

RIMS-1874

**Algorithmic approach to Uchida's theorem for
one-dimensional function fields over finite fields**

By

Koichiro SAWADA

April 2017



京都大学 数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

ALGORITHMIC APPROACH TO UCHIDA'S THEOREM FOR ONE-DIMENSIONAL FUNCTION FIELDS OVER FINITE FIELDS

KOICHIRO SAWADA

ABSTRACT. Uchida proved that the isomorphism class of a one-dimensional function field over a finite field is completely determined by (a suitable quotient of) its absolute Galois group. But his proof of this theorem essentially gives a group-theoretic reconstruction algorithm for one-dimensional function fields over finite fields. In this article, we discuss the group-theoretic reconstruction algorithm.

1. INTRODUCTION

In [10], Uchida proved the following theorem:

Theorem A (Uchida). *For $i \in \{1, 2\}$, let K_i be a one-dimensional function field over a finite field and Ω_i a solvably closed Galois extension of K_i (i.e., Galois extension of K_i which has no nontrivial abelian extension). For $i \in \{1, 2\}$, write $G_i := \text{Gal}(\Omega_i/K_i)$. Moreover, write $\text{Isom}(\Omega_2/K_2, \Omega_1/K_1)$ for the set of isomorphisms $\Omega_2 \xrightarrow{\sim} \Omega_1$ of fields such that the image of K_2 coincides with K_1 and $\text{Isom}(G_1, G_2)$ for the set of isomorphisms $G_1 \xrightarrow{\sim} G_2$ of profinite groups. Then the natural map $\text{Isom}(\Omega_2/K_2, \Omega_1/K_1) \rightarrow \text{Isom}(G_1, G_2)$ is bijective.*

In particular, the isomorphism class of a one-dimensional function field over a finite field is completely determined by (a suitable quotient of) its absolute Galois group. We may consider that the assertion of Theorem A gives a “bi-anabelian” reconstruction (in the sense of [4]) of one-dimensional function fields over finite fields.

But in fact, the proof of Theorem A in [10] essentially gives a “mono-anabelian reconstruction” (in the sense of [4]). In other words, the argument in [10] implies that a one-dimensional function field over a finite field can be reconstructed from (a suitable quotient of) its absolute Galois group by a functorial group-theoretic reconstruction algorithm.

We shall say that a profinite group G is of *PGF-type* if there exist a one-dimensional function field K over a finite field and a solvably closed Galois extension Ω of K such that G is isomorphic to the Galois group $\text{Gal}(\Omega/K)$ (cf. Definition 3.1(iv)). Let us express more precisely the statement of the “mono-anabelian” version of Theorem A:

Theorem B. *There exists a functorial group-theoretic algorithm $G \mapsto K(G)$ for constructing a field $K(G)$ from a profinite group G of PGF-type such that the following hold: an isomorphism $\alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G$ (where K is a one-dimensional*

2010 *Mathematics Subject Classification.* 11R32.

Key words and phrases. Uchida's theorem, mono-anabelian reconstruction, one-dimensional function fields over finite fields.

function field over a finite field and Ω is a solvably closed Galois extension of K) induces a natural isomorphism $K \xrightarrow{\sim} K(G)$ of fields.

The purpose of this article is to explain in detail this “mono-anabelian” reconstruction algorithm.

Remark 1. Uchida also proved for the “bi-anabelian” results for number fields (cf. [9], [11]). However, in this case, the proofs of [9], [11] do not give a “mono-anabelian” reconstruction. A “mono-anabelian” reconstruction algorithm of number fields is given in [2].

Remark 2. Some notations and discussions in this article are based on those of [2].

2. LOCAL THEORY

In this section, we discuss generalities of the absolute Galois group of positive characteristic local fields, and review mono-anabelian reconstructions of various objects.

Definition 2.1.

- (i) We shall refer to a field which is isomorphic to a finite extension of $\mathbb{F}_p((t))$ for some prime number p as a *PLF* (Positive characteristic Local Field).
- (ii) Let k be a PLF and k^{sep} a separable closure of k . Then we shall write
 - $p_k := \text{char}(k) (> 0)$ for the characteristic of k ,
 - $\mathcal{O}_k \subset k$ for the ring of integers of k ,
 - $\mathcal{O}_k^\times := \mathcal{O}_k \setminus \{0\}$ for the multiplicative monoid of nonzero integers of k ,
 - $\mathfrak{m}_k \subset \mathcal{O}_k$ for the maximal ideal of \mathcal{O}_k ,
 - $U_k^{(1)} := 1 + \mathfrak{m}_k \subset \mathcal{O}_k^\times$ for the multiplicative group of principal units of k ,
 - $\kappa_k := \mathcal{O}_k/\mathfrak{m}_k$ for the residue field of \mathcal{O}_k ,
 - $\bar{\kappa}_k$ for the residue field of (the ring of integers of) k^{sep} (note that $\bar{\kappa}_k$ is an algebraic closure of κ_k),
 - $f_k := [\kappa_k : \mathbb{F}_{p_k}]$ for the extension degree of κ_k over the prime field contained in κ_k ,
 - $G_k := \text{Gal}(k^{\text{sep}}/k)$ for the absolute Galois group of k ,
 - $I_k \subset G_k$ for the inertia subgroup of G_k ,
 - $P_k \subset I_k$ for the wild inertia subgroup of G_k , and
 - $\text{Frob}_{\kappa_k} \in \text{Gal}(\bar{\kappa}_k/\kappa_k)$ for the ($\sharp\kappa_k$ -th power) Frobenius element of $\text{Gal}(\bar{\kappa}_k/\kappa_k)$.
- (iii) Let G be a profinite group. Then we shall refer to a collection of data

$$(k, k^{\text{sep}}, \alpha : G_k \xrightarrow{\sim} G)$$

consisting of a PLF k , a separable closure k^{sep} of k , and an isomorphism of profinite groups $\alpha : G_k \xrightarrow{\sim} G$ as a *PLF-envelope* for G . We shall say that the profinite group G is of *PLF-type* if there exists a PLF-envelope for G .

Remark 3. An open subgroup of a profinite group of PLF-type is of PLF-type.

Lemma 2.2 (Local class field theory). *Let k be a PLF. Let us write $(k^\times)^\wedge := \varprojlim_{n \geq 1} k^\times / (k^\times)^n$. Then there exists a commutative diagram*

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mathcal{O}_k^\times & \longrightarrow & (k^\times)^\wedge & \longrightarrow & \hat{\mathbb{Z}} \longrightarrow 1 \\
& & \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\
1 & \longrightarrow & \text{Im}(I_k \hookrightarrow G_k \twoheadrightarrow G_k^{\text{ab}}) & \longrightarrow & G_k^{\text{ab}} & \longrightarrow & G_k/I_k \longrightarrow 1,
\end{array}$$

where the horizontal sequences are exact, the middle vertical arrow $(k^\times)^\wedge \xrightarrow{\wr} G_k^{\text{ab}}$ is the homomorphism induced by the reciprocity homomorphism $k^\times \rightarrow G_k^{\text{ab}}$ in local class field theory, and the right-hand vertical arrow maps $1 \in \mathbb{Z}$ to $\text{Frob}_{\kappa_k} \in \text{Gal}(\bar{\kappa}_k/\kappa_k) \xrightarrow{\wr} G_k/I_k$.

Lemma 2.3. *Let k be a PLF and $\pi \in \mathcal{O}_k$ a prime element of \mathcal{O}_k . Then it holds that $k^\times \cong \langle \pi \rangle \times \mathcal{O}_k^\times \cong \langle \pi \rangle \times (k^\times)_{\text{tor}} \times U_k^{(1)}$.*

Proof. Well-known (cf. e.g., [7] Chapter II, Proposition (5.3)). \square

Lemma 2.4. *Let k be a PLF. Then the following hold:*

- (i) p_k is the unique prime number l such that $l \mid \#(G_k^{\text{ab}})_{\text{tor}} + 1$.
- (ii) It holds that $f_k = \log_{p_k}(\#(G_k^{\text{ab}})_{\text{tor}} + 1)$.
- (iii) It holds that $I_k = \text{Gal}(k^{\text{sep}}/k^{\text{ur}}) = \bigcap_{k'} \text{Gal}(k^{\text{sep}}/k')$, where $k' \subset k^{\text{sep}}$ runs over all finite unramified extensions of k contained in k^{sep} .
- (iv) Let $k' \subset k^{\text{sep}}$ be a finite extension of k contained in k^{sep} . Then k' is unramified over k if and only if it holds that $[\text{Gal}(k^{\text{sep}}/k) : \text{Gal}(k^{\text{sep}}/k')] = f_{k'}/f_k$.
- (v) P_k is the unique Sylow pro- p_k -subgroup of I_k .
- (vi) $\text{Frob}_{\kappa_k} \in \text{Gal}(\bar{\kappa}_k/\kappa_k) \xrightarrow{\wr} G_k/I_k$ is the unique element of G_k/I_k which acts by conjugation on I_k/P_k by multiplication by $p_k^{f_k}$.
- (vii) It holds that $\text{Im}(\mathcal{O}_k^\times \hookrightarrow k^\times \hookrightarrow G_k^{\text{ab}}) = \text{Im}(I_k \twoheadrightarrow G_k^{\text{ab}})$.
- (viii) $\text{Im}(k^\times \hookrightarrow G_k^{\text{ab}})$ coincides with a subgroup of G_k^{ab} generated by $\text{Im}(\mathcal{O}_k^\times \hookrightarrow G_k^{\text{ab}})$ and (a lifting of) Frob_{κ_k} (in G_k^{ab}). In other words, $\text{Im}(k^\times \hookrightarrow G_k^{\text{ab}}) = G_k^{\text{ab}} \times_{G_k/I_k} \text{Frob}_{\kappa_k}^{\mathbb{Z}}$, where we write $\text{Frob}_{\kappa_k}^{\mathbb{Z}}$ for the discrete subgroup of G_k/I_k generated by Frob_{κ_k} .
- (ix) $\text{Im}(\mathcal{O}_k^\times \hookrightarrow k^\times \hookrightarrow G_k^{\text{ab}})$ coincides with a submonoid of G_k^{ab} generated by $\text{Im}(\mathcal{O}_k^\times \hookrightarrow G_k^{\text{ab}})$ and (a lifting of) Frob_{κ_k} (in G_k^{ab}). In other words, $\text{Im}(\mathcal{O}_k^\times \hookrightarrow k^\times \hookrightarrow G_k^{\text{ab}}) = G_k^{\text{ab}} \times_{G_k/I_k} \text{Frob}_{\kappa_k}^{\mathbb{Z}_{\geq 0}}$, where we write $\text{Frob}_{\kappa_k}^{\mathbb{Z}_{\geq 0}}$ for the discrete submonoid of G_k/I_k generated by Frob_{κ_k} .
- (x) $U_k^{(1)}$ is the unique Sylow pro- p_k -subgroup of \mathcal{O}_k^\times .

Proof. Assertions (i), (ii) follow from Lemmas 2.2, 2.3. Assertions (iii)-(v), (vii)-(x) are immediate. Assertion (vi) follows from [8] Proposition (7.5.2). \square

Definition 2.5. Let G be a profinite group of PLF-type.

- (i) It follows from Lemma 2.4(i) that there exists a unique prime number l such that $l \mid \#(G^{\text{ab}})_{\text{tor}} + 1$. Write $p(G)$ for this prime number.
- (ii) Write $f(G) := \log_{p(G)}(\#(G^{\text{ab}})_{\text{tor}} + 1)$.

- (iii) Write $I(G) := \bigcap_{G'} G'$, where G' runs over all open subgroups of G such that $[G : G'] = f(G')/f(G)$ (cf. Remark 3).
- (iv) It follows from Lemma 2.4(v), together with Theorem 2.6(i), (ii) below, that there exists a unique Sylow pro- $p(G)$ -subgroup of $I(G)$. Write $P(G)$ for this subgroup of $I(G)$.
- (v) It follows from Lemma 2.4(vi), together with Theorem 2.6(i)-(iii) below, that there exists a unique element of $G/I(G)$ which acts by conjugation on $I(G)/P(G)$ by multiplication by $p(G)^{f(G)}$. Write $\text{Frob}(G) \in G/I(G)$ for this element of $G/I(G)$.
- (vi) Write $\mathcal{O}^\times(G) := \text{Im}(I(G) \rightarrow G^{\text{ab}})$.
- (vii) Write $k^\times(G) := G^{\text{ab}} \times_{G/I(G)} \text{Frob}(G)^\mathbb{Z} \subset G^{\text{ab}}$, where we write $\text{Frob}(G)^\mathbb{Z}$ for the discrete subgroup of $G/I(G)$ generated by $\text{Frob}(G)$.
- (viii) Write $\mathcal{O}^\geq(G) := G^{\text{ab}} \times_{G/I(G)} \text{Frob}(G)^{\mathbb{Z}_{\geq 0}} \subset G^{\text{ab}}$, where we write $\text{Frob}(G)^{\mathbb{Z}_{\geq 0}}$ for the discrete submonoid of $G/I(G)$ generated by $\text{Frob}(G)$.
- (ix) Since $\mathcal{O}^\times(G) \subset G^{\text{ab}}$ is abelian, there exists a unique Sylow pro- $p(G)$ -subgroup of $\mathcal{O}^\times(G)$. Write $U^{(1)}(G)$ for this subgroup of $\mathcal{O}^\times(G)$.

Theorem 2.6. *Let G be a profinite group of PLF-type and $(k, k^{\text{sep}}, \alpha : G_k \xrightarrow{\sim} G)$ a PLF-envelope for G . Then the following hold:*

- (i) *It holds that $p_k = p(G)$, $f_k = f(G)$.*
- (ii) *It holds that $\alpha(I_k) = I(G)$.*
- (iii) *It holds that $\alpha(P_k) = P(G)$.*
- (iv) *The image of $\text{Frob}_{\kappa_k} \in G_k/I_k$ by the isomorphism $G_k/I_k \xrightarrow{\sim} G/I(G)$ determined by α (cf. (ii)) coincides with $\text{Frob}(G) \in G/I(G)$.*
- (v) *The reciprocity homomorphism $k^\times \rightarrow G_k^{\text{ab}}$ and the isomorphism α determine an isomorphism $k^\times \xrightarrow{\sim} k^\times(G)$. Moreover, the image of \mathcal{O}_k^\times (resp. $\mathcal{O}_k^\times, U_k^{(1)}$) by the isomorphism $k^\times \xrightarrow{\sim} k^\times(G)$ coincides with $\mathcal{O}^\geq(G)$ (resp. $\mathcal{O}^\times(G), U^{(1)}(G)$).*

Proof. These assertions follow from Lemma 2.4. □

Theorem 2.7. *Let G be a profinite group of PLF-type, $(k, k^{\text{sep}}, \alpha : G_k \xrightarrow{\sim} G)$ a PLF-envelope for G , and $H \subset G$ an open subgroup of G . Write k' for the finite extension of k contained in k^{sep} which corresponds to the open subgroup $\alpha^{-1}(H) \subset G_k$ of G_k . Then we obtain a commutative diagram*

$$\begin{array}{ccc}
 k^\times & \xrightarrow{\sim} & k^\times(G) \\
 \downarrow & & \downarrow \\
 (k')^\times & \xrightarrow{\sim} & k^\times(H),
 \end{array}$$

where the horizontal arrows are the isomorphism appearing in Theorem 2.6(v), and the right-hand vertical arrow is the homomorphism induced by the transfer homomorphism $G^{\text{ab}} \rightarrow H^{\text{ab}}$.

Proof. This follows from Theorem 2.6(v), together with [12] Chapter XII, Theorem 6. □

3. MULTIPLICATIVE STRUCTURE OF ONE-DIMENSIONAL FUNCTION FIELDS OVER FINITE FIELDS

In this section, we reconstruct the multiplicative structure of one-dimensional function fields over finite fields.

Definition 3.1.

- (i) We shall refer to a field which is isomorphic to a one-dimensional function field over a finite field as a *PGF* (Positive characteristic Global Field).
- (ii) Let K be an algebraic extension (not necessarily finite) of a PGF. Then we shall write \mathcal{V}_K for the set of all places of K .
- (iii) Let K be a PGF and $v \in \mathcal{V}_K$ a place of K . Then we shall write
 - K_v for the PLF obtained by forming the completion of K at v ,
 - $\text{ord}_v : K^\times \rightarrow \mathbb{Z}$ for the uniquely determined surjective valuation associated to v ,
 - $\mathcal{O}_v := \{a \in K \mid \text{ord}_v(a) \geq 0\} \subset K$ for the discrete valuation ring at v ,
 - $\mathcal{O}_v^\times := \mathcal{O}_v \setminus \{0\}$ for the multiplicative monoid of nonzero elements of \mathcal{O}_v ,
 - $\mathfrak{m}_v \subset \mathcal{O}_v$ for the maximal ideal of \mathcal{O}_v ,
 - $U_v^{(1)} := 1 + \mathfrak{m}_v \subset \mathcal{O}_v^\times$, and
 - $J_K := \varinjlim_S (\prod_{v \in S} K_v^\times) \times (\prod_{v \in \mathcal{V}_K \setminus S} \mathcal{O}_{K_v}^\times)$ for the idèle group of K , where S runs over all finite subsets of \mathcal{V}_K .
- (iv) Let G be a profinite group. Then we shall refer to a collection of data

$$(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$$

consisting of a PGF K , a solvably closed Galois extension Ω of K , and an isomorphism of profinite groups $\alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G$ as a *PGF-envelope* for G . We shall say that the profinite group G is of *PGF-type* if there exists a PGF-envelope for G .

Remark 4. An open subgroup of a profinite group of PGF-type is of PGF-type.

Lemma 3.2 (PGF-analogue of [3] Proposition 2.1(i)). *Let K be a PGF, K^{sep} a separable closure of K , Ω a solvably closed Galois extension of K contained in K^{sep} , and A a continuous discrete torsion $\text{Gal}(\Omega/K)$ -module. Then, for each integer $i \geq 0$, the natural surjection $G_K = \text{Gal}(K^{\text{sep}}/K) \twoheadrightarrow \text{Gal}(\Omega/K)$ induces an isomorphism*

$$H^i(\text{Gal}(\Omega/K), A) \xrightarrow{\sim} H^i(G_K, A).$$

$$\text{In particular, } \text{cd}_p(\text{Gal}(\Omega/K)) = \begin{cases} 2 & (p \neq \text{char}(K)) \\ 1 & (p = \text{char}(K)). \end{cases}$$

Proof. It is well-known that $\text{cd}_p(G_K) = \begin{cases} 2 & (p \neq \text{char}(K)) \\ 1 & (p = \text{char}(K)) \end{cases}$ (cf. e.g., [8] Proposition (6.5.10), Theorem (7.1.8)(i), Theorem (8.3.17)). Thus, the second assertion follows from the first assertion. We verify the first assertion. Write $J := \ker(G_K \twoheadrightarrow \text{Gal}(\Omega/K))$. It suffices to prove that $H^i(J, A) = 0$ for $i \geq 1$. We may assume that A is finite and p -primary for some prime number p . Since $\text{cd}_p(J) \leq \text{cd}_p(G_K)$, we may assume that $1 \leq i \leq \text{cd}_p(G_K)$. If $i = 2$ (hence $p \neq \text{char}(K)$), then it follows from an argument similar to the argument in [3] Proposition 2.1(i), that $H^2(J, A) = 0$. Moreover, if $i = 1$, then, since Ω is solvably closed, we obtain

$H^1(J, A) = \text{Hom}_{\text{cts}}(J, A) = \{0\}$, where we write $\text{Hom}_{\text{cts}}(J, A)$ for the set of continuous homomorphisms from J to A . This completes the proof of Lemma 3.2. \square

Lemma 3.3 (PGF-analogue of [3] Proposition 2.3(iii)-(v)). *Let K be a PGF, K^{sep} a separable closure of K , Ω a solvably closed Galois extension of K contained in K^{sep} , and $v, w \in \mathcal{V}_\Omega$ places of Ω . Suppose that $v \neq w$. Write $D_v, D_w \subset \text{Gal}(\Omega/K)$ for the decomposition subgroups associated to v, w , respectively. Then the following hold:*

- (i) *The natural surjection $\text{Gal}(K^{\text{sep}}/K) \twoheadrightarrow \text{Gal}(\Omega/K)$ induces an isomorphism of D_v with the decomposition subgroup associated to a lifting of v in $\mathcal{V}_{K^{\text{sep}}}$.*
- (ii) *It holds that $D_v \cap D_w = \{1\}$.*
- (iii) *D_v is its own commensurator in $\text{Gal}(\Omega/K)$, i.e., for $g \in \text{Gal}(\Omega/K)$, g lies in D_v if and only if $D_v \cap gD_vg^{-1}$ is of finite index in both D_v and gD_vg^{-1} .*

Proof. Assertion (i) follows from an argument similar to [3] Proposition 2.3(iii). Assertion (iii) follows from assertion (ii). We verify assertion (ii). Since $v \neq w$, there exists a finite extension L of K contained in Ω such that v and w are not equivalent over L . Then it follows from an argument similar to [3] Proposition 2.3(iv) that $(D_v \cap \text{Gal}(\Omega/L)) \cap (D_w \cap \text{Gal}(\Omega/L)) = \{1\}$, which implies that $D_v \cap D_w$ is finite. Since $\text{Gal}(\Omega/K)$ is of finite cohomological dimension (cf. Lemma 3.2), hence torsion-free, we conclude that $D_v \cap D_w = \{1\}$. This completes the proof of assertion (ii), hence also of Lemma 3.3. \square

Lemma 3.4. *Let K be a PGF, Ω a solvably closed Galois extension of K , $H \subset \text{Gal}(\Omega/K)$ a closed subgroup of $\text{Gal}(\Omega/K)$, and l a prime number different from $\text{char}(K)$. Then the following hold:*

- (i) *The natural map $\mathcal{V}_\Omega \rightarrow \mathcal{V}_K$ and the natural action of $\text{Gal}(\Omega/K)$ on \mathcal{V}_Ω determines a bijection $\mathcal{V}_\Omega / \text{Gal}(\Omega/K) \xrightarrow{\sim} \mathcal{V}_K$.*
- (ii) *Consider the following conditions:*
 - (1) *H is an open subgroup of the decomposition subgroup of $\text{Gal}(\Omega/K)$ associated to some $v \in \mathcal{V}_\Omega$.*
 - (2) *H is of PLF-type.*
 - (3) *There exists an open subgroup V of H such that, for any open subgroup $U \subset V$ of V , it holds that $\dim_{\mathbb{F}_l} H^2(U, \mathbb{F}_l) = 1$, where the action of U on \mathbb{F}_l is trivial.*
 - (4) *H is a closed subgroup of the decomposition subgroup of $\text{Gal}(\Omega/K)$ associated to some $v \in \mathcal{V}_\Omega$.*

Then we have implications (1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4).

Proof. Assertion (i) is immediate. We verify assertion (ii). The implication (1) \Rightarrow (2) follows from Lemma 3.3(i), together with Remark 3. Next, we verify the implication (2) \Rightarrow (3). Suppose that condition (2) is satisfied. Let $(k, k^{\text{sep}}, \alpha : G_k \xrightarrow{\sim} H)$ be a PLF-envelope for H . Write $V := \text{Gal}(k^{\text{sep}}/k(\mu_l)) \subset H$. Then V is an open subgroup of H , and, moreover, for any open subgroup $U \subset V$ of V , it holds that $H^2(U, \mathbb{F}_l) \cong H^2(U, \mu_l)$. On the other hand, it follows from Hilbert's theorem 90, together with the well-known fact that $\text{cd}_l U = 2$ (cf. e.g., [8] Theorem (7.1.8)(i)), that the exact sequence

$$1 \rightarrow \mu_l \rightarrow (k^{\text{sep}})^\times \xrightarrow{l} (k^{\text{sep}})^\times \rightarrow 1$$

induces an exact sequence

$$0 \rightarrow H^2(U, \mu_l) \rightarrow H^2(U, (k^{\text{sep}})^\times) \xrightarrow{l} H^2(U, (k^{\text{sep}})^\times) \rightarrow 0.$$

Since (it is well-known that) $H^2(U, (k^{\text{sep}})^\times) \cong \text{Br}((k^{\text{sep}})^U)$ is isomorphic to \mathbb{Q}/\mathbb{Z} , it holds that $\dim_{\mathbb{F}_l} H^2(U, \mu_l) = 1$. This completes the proof of the implication (2) \Rightarrow (3).

Finally, we verify the implication (3) \Rightarrow (4). Suppose that condition (3) is satisfied. Let $v \in \mathcal{V}_\Omega$. By abuse of notation, let us write K_v for the “ K_v ”, where we take “ $v \in \mathcal{V}_K$ ” to be the image of $v \in \mathcal{V}_\Omega$ by the natural surjection $\mathcal{V}_\Omega \twoheadrightarrow \mathcal{V}_K$. Then we can consider Ω as a subfield of a separable closure of K_v . For any intermediate field L of K and Ω , write $L_v := L \cdot K_v$. Let V be as in condition (3) and F a finite extension of $(\Omega^V)(\mu_l)$ contained in Ω . Write $U := \text{Gal}(\Omega/F) \subset V$. Then it follows from condition (3) that $\dim_{\mathbb{F}_l} H^2(U, \mathbb{F}_l) = 1$. Moreover, it holds that $H^2(U, \mathbb{F}_l) \cong H^2(U, \mu_l)$. Thus, it follows from Hilbert’s theorem 90, together with Lemma 3.2, that the exact sequence

$$1 \rightarrow \mu_l \rightarrow \Omega^\times \xrightarrow{l} \Omega^\times \rightarrow 1,$$

induces an exact sequence

$$0 \rightarrow H^2(U, \mu_l) \rightarrow H^2(U, \Omega^\times) \xrightarrow{l} H^2(U, \Omega^\times) \rightarrow 0,$$

which implies that the l -primary part $H^2(U, \Omega^\times)(l)$ of $H^2(U, \Omega^\times)$ is of corank 1. It follows from [10] Lemma 1 that there exists a unique $v(F) \in \mathcal{V}_F$ such that, for any extension $v \in \mathcal{V}_\Omega$ of $v(F)$ in Ω , it holds that $H^2(\text{Gal}(\Omega_v/F_v), \Omega_v^\times)(l) \neq \{0\}$. Moreover, it follows from the uniqueness of $v(F')$ for any finite extension of F contained in Ω , that $v(F)$ has a unique extension in Ω .

Now let us write $E := \Omega^H \subset F$ and $v(E) \in \mathcal{V}_E$ for the restriction of $v(F) \in \mathcal{V}_F$ to E . Then, since F is finite over E , it follows from [10] Lemma 1, together with the (already verified) fact that $H^2(U, \Omega^\times)(l)$ is of corank 1, that $v(F)$ is the unique extension of $v(E)$. Thus, we conclude that $v(E)$ has a unique extension $v \in \mathcal{V}_\Omega$ in Ω , which implies that H is contained in the decomposition subgroup of $\text{Gal}(\Omega/K)$ associated to $v \in \mathcal{V}_\Omega$. This completes the proof of the implication (3) \Rightarrow (4), hence also of Lemma 3.4. \square

Definition 3.5. Let G be a profinite group of PGF-type.

- (i) Write $\overline{\mathcal{V}}(G)$ for the set of maximal elements of the set of all closed subgroups $H \subset G$ satisfying the following condition:

there exist a prime number l and an open subgroup V of H such that, for any open subgroup $U \subset V$ of V , it holds that $\dim_{\mathbb{F}_l} H^2(U, \mathbb{F}_l) = 1$, where the action of U on \mathbb{F}_l is trivial.

Let us define the action of G on $\overline{\mathcal{V}}(G)$ by conjugation.

- (ii) Write $\mathcal{V}(G) := \overline{\mathcal{V}}(G)/G$.

Theorem 3.6. Let G be a profinite group of PGF-type and $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G .

- (i) The isomorphism α determines a bijection $\mathcal{V}_\Omega \xrightarrow{\sim} \overline{\mathcal{V}}(G)$, which is compatible with the actions of $\text{Gal}(\Omega/K)$ and G . In particular, any $D \in \overline{\mathcal{V}}(G)$ is of PLF-type. Moreover, the above bijection induces a bijection $\mathcal{V}_K \xrightarrow{\sim} \mathcal{V}(G)$.

- (ii) Let $H \subset G$ be an open subgroup of G . Write L for the finite extension of K contained in Ω which corresponds to the open subgroup $\alpha^{-1}(H) \subset \text{Gal}(\Omega/K)$ of $\text{Gal}(\Omega/K)$. Then we obtain a commutative diagram

$$\begin{array}{ccc} \mathcal{V}_\Omega & \xrightarrow{\sim} & \overline{\mathcal{V}}(G) \\ \parallel & & \downarrow \wr \\ \mathcal{V}_\Omega & \xrightarrow{\sim} & \overline{\mathcal{V}}(H), \end{array}$$

where the horizontal arrows are the bijection appearing in (i), and the right-hand vertical arrow is the bijection which maps $D \in \overline{\mathcal{V}}(G)$ to $D \cap H \in \overline{\mathcal{V}}(H)$. Moreover, the inverse map of the right-hand vertical arrow of this diagram determines a commutative diagram

$$\begin{array}{ccc} \mathcal{V}_L & \xrightarrow{\sim} & \mathcal{V}(H) \\ \downarrow & & \downarrow \\ \mathcal{V}_K & \xrightarrow{\sim} & \mathcal{V}(G). \end{array}$$

(Note that it follows from Lemma 3.3(iii) that the inverse map $\overline{\mathcal{V}}(H) \xrightarrow{\sim} \overline{\mathcal{V}}(G)$ maps $D \in \overline{\mathcal{V}}(H)$ to the commensurator of D in G .)

Proof. Assertion (i) follows from Lemma 3.4, together with Lemma 3.2 and Lemma 3.3(ii). Assertion (ii) follows from assertion (i). \square

Remark 5. The reconstruction of \mathcal{V}_Ω is essentially due to J. Neukirch [5], [6].

Lemma 3.7 (Global class field theory). *Let K be a PGF and Ω a solvably closed Galois extension of K . Let us consider the homomorphism $J_K \rightarrow \text{Gal}(\Omega/K)^{\text{ab}}$ determined by the reciprocity homomorphisms $K_v^\times \rightarrow D_v^{\text{ab}}$, where $D_v \subset \text{Gal}(\Omega/K)$ is the decomposition subgroup associated to a lifting of $v \in \mathcal{V}_K$ in \mathcal{V}_Ω (note that, since D_v is well-defined up to conjugation, $J_K \rightarrow \text{Gal}(\Omega/K)^{\text{ab}}$ is well-defined). Then it holds that $K^\times = \ker(J_K \rightarrow \text{Gal}(\Omega/K)^{\text{ab}})$.*

Lemma 3.8. *Let G be a profinite group of PGF-type and $v \in \mathcal{V}(G) = \overline{\mathcal{V}}(G)/G$.*

- (i) *There exists a unique submodule M of $\prod_{D \in v} k^\times(D)$ (cf. Theorem 3.6(i)) which satisfies the following conditions:*
- (1) *The action of G on $\prod_{D \in v} k^\times(D)$ by conjugation induces the identity automorphism on M .*
 - (2) *For any $D_0 \in v$, the composite $M \hookrightarrow \prod_{D \in v} k^\times(D) \rightarrow k^\times(D_0)$ is an isomorphism of modules.*
- (ii) *The inverse image of $\mathcal{O}^\times(D_0)$ (resp. $\mathcal{O}^\times(D_0)$, $U^{(1)}(D_0)$) by the isomorphism $M \xrightarrow{\sim} k^\times(D_0)$ of condition (2) of assertion (i) does not depend on the choice of $D_0 \in v$.*

Proof. In light of Theorem 2.6(v) and Theorem 3.3(iii), it is clear that the “diagonal” of $\prod_{D \in v} k^\times(D)$ is the unique submodule satisfying the conditions of (i). Assertion (ii) is immediate. \square

Lemma 3.9. *Let K be a PGF and $v \in \mathcal{V}_K$. Then the inverse image of $\mathcal{O}_{K_v}^\times$ (resp. $\mathcal{O}_{K_v}^\times, U_{K_v}^{(1)}$) by the natural inclusion $K^\times \hookrightarrow K_v^\times$ coincides with \mathcal{O}_v^\times (resp. $\mathcal{O}_v^\times, U_v^{(1)}$).*

Proof. Trivial. \square

Definition 3.10. Let G be a profinite group of PGF-type and $v \in \mathcal{V}(G)$.

- (i) Write $k^\times(v)$ for the unique submodule M of $\prod_{D \in v} k^\times(D)$ (cf. Theorem 3.6(i)) satisfying the conditions of Lemma 3.8(i).
- (ii) It follows from Lemma 3.8(ii) that the inverse image of $\mathcal{O}^\times(D_0)$ (resp. $\mathcal{O}^\times(D_0), U^{(1)}(D_0)$) by the isomorphism $k^\times(v) \xrightarrow{\sim} k^\times(D_0)$ of condition (2) of Lemma 3.8(i) does not depend on the choice of $D_0 \in v$. Write $\mathcal{O}^\times(v)$ (resp. $\mathcal{O}^\times(v), U^{(1)}(v)$) for this inverse image in $k^\times(v)$.
- (iii) Write $J(G) := \varinjlim_S (\prod_{w \in S} k^\times(w)) \times (\prod_{w \in \mathcal{V}(G) \setminus S} \mathcal{O}^\times(w))$, where S runs over all finite subsets of $\mathcal{V}(G)$. Note that $J(G) \subset \prod_{w \in \mathcal{V}(G)} \prod_{D \in w} D^{\text{ab}} = \prod_{D \in \bar{\mathcal{V}}(G)} D^{\text{ab}}$.
- (iv) It follows from Lemma 3.7, together with Theorem 3.11(i), (ii) below, that the inclusions $D \hookrightarrow G$ ($D \in \bar{\mathcal{V}}(G)$) determine a homomorphism $J(G) \rightarrow G^{\text{ab}}$. Write $K^\times(G) := \ker(J(G) \rightarrow G^{\text{ab}})$.
- (v) Write $\mathcal{O}_v^\times(G)$ (resp. $\mathcal{O}_v^\times(G), U_v^{(1)}(G)$) for the inverse image of $\mathcal{O}^\times(v)$ (resp. $\mathcal{O}^\times(v), U^{(1)}(v)$) by the composite of the inclusion $K^\times(G) \hookrightarrow J(G)$ and the projection $J(G) \rightarrow k^\times(v)$.

