A NUMBER FIELD ANALOGUE OF THE GROTHENDIECK CONJECTURE FOR CURVES OVER FINITE FIELDS

MANABU OZAKI

Dedicated to the memory of Tamao Ozaki

1. Introduction

Analogy between number fields and 1-dimensional function fields (or algebraic curves) over finite fields has led us to a deep insight into these two arithmetic objects. For example, the "Main Conjecture" of Iwasawa theory of cyclotomic $\mathbb{Z}_p$-extensions can be regard as an analogy of Weil's theorem on the relationship among the congruent zeta function and the Frobenius action on the Tate module associated to a curve over a finite field. Here, we regard that the cyclotomic $\mathbb{Z}_p$-extension, or adjoining all the p-power-th roots of unity, is analogous to the constant field extension $\overline{\mathbb{F}}K/K$ of a function field K over a finite field $\mathbb{F}$ to an algebraic closure $\overline{\mathbb{F}}$.

However the extension $\overline{\mathbb{F}}K/K$ is in fact given by ajoining *all* the roots of unity in $\overline{\mathbb{F}}$. Therefore it is natural to ask what happens if we consider the *maximal cyclotomic extension* of a number field k, namely, the extension $k(\mu_\infty)/k$ given by adjoining all the roots of unity μ_∞, instead of the cyclotomic $\mathbb{Z}_p$-extension.

In the present paper, we choose the maximal cyclotomic extension as the analogous object of the constant field extension $\overline{\mathbb{F}}K/K$. Then we will give a number field analogue of the Grothendieck conjecture for curves over finite fields, proved by Tamagawa [8] and Mochizuki [5].

Let C be a non-singular geometrically connected curve over a field F. Denote by $F(C)$ the function field of C over F, and by $\overline{F}^{\mathrm{sep}}$ a separable closure of F. We put $\overline{F}^{\mathrm{sep}}(C) := F(C)\overline{F}^{\mathrm{sep}}$, and define $L(C)$ to be the maximal extension field (in a fixed algebraic closure) of $\overline{F}^{\mathrm{sep}}(C)$ unramified at $C \times_F \overline{F}^{\mathrm{sep}}$ (Note that $L(C)/\overline{F}^{\mathrm{sep}}(C)$ is the maximal unramified extension if C is projective).

Then we get the following fundamental exact sequence:

$$1 \longrightarrow \mathrm{Gal}(L(C)/\overline{F}^{\mathrm{sep}}(C)) \longrightarrow \mathrm{Gal}(L(C)/F(C)) \xrightarrow{P_C} G_F \longrightarrow 1, \tag{1}$$

where $G_F := \mathrm{Gal}(\overline{F}^{\mathrm{sep}}/F) \simeq \mathrm{Gal}(\overline{F}^{\mathrm{sep}}(C)/F(C))$ is the absolute Galois group of F.

Assume that C is *hyperbolic*, namely, $2 - 2g_C - n_C < 0$ holds, where g_C is the genus of C and $n_C := \#(C^*(\overline{F}) - C(\overline{F}))$, C^* being the compactification of C. This assumption is equivalent to that $\mathrm{Gal}(L(C)/\overline{F}^{\mathrm{sep}}(C))$ is non-abelian if $\mathrm{char}(F) = 0$. The Grothendieck conjecture asserts that the pro-finite group homomorphism $P_C : \mathrm{Gal}(L(C)/F(C)) \quad G_F$ has much information to reconstruct the curve C itself. This conjecture has been established by A.Tamagawa (case $n_C > 0$) and S.Mochizuki (case $n_C = 0$) in the case where F is finitely generated over $\mathbb{Q}$ or finite. More presisely:

Theorem A (Tamagawa[8], Mochizuki[4])**.** Let F be a field finitely generated over $\mathbb{Q}$, and C_i a hyperbolic curve over F $(i = 1, 2)$. Put $G_i := \mathrm{Gal}(L(C_i)/F(C_i))$ $(i = 1, 2)$. Then there is the natural bijection

$$\mathrm{Isom}_F(C_1, C_2) \simeq \mathrm{Isom}_{G_F}(G_1, G_2)/\mathrm{Inn}(\mathrm{Gal}(L(C_2)/\overline{F}(C_2)),$$

where the left hand side is the set of the F-isomorphisms of curves from C_1 to C_2 and the right hand side is the quotient of the set of the pro-finite group isomorphisms from G_1 to G_2 which are compatible with P_{C_1} and P_{C_2} by the right action of the inner automorphism group of $\mathrm{Gal}(L(C_2)/\overline{F}(C_2))$.

