–423.

[Mochizuki2] —, Absolute anabelian cuspidalizations of proper hyperbolic curves, preprint RIMS-1490 (2005), revised version (2007), available at [http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html](http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html), to appear in Journal of Mathematics of Kyoto University.

[Nakamura1] Nakamura, H., 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, International Journal of Mathematics, 4 (1993), 421–438.

[Nakamura3] —, Galois rigidity of pure sphere braid groups and profinite calculus, J. Math. Sci. Univ. Tokyo, 1 (1994), 71–136.
[NT] Nakamura, H. and Tsunogai, H., Some finiteness theorems on Galois centralizers in pro-$l$ mapping class groups, J. Reine Angew. Math., 441 (1993), 115–144.

[Rosen] Rosen, M., Number Theory in Function Fields, Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.

[Stix1] Stix, J., 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. Dissertation, Rheinische Friedrich-Wilhelms-Universität Bonn, Bonn, 2002. Bonner Mathematische Schriften, 354. Universität Bonn, Mathematisches Institut, Bonn, 2002.

[Tamagawa1] Tamagawa, A., The Grothendieck conjecture for affine curves, Compositio Math. 109 (1997), 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, Cambridge Univ. Press, Cambridge, 2003, 47–105.

[Tamagawa3] —, Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups, J. Algebraic Geom. 13 (2004), 675–724.

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

Mohamed Saïdi
School of Engineering, Computer Science, and Mathematics
University of Exeter
Harrison Building
North Park Road
EXETER EX4 4QF
United Kingdom
M.Saidi@exeter.ac.uk

Akio Tamagawa
Research Institute for Mathematical Sciences
Kyoto University
KYOTO 606-8502
Japan
tamagawa@kurims.kyoto-u.ac.jp