Theorem 3.11. *Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , and $v \in \mathcal{V}_K$. Write $v_G \in \mathcal{V}(G)$ for the image of $v \in \mathcal{V}_K$ by the bijection $\mathcal{V}_K \xrightarrow{\sim} \mathcal{V}(G)$ appearing in Theorem 3.6(i).*

- (i) *The isomorphism α determines an isomorphism $K_v^\times \xrightarrow{\sim} k^\times(v_G)$.*
- (ii) *The image of $\mathcal{O}_{K_v}^\times$ (resp. $\mathcal{O}_{K_v}^\times, U_{K_v}^{(1)}$) by the isomorphism $K_v^\times \xrightarrow{\sim} k^\times(v_G)$ appearing in (i) coincides with $\mathcal{O}^\times(v_G)$ (resp. $\mathcal{O}^\times(v_G), U^{(1)}(v_G)$).*
- (iii) *The isomorphism α and various isomorphisms appearing in (i) determine a commutative diagram of groups*

$$\begin{array}{ccc} J_K & \longrightarrow & \text{Gal}(\Omega/K)^{\text{ab}} \\ \downarrow \wr & & \downarrow \wr \\ J(G) & \longrightarrow & G^{\text{ab}}, \end{array}$$

where the lower horizontal arrow is the homomorphism appearing in Definition 3.10(iv). Moreover, this diagram determines an isomorphism of groups $K^\times \xrightarrow{\sim} K^\times(G)$.

- (iv) *The image of \mathcal{O}_v^\times (resp. $\mathcal{O}_v^\times, U_v^{(1)}$) by the isomorphism $K^\times \xrightarrow{\sim} K^\times(G)$ appearing in (iii) coincides with $\mathcal{O}_{v_G}^\times(G)$ (resp. $\mathcal{O}_{v_G}^\times(G), U_{v_G}^{(1)}(G)$).*

Proof. These assertions follow from Lemmas 3.7, 3.8, 3.9, together with Theorems 2.6, 3.6. \square

Theorem 3.12. *Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , $H \subset G$ an open subgroup of G , and $w \in \mathcal{V}(H)$. Write*

$v \in \mathcal{V}(G)$ for the image of w by the surjection $\mathcal{V}(H) \rightarrow \mathcal{V}(G)$ appearing in Theorem 3.6(ii) and L for the finite extension of K contained in Ω which corresponds to the open subgroup $\alpha^{-1}(H) \subset \text{Gal}(\Omega/K)$ of $\text{Gal}(\Omega/K)$. Then we obtain a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\sim} & K^\times(G) \\ \downarrow & & \downarrow \\ L^\times & \xrightarrow{\sim} & K^\times(H), \end{array}$$

where the horizontal arrows are the isomorphism appearing in Theorem 3.11(iii), and the right-hand vertical arrow is an injection determined by various injections “ $k^\times(v) \hookrightarrow k^\times(w)$ ” induced by the right-hand vertical arrow of the commutative diagram appearing in Theorem 2.7. In particular, the inverse image of $\mathcal{O}_w^\times(H)$ (resp. $\mathcal{O}_w^\times(H), U_w^{(1)}(H)$) by the injection $K^\times(G) \hookrightarrow K^\times(H)$ coincides with $\mathcal{O}_v^\times(G)$ (resp. $\mathcal{O}_v^\times(G), U_v^{(1)}(G)$).

Proof. This follows from Theorems 2.7, 3.11. \square

4. ADDITIVE STRUCTURE OF ONE-DIMENSIONAL FUNCTION FIELDS OVER FINITE FIELDS

In this section, we reconstruct the additive structure of one-dimensional function fields over finite fields.

Definition 4.1. Let K be a PGF.

- (i) We shall write
 - $F_K \subset K$ for the constant field of K ,
 - $\tilde{K} := K \otimes_{F_K} \overline{F}_K$, where \overline{F}_K is an algebraic closure of F_K ,
 - $C_{\tilde{K}}$ for a nonsingular projective curve whose function field is \tilde{K} (which is unique up to isomorphism, cf. e.g., [1] Chapter I, Corollary 6.12), and
 - $\text{Div}(\tilde{K})$ for the group of divisors of $C_{\tilde{K}}$.
- (ii) Let $v \in \mathcal{V}_{\tilde{K}}$. Then we shall write
 - $\text{ord}_v : \tilde{K}^\times \rightarrow \mathbb{Z}$ for the uniquely determined surjective valuation associated to v ,
 - $\tilde{\mathcal{O}}_v := \{a \in \tilde{K} \mid \text{ord}_v(a) \geq 0\} \subset \tilde{K}$ for the discrete valuation ring at v ,
 - $\tilde{\mathcal{O}}_v^\times := \tilde{\mathcal{O}}_v \setminus \{0\}$ for the multiplicative monoid of nonzero elements of $\tilde{\mathcal{O}}_v$,
 - $\tilde{\mathfrak{m}}_v \subset \tilde{\mathcal{O}}_v$ for the maximal ideal of $\tilde{\mathcal{O}}_v$,
 - $\tilde{U}_v^{(1)} := 1 + \tilde{\mathfrak{m}}_v \subset \tilde{\mathcal{O}}_v^\times$, and
 - $\tilde{\kappa}_v := \tilde{\mathcal{O}}_v / \tilde{\mathfrak{m}}_v$ for the residue field of $\tilde{\mathcal{O}}_v$.
- (iii) Let $v \in \mathcal{V}_{\tilde{K}}$ and $s \in \tilde{\mathcal{O}}_v$. Then we shall write $s(v) \in \tilde{\kappa}_v$ for the image of $s \in \tilde{\mathcal{O}}_v$ by the natural surjection $\tilde{\mathcal{O}}_v \rightarrow \tilde{\kappa}_v$.
- (iv) Let $D \in \text{Div}(\tilde{K})$. Then we shall write
 - $H^0(D) := H^0(C_{\tilde{K}}, \mathcal{L}(D))$, where $\mathcal{L}(D)$ is the invertible sheaf associated to D , and
 - $l(D) := \dim_{\overline{F}_K} H^0(D)$.

Lemma 4.2. *Let K be a PGF, Ω a solvably closed Galois extension of K , and $H \subset \text{Gal}(\Omega/K)$ an open subgroup of $\text{Gal}(\Omega/K)$. We regard \overline{F}_K and \tilde{K} as subfields of Ω in a natural way (i.e., \overline{F}_K is the algebraic closure of F_K in Ω). Write L for the finite extension of K contained in Ω associated to $H \subset \text{Gal}(\Omega/K)$. Then the following hold:*

- (i) *It holds that $F_K^\times = \bigcap_{v \in \mathcal{V}_K} \mathcal{O}_v^\times$.*
- (ii) *H contains $\ker(\text{Gal}(\Omega/K) \rightarrow \text{Gal}(\overline{F}_K/F_K))$ if and only if $[G : H] = [F_L : F_K] = \log_{\#F_K}(\#F_L)$ (in this case, $L = K \otimes_{F_K} F_L$).*

Proof. Trivial. \square

Definition 4.3. Let M be a monoid. Then let us write $M^\otimes := M \cup \{*_M\}$. We regard M^\otimes as a monoid by $a \cdot *_M = *_M \cdot a = *_M$ for every $a \in M^\otimes$. If $N \subset M$ is a submonoid of M , then we regard $N^\otimes \subset M^\otimes$ by identifying $*_N$ by $*_M$. We always write $*$ instead of $*_M$ for simplicity.

Definition 4.4. Let G be a profinite group of PGF-type.

- (i) Write $K(G) := (K^\times(G))^\otimes$.
- (ii) Write $F^\times(G) := \bigcap_{v \in \mathcal{V}(G)} \mathcal{O}_v^\times(G) \subset K^\times(G)$.
- (iii) It follows from Theorem 4.5(i) below that $\#F^\times(G)$ is finite and nonzero. Write $\tilde{G} := \bigcap_H H$, where H runs over all open subgroups of G such that $[G : H] = \log_{\#F^\times(G)+1}(\#F^\times(H) + 1)$ (cf. Remark 4).
- (iv) Write $\tilde{K}^\times(G) := \varinjlim_H K^\times(H)$, $\tilde{\mathcal{V}}(G) := \varinjlim_H \tilde{\mathcal{V}}(H)$ (cf. Remark 4), where H runs over all open subgroups of G containing \tilde{G} , and the transition maps are the maps appearing in Theorem 3.12, Theorem 3.6(ii). Note that the actions of “ H ”s on “ $\tilde{\mathcal{V}}(H)$ ”s determine an action of \tilde{G} on $\tilde{\mathcal{V}}(G)$.
- (v) Write $\tilde{\mathcal{V}}(G) := \tilde{\mathcal{V}}(G)/\tilde{G}$, $\text{Div}(G) := \bigoplus_{v \in \tilde{\mathcal{V}}(G)} \mathbb{Z} \cdot v$.
- (vi) It follows from Theorem 4.5(ii) below that any open subgroup of G containing \tilde{G} is normal in G . We define an action of G on $\tilde{K}^\times(G)$ by conjugation.
- (vii) Write $\tilde{K}(G) := (\tilde{K}^\times(G))^\otimes$, and define an action of G on $\tilde{K}(G)$ by the natural action determined by the action of G on $\tilde{K}^\times(G)$ appearing in (vi) and the trivial action of G on $\{*\} \subset \tilde{K}(G)$.