In the case where F is finite, the following "absolute version" of the Grothendieck conjecture holds:

Theorem B (Tamagawa[8], Mochizuki[5])**.** Let F_i be a finite field, and C_i a hyperbolic curve over F_i $(i = 1, 2)$. Put $G_i := \mathrm{Gal}(L(C_i)/F_i(C_i))$ $(i = 1, 2)$. Then there is the natural bijection

$$\mathrm{Isom}(C_1, C_2) \simeq \mathrm{Isom}(G_1, G_2)/\mathrm{Inn}(G_2),$$

where the left hand side is the set of the isomorphisms as schemes from C_1 to C_2 and the right hand side is the quotient of the set of the pro-finite group isomorphisms from G_1 to G_2 by the right action of the inner automorphism group of G_2.

From the viewpoint that the maximal cyclotomic extension $k(\mu_\infty)/k$ of a number field k is an analogous object to the constant field extension $\overline{\mathbb{F}}(C)/\mathbb{F}(C)$ for the function field of a curve C over a finite field $\mathbb{F}$, we find that the number field analogue of the fundamental exact sequence (1) in the case where C is projective is

$$1 \longrightarrow \mathrm{Gal}(L(\tilde{k})/\tilde{k}) \longrightarrow \mathrm{Gal}(L(\tilde{k})/k) \longrightarrow \mathrm{Gal}(\tilde{k}/k) \longrightarrow 1,$$

where $L(\tilde{k})$ is the maximal unramified exttension over $\tilde{k} := k(\mu_\infty)$.

Under this situation, we will give the following theorem analogous to Theorem B:

Theorem 1. Let k_i be a number field of finite degree, and L_i the maximal unramified extension field over $k_i(\mu_\infty)$ $(i = 1, 2)$. For any isomorphism

$$\varphi : \mathrm{Gal}(L_1/k_1) \simeq \mathrm{Gal}(L_2/k_2)$$

of pro-finite groups, there exists the unique field isomorphism

$$\tau : L_1 \simeq L_2$$

such that $\tau(k_1) = k_2$ and

$$\varphi(x) = \tau x \tau^{-1}$$

holds for every $x \in \mathrm{Gal}(L_1/k_1)$. In other words, we have the natural bijection

$$\mathrm{Isom}(L_1/k_1, L_2/k_2) \simeq \mathrm{Isom}(\mathrm{Gal}(L_1/k_1), \mathrm{Gal}(L_2/k_2)),$$

where the left hand side is the set of all the field isomorphisms $\tau : L_1 \simeq L_2$ with $\tau(k_1) = k_2$, and the right hand side is the set of all the isomorphism $\mathrm{Gal}(L_1/k_1) \simeq \mathrm{Gal}(L_2/k_2)$ of pro-finite groups.

Remark 1. The above theorem is an affirmative answer to [6, Conjecture(12.5.3)] in the case where the ramified prime sets are empty.

2. Arithmetically equivalence

For any number field F, we put $\tilde{F} := F(\mu_\infty)$, and denote by $L(F)$ the maximal unramified extension field over F.

In this section, we will show the following proposition, which plays a crucial role in the proof of Theorem 1.

Proposition 1. Let k_i be a number field of finite degree ($i = 1, 2$). Assume that there exists an isomorphism

$$\varphi : \mathrm{Gal}(L_1/k_1) \simeq \mathrm{Gal}(L_2/k_2)$$

of pro-finite groups, where $L_i := L(\tilde{k_i})$ $(i = 1, 2)$.

Then for any finite subextension M_1/k_1 of L_1/k_1, M_1 and $M_2 := L_2^{\varphi(\mathrm{Gal}(L_1/M_1))}$ are arithmetically equivalent: $M_1 \approx M_2$. Namely, they have the same Dedekind zeta function: $\zeta_{M_1}(s) = \zeta_{M_2}(s)$.

In Proposition 1, we note that $L_i = L(\tilde{M_i})$ and φ induces $\mathrm{Gal}(L_1/M_1) \simeq \mathrm{Gal}(L_2/M_2)$, hence it is enough to show the proposition in the case where $M_1 = k_1$.

Let K_i/k_i be the maximal abelian subextension of L_i/k_i, and denote by $L^{\mathrm{ab}}(K_i)$ the maximal unramified abelian extension field over K_i. Since $L^{\mathrm{ab}}(K_i) \subseteq L_i$ and

$$\begin{aligned}&\mathrm{Gal}(L^{\mathrm{ab}}(K_i)/k_i)\\ &\qquad \simeq \mathrm{Gal}(L_i/k_i)/((\mathrm{Gal}(L_i/k_i), \mathrm{Gal}(L_i/k_i)), (\mathrm{Gal}(L_i/k_i), \mathrm{Gal