Theorem 4.5. *Let G be a profinite group of PGF-type and $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G . We regard \overline{F}_K and \tilde{K} as subfields of Ω in a natural way. Then the following hold:*

- (i) *The isomorphism of groups $K^\times \xrightarrow{\sim} K^\times(G)$ appearing in Theorem 3.11(iii) determines an isomorphism of monoids $K \xrightarrow{\sim} K(G)$. Moreover, the image of $F_K^\times \subset K$ by the isomorphism $K \xrightarrow{\sim} K(G)$ coincides with $F^\times(G)$.*
- (ii) *It holds that $\tilde{G} = \alpha(\ker(\text{Gal}(\Omega/K) \rightarrow \text{Gal}(\overline{F}_K/F_K)))$.*
- (iii) *The isomorphisms of groups “ $K^\times \xrightarrow{\sim} K^\times(G)$ ” appearing in Theorem 3.11(iii) for various open subgroups of G containing \tilde{G} determine an isomorphism of groups $\tilde{K}^\times \xrightarrow{\sim} \tilde{K}^\times(G)$, which is compatible with the actions of $\text{Gal}(\Omega/K)$ and G with respect to α . In particular, the above isomorphism induces an isomorphism of monoids $\tilde{K} \xrightarrow{\sim} \tilde{K}(G)$, which is compatible with the actions of $\text{Gal}(\Omega/K)$ and G .*
- (iv) *Let $H \subset G$ be an open subgroup of G containing \tilde{G} . Write L for the finite extension of K contained in Ω which corresponds to the open subgroup*

$\alpha^{-1}(H) \subset \text{Gal}(\Omega/K)$ of $\text{Gal}(\Omega/K)$. Then the natural map $\bar{\mathcal{V}}(H) \rightarrow \bar{\mathcal{V}}(G)$ is bijective. Moreover, the inverse map of this bijection and the bijection $\mathcal{V}_\Omega \xrightarrow{\sim} \bar{\mathcal{V}}(G)$ appearing in Theorem 3.6(i) determine a commutative diagram

$$\begin{array}{ccc} \mathcal{V}_{\tilde{K}} & \xrightarrow{\sim} & \tilde{\mathcal{V}}(G) \\ \downarrow & & \downarrow \\ \mathcal{V}_L & \xrightarrow{\sim} & \mathcal{V}(H). \end{array}$$

In particular, the bijection $\mathcal{V}_{\tilde{K}} \xrightarrow{\sim} \tilde{\mathcal{V}}(G)$ determines an isomorphism $\text{Div}(\tilde{K}) \xrightarrow{\sim} \text{Div}(G)$.

Proof. Assertion (i) follows from Lemma 4.2(i). Assertion (ii) follows from assertion (i) and Lemma 4.2(ii). Assertion (iii) is immediate. Assertion (iv) follows from Theorem 3.6. \square

Lemma 4.6. *Let K be a PGF and $v \in \mathcal{V}_{\tilde{K}}$. For any finite extension L of K contained in \tilde{K} , write $v_L \in \mathcal{V}_L$ for the image of $v \in \mathcal{V}_{\tilde{K}}$ by the natural surjection $\mathcal{V}_{\tilde{K}} \rightarrow \mathcal{V}_L$. Then the following hold:*

- (i) *It holds that $\tilde{\mathcal{O}}_v^\triangleright = \bigcup_L \mathcal{O}_{v_L}^\triangleright$, $\tilde{\mathcal{O}}_v^\times = \bigcup_L \mathcal{O}_{v_L}^\times$, $\tilde{U}_v^{(1)} = \bigcup_L U_{v_L}^{(1)}$, where L runs over all finite extensions of K contained in \tilde{K} .*
- (ii) *The natural surjection $\tilde{\mathcal{O}}_v \rightarrow \tilde{\kappa}_v$ induces an isomorphism of groups $\tilde{\mathcal{O}}_v^\times / \tilde{U}_v^{(1)} \xrightarrow{\sim} \tilde{\kappa}_v^\times$.*

Proof. Trivial. \square

Definition 4.7. Let G be a profinite group of PGF-type and $v \in \tilde{\mathcal{V}}(G)$. For any open subgroup $H \subset G$ of G containing \tilde{G} , write $v_H \in \mathcal{V}(H)$ for the image of $v \in \tilde{\mathcal{V}}(G)$ by the surjection $\tilde{\mathcal{V}}(G) \rightarrow \mathcal{V}(H)$ appearing in Theorem 4.5(iv).

- (i) Write $\tilde{\mathcal{O}}_v^\triangleright(G) := \varinjlim_H \mathcal{O}_{v_H}^\triangleright(H)$, $\tilde{\mathcal{O}}_v^\times(G) := \varinjlim_H \mathcal{O}_{v_H}^\times(H)$, $\tilde{U}_v^{(1)}(G) := \varinjlim_H U_{v_H}^{(1)}(H)$ (cf. Remark 4), where H runs over all open subgroups of G containing \tilde{G} , and the transition maps are the maps induced by the map “ $K^\times(G) \hookrightarrow K^\times(H)$ ” appearing in Theorem 3.12.
- (ii) Write $\tilde{\kappa}_v^\times(G) := \tilde{\mathcal{O}}_v^\times(G) / \tilde{U}_v^{(1)}(G)$.
- (iii) Write $\tilde{\mathcal{O}}_v(G) := (\tilde{\mathcal{O}}_v^\triangleright(G))^\otimes$, $\tilde{\kappa}_v(G) := (\tilde{\kappa}_v^\times(G))^\otimes$.

Theorem 4.8. *Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , and $v \in \mathcal{V}_{\tilde{K}}$. Write $v_G \in \tilde{\mathcal{V}}(G)$ for the image of $v \in \mathcal{V}_{\tilde{K}}$ by the bijection $\mathcal{V}_{\tilde{K}} \xrightarrow{\sim} \tilde{\mathcal{V}}(G)$ appearing in Theorem 4.5(iv). Then the following hold:*

- (i) *The image of $\tilde{\mathcal{O}}_v$ (resp. $\tilde{\mathcal{O}}_v^\triangleright$, $\tilde{\mathcal{O}}_v^\times$, $\tilde{U}_v^{(1)}$) by the isomorphism $\tilde{K} \xrightarrow{\sim} \tilde{K}(G)$ appearing in Theorem 4.5(iii) coincides with $\tilde{\mathcal{O}}_{v_G}(G)$ (resp. $\tilde{\mathcal{O}}_{v_G}^\triangleright(G)$, $\tilde{\mathcal{O}}_{v_G}^\times(G)$, $\tilde{U}_{v_G}^{(1)}(G)$).*
- (ii) *The isomorphisms of groups $\tilde{\mathcal{O}}_v^\times \xrightarrow{\sim} \tilde{\mathcal{O}}_{v_G}^\times(G)$, $\tilde{U}_v^{(1)} \xrightarrow{\sim} \tilde{U}_{v_G}^{(1)}(G)$ obtained in (i) determine an isomorphism of groups $\tilde{\kappa}_v^\times \xrightarrow{\sim} \tilde{\kappa}_{v_G}^\times(G)$. In particular, we obtain an isomorphism of monoids $\tilde{\kappa}_v \xrightarrow{\sim} \tilde{\kappa}_{v_G}(G)$.*

Proof. Assertion (i) follows from Theorem 3.11(iv), Theorem 3.12, Theorem 4.5(iii), (iv), Lemma 4.6(i). Assertion (ii) follows from assertion (i) and Lemma 4.6(ii). \square

Definition 4.9. Let G be a profinite group of PGF-type, $v \in \tilde{\mathcal{V}}(G)$, and $s \in \tilde{\mathcal{O}}_v(G)$. If $s \in \tilde{\mathcal{O}}_v^\times(G)$, then we shall write $s(v) \in \tilde{\kappa}_v(G)$ for the image of the composite $\tilde{\mathcal{O}}_v^\times(G) \twoheadrightarrow \tilde{\kappa}_v^\times(G) \hookrightarrow \tilde{\kappa}_v(G)$. If $s \notin \tilde{\mathcal{O}}_v^\times(G)$, then we shall write $s(v) := * \in \tilde{\kappa}_v(G)$.

Theorem 4.10. Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , $v \in \mathcal{V}_{\tilde{K}}$, and $s \in \tilde{\mathcal{O}}_v$. Write $v_G \in \tilde{\mathcal{V}}(G)$ for the image of $v \in \mathcal{V}_{\tilde{K}}$ by the bijection $\mathcal{V}_{\tilde{K}} \xrightarrow{\sim} \tilde{\mathcal{V}}(G)$ appearing in Theorem 4.5(iv), and $s_G \in \tilde{\mathcal{O}}_{v_G}(G)$ for the image of $s \in \tilde{\mathcal{O}}_v$ by the isomorphism $\tilde{\mathcal{O}}_v \xrightarrow{\sim} \tilde{\mathcal{O}}_{v_G}(G)$ obtained in Theorem 4.8(i). Then the image of $s(v) \in \tilde{\kappa}_v$ by the isomorphism $\tilde{\kappa}_v \xrightarrow{\sim} \tilde{\kappa}_{v_G}(G)$ appearing in Theorem 4.8(ii) coincides with $s_G(v_G) \in \tilde{\kappa}_{v_G}(G)$.

Proof. This follows from Theorem 4.8(ii). \square

Lemma 4.11. Let K be a PGF, $v \in \mathcal{V}_{\tilde{K}}$ and $s \in \tilde{K}^\times$. Then the following hold:

- (i) $\text{ord}_v(s) = 1$ if and only if $\mathcal{O}_v^\times \subset \tilde{K}^\times$ is generated by $\tilde{\mathcal{O}}_v^\times$ and s as a monoid.
- (ii) Let $t \in \tilde{K}^\times$ such that $\text{ord}_v(t) = 1$. Then $\text{ord}_v(s)$ is the unique integer n such that $s \cdot t^{-n} \in \tilde{\mathcal{O}}_v^\times$.

Proof. Trivial. \square

Definition 4.12. Let G be a profinite group of PGF-type, $v \in \tilde{\mathcal{V}}(G)$, and $s \in \tilde{K}^\times(G)$. Let us define $\text{ord}_v^G(s) \in \mathbb{Z}$ as follows:

- (i) If $\tilde{\mathcal{O}}_v^\times(G) \subset \tilde{K}^\times(G)$ is generated by $\tilde{\mathcal{O}}_v^\times(G) \subset \tilde{\mathcal{O}}_v^\times(G)$ and s as a monoid, then let us write $\text{ord}_v^G(s) := 1$.
- (ii) It follows from Theorem 4.5(iii), Theorem 4.8(i), Lemma 4.11 that there exists $t \in \tilde{K}^\times(G)$ such that $\text{ord}_v^G(t) = 1$ (in the sense of (i)), and, moreover, there exists a unique integer n such that $s \cdot t^{-n} \in \tilde{\mathcal{O}}_v^\times(G)$. Let us write $\text{ord}_v^G(s)$ for this integer n .

Note that it follows from Theorem 4.5(iii), Theorem 4.8(i), Lemma 4.11 that $\text{ord}_v^G(s)$ is well-defined, i.e.,

- the condition “ $s \cdot t^{-n} \in \tilde{\mathcal{O}}_v^\times(G)$ ” does not depend on the choice of t , and
- “ $\text{ord}_v^G(s) = 1$ ” in the sense of (i) if and only if “ $\text{ord}_v^G(s) = 1$ ” in the sense of (ii).

Theorem 4.13. Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , and $v \in \mathcal{V}_{\tilde{K}}$. Write v_G for the image of $v \in \mathcal{V}_{\tilde{K}}$ by the bijection $\mathcal{V}_{\tilde{K}} \xrightarrow{\sim} \tilde{\mathcal{V}}(G)$ appearing in Theorem 4.5(iv). Then the composite of $\text{ord}_{v_G}^G : \tilde{K}^\times(G) \rightarrow \mathbb{Z}$ and the isomorphism $\tilde{K}^\times \xrightarrow{\sim} \tilde{K}^\times(G)$ appearing in Theorem 4.5(iii) coincides with $\text{ord}_v : \tilde{K}^\times \rightarrow \mathbb{Z}$.

Proof. This follows from Theorem 4.5(iii), Theorem 4.8(i), Lemma 4.11. \square

Lemma 4.14. Let K be a PGF. Then the following hold:

- (i) Let $D = \sum_{v \in \mathcal{V}_{\tilde{K}}} n_v \cdot v \in \text{Div}(\tilde{K})$. Then it holds that

$$H^0(D) = \{s \in \tilde{K}^\times \mid \text{ord}_v(s) + n_v \geq 0 \text{ for all } v \in \mathcal{V}_{\tilde{K}}\} \cup \{0\},$$

$$l(D) = \min\{n \in \mathbb{Z}_{\geq 0} \mid \text{there exist } v_1, \dots, v_n \in \mathcal{V}_{\tilde{K}} \text{ such that } H^0(D - \sum_{m=1}^n v_m) = \{0\}\}.$$

- (ii) For any $v \in \mathcal{V}_{\tilde{K}}$, there exist $D = \sum_{w \in \mathcal{V}_{\tilde{K}}} n_w \cdot w \in \text{Div}(\tilde{K})$ and $w_1, w_2 \in \mathcal{V}_{\tilde{K}}$ such that v, w_1, w_2 are distinct, $n_v = n_{w_1} = n_{w_2} = 0$, $l(D) = 2$, $l(D - v - w_1) = l(D - v - w_2) = l(D - w_1 - w_2) = 0$.
- (iii) Let $v, w_1, w_2 \in \mathcal{V}_{\tilde{K}}$, $D \in \text{Div}(\tilde{K})$ be as in (ii). Moreover, let $\zeta, \lambda \in \tilde{\kappa}_v^\times$. Then there exists a unique element s (resp. t) of $H^0(D)$ such that $s(v) = \zeta$, $s(w_1) = 0$, $s(w_2) \neq 0$ (resp. $t(v) = \lambda$, $t(w_1) \neq 0$, $t(w_2) = 0$). Moreover, $s + t \in H^0(D)$ is the unique element u of $H^0(D)$ such that $u(w_1) = t(w_1)$, $u(w_2) = s(w_2)$.

Proof. Let us observe that, it follows from the proof of [1] Chapter IV, Proposition 3.1 that, for any $D \in \text{Div}(\tilde{K})$ and $w \in \mathcal{V}_{\tilde{K}}$, it holds that $l(D - w) \geq l(D) - 1$, and, moreover, if $l(D) > 0$, then for all but finitely many $w \in \mathcal{V}_{\tilde{K}}$, it holds that $l(D - w) = l(D) - 1$. In particular, assertion (i) holds. Next, we verify assertion (ii). Let W be a canonical divisor (cf. [1] Chapter IV, §1). Write g for the genus of $C_{\tilde{K}}$. Then it follows from Riemann-Roch theorem (cf. [1] Chapter IV, Theorem 1.3) that $l(W + v) = \deg(W + v) + 1 - g + l(-v) = g < g + 1$. Thus, it follows from the observation above that there exists a divisor $D = \sum_{w \in \mathcal{V}_{\tilde{K}}} n_w \cdot w \in \text{Div}(\tilde{K})$ such that $n_v = 0$, $\deg D = g + 1$ and $l(W + v - D) = 0$. Then, since $l(W - D) \leq l(W + v - D) = 0$ (hence $l(W - D) = 0$), it follows from Riemann-Roch theorem that $l(D) = \deg D + 1 - g - l(W - D) = 2$, $l(D - v) = \deg(D - v) + 1 - g - l(W + v - D) = 1$. Moreover, it follows from the observation above that there exist $w_1, w_2 \in \mathcal{V}_{\tilde{K}}$ such that v, w_1, w_2 are distinct, $n_v = n_{w_1} = n_{w_2} = 0$, $l(D - v - w_1) = l(D - v) - 1$, $l(D - v - w_2) = l(D - v) - 1$, $l(D - w_1 - w_2) = l(D - w_1) - 1$. Now we can easily check that D, w_1, w_2 satisfy the condition of assertion (ii). This completes the proof of assertion (ii). Finally, we verify assertion (iii). The existence of s (resp. t) follows from the fact that $l(D - w_1) = 1$ (resp. $l(D - w_2) = 1$), and the uniqueness of s (resp. t, u) follows from the assumption that $l(D - v - w_1) = 0$ (resp. $l(D - v - w_2) = 0, l(D - w_1 - w_2) = 0$). This completes the proof of assertion (iii), hence also of Lemma 4.14. \square

Definition 4.15. Let G be a profinite group of PGF-type and $D = \sum_{v \in \tilde{\mathcal{V}}(G)} n_v \cdot v \in \text{Div}(G)$.

- (i) Write $H_G^0(D) = \{s \in \tilde{K}^\times(G) \mid \text{ord}_v^G(s) + n_v \geq 0 \text{ for all } v \in \tilde{\mathcal{V}}(G)\} \cup \{*\} \subset \tilde{K}(G)$.
- (ii) It follows from Theorem 4.5(iii), (iv), Theorem 4.13, Lemma 4.14(i), together with Theorem 4.16(i) below, that the set $\{n \in \mathbb{Z}_{\geq 0} \mid \text{there exist } v_1, \dots, v_n \in \tilde{\mathcal{V}}(G) \text{ such that } H_G^0(D - \sum_{m=1}^n v_m) = \{*\}\}$ is not empty. Write $l_G(D)$ for the smallest integer in this set.

Theorem 4.16. Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , and $D \in \text{Div}(\tilde{K})$. Write $D_G \in \text{Div}(G)$ for the image of $D \in \text{Div}(\tilde{K})$ by the isomorphism $\text{Div}(\tilde{K}) \xrightarrow{\sim} \text{Div}(G)$ appearing in Theorem 4.5(iv). Then the following hold:

- (i) The image of $H^0(D) \subset \tilde{K}$ by the isomorphism of monoids $\tilde{K} \xrightarrow{\sim} \tilde{K}(G)$ appearing in Theorem 4.5(iii) coincides with $H_G^0(D_G) \subset \tilde{K}(G)$.
- (ii) It holds that $l(D) = l_G(D_G)$.

Proof. These assertions follow from Theorem 4.13, Lemma 4.14(i). \square

Definition 4.17. Let G be a profinite group of PGF-type, $v \in \tilde{\mathcal{V}}(G)$, and $\zeta, \lambda \in \tilde{\kappa}_v(G)$. Let us define $\zeta \boxplus_v \lambda \in \tilde{\kappa}_v(G)$ as follows:

- (i) If $\zeta = *$, then $\zeta \boxplus_v \lambda := \lambda$.
- (ii) If $\lambda = *$, then $\zeta \boxplus_v \lambda := \zeta$.
- (iii) Suppose that $\zeta \neq *$, $\lambda \neq *$. Then it follows from Theorem 4.5(iv), Lemma 4.14(ii), Theorem 4.16(ii) that there exist $D = \sum_{w \in \tilde{\mathcal{V}}(G)} n_w \cdot w \in \text{Div}(G)$ and $w_1, w_2 \in \tilde{\mathcal{V}}(G)$ such that v, w_1, w_2 are distinct, $n_v = n_{w_1} = n_{w_2} = 0$, $l_G(D) = 2$, $l_G(D - v - w_1) = l_G(D - v - w_2) = l_G(D - w_1 - w_2) = 0$. Moreover, it follows from Theorem 4.5(iv), Theorem 4.10, Lemma 4.14(iii), Theorem 4.16 that there exists a unique element s (resp. t, u) of $H_G^0(D)$ such that $s(v) = \zeta$, $s(w_1) = *$, $s(w_2) \neq *$ (resp. $t(v) = \lambda$, $t(w_1) \neq *$, $t(w_2) = *$; $u(w_1) = t(w_1)$, $u(w_2) = s(w_2)$). Then we shall write $\zeta \boxplus_v \lambda := u(v)$.

Theorem 4.18. Let G be a profinite group of PGF-type, $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G , and $v \in \mathcal{V}_{\tilde{K}}$. Write $v_G \in \tilde{\mathcal{V}}(G)$ for the image of $v \in \mathcal{V}_{\tilde{K}}$ by the bijection $\mathcal{V}_{\tilde{K}} \xrightarrow{\sim} \tilde{\mathcal{V}}(G)$ appearing in Theorem 4.5(iv). Then $\boxplus_{v_G} : \tilde{\kappa}_{v_G}(G) \times \tilde{\kappa}_{v_G}(G) \rightarrow \tilde{\kappa}_{v_G}(G)$ is well-defined (i.e., does not depend on the choice of D, w_1, w_2) and determines a structure of field on $\tilde{\kappa}_{v_G}(G)$. Moreover, the isomorphism of monoids $\tilde{\kappa}_v \xrightarrow{\sim} \tilde{\kappa}_{v_G}(G)$ appearing in Theorem 4.8(ii) is an isomorphism of fields.

Proof. This follows from Theorem 4.5(iv), Theorem 4.10, Lemma 4.14(iii), Theorem 4.16. \square

Lemma 4.19. Let $x, y \in \tilde{K}$. Then $x + y \in \tilde{K}$ is the unique element z of \tilde{K} such that, for any $v \in \mathcal{V}_{\tilde{K}}$, if $x, y, z \in \tilde{\mathcal{O}}_v$, then it holds that $x(v) + y(v) = z(v)$.

Proof. Trivial. \square

Definition 4.20. Let G be a profinite group of PGF-type and $x, y \in \tilde{K}(G)$. Then it follows from Theorem 4.5(iii), (iv), Theorem 4.10, Theorem 4.18, Lemma 4.19 that there exists a unique element z of $\tilde{K}(G)$ such that, for any $v \in \tilde{\mathcal{V}}(G)$, if $x, y, z \in \tilde{\mathcal{O}}_v(G)$, then it holds that $x(v) \boxplus_v y(v) = z(v)$. Write $x \boxplus y \in \tilde{K}(G)$ for this element z .

Theorem 4.21. Let G be a profinite group of PGF-type and $(K, \Omega, \alpha : \text{Gal}(\Omega/K) \xrightarrow{\sim} G)$ a PGF-envelope for G .

- (i) $\boxplus : \tilde{K}(G) \times \tilde{K}(G) \rightarrow \tilde{K}(G)$ determines a structure of field on $\tilde{K}(G)$. Moreover, the isomorphism of monoids $\tilde{K} \xrightarrow{\sim} \tilde{K}(G)$ appearing in Theorem 4.5(iii) is an isomorphism of fields.
- (ii) It holds that $(\tilde{K}(G))^G = K(G)$, hence \boxplus determines a structure of field on $K(G)$. In particular, the isomorphism of monoids $K \xrightarrow{\sim} K(G)$ appearing in Theorem 4.5(i) is an isomorphism of fields.

Proof. Assertion (i) follows from Theorem 4.5(iii), (iv), Theorem 4.10, Theorem 4.18, Lemma 4.19. Assertion (ii) follows from assertion (i) and Theorem 4.5(iii). \square

Acknowledgement

I would like to thank the organizers of the workshop ‘‘Inter-universal Teichmüller Theory Summit 2016’’ for the opportunity to talk at this workshop. I would also like to thank Professor Yuichiro Hoshi for valuable discussions. I would also like to thank Professor Akio Tamagawa for incisive comments on this manuscript.

REFERENCES

- [1] Hartshorne, R., *Algebraic geometry*, Graduate Texts in Mathematics, No. **52**, Springer-Verlag, New York-Heidelberg, 1977.
- [2] Hoshi, Y., Mono-anabelian reconstruction of number fields, RIMS preprint **1819** (2015).
- [3] Mochizuki, S., Global solvably closed anabelian geometry, *Math. J. Okayama Univ.* **48** (2006), 57-71.
- [4] Mochizuki, S., Topics in absolute anabelian geometry III: global reconstruction algorithms, *J. Math. Sci. Univ. Tokyo* **22** (2015), no. 4, 939-1156.
- [5] Neukirch, J., Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, *J. Reine Angew. Math.* **238** (1969), 135-147.
- [6] Neukirch, J., Über die absoluten Galoisgruppen algebraischer Zahlkörper, *Journées Arithmétiques de Caen, Astérisque* **41-42** (1977), Soc. Math. de France, 67-79.
- [7] Neukirch, J., *Algebraic number theory*, Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **322**, Springer-Verlag, Berlin, 1999.
- [8] Neukirch, J., Schmidt, A. and Wingberg, K., *Cohomology of number fields*, Second Edition, Grundlehren der mathematischen Wissenschaften. A Series of Comprehensive Studies in Mathematics **323**, Springer-Verlag, Berlin, 2008.
- [9] Uchida, K., Isomorphisms of Galois groups, *J. Math. Soc. Japan* **28** (1976), no. 4, 617-620.
- [10] Uchida, K., Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math.* **106** (1977), no. 3, 589-598.
- [11] Uchida, K., Isomorphisms of Galois groups of solvably closed Galois extensions, *Tôhoku Math. J.* **31** (1979), no. 3, 359-362.
- [12] Weil, A., *Basic number theory*, Third Edition, Die Grundlehren der Mathematischen Wissenschaften **144**, Springer-Verlag, New York-Berlin, 1974.

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KYOTO 606-8502,
JAPAN

E-mail address: sawada@kurims.kyoto-u.ac.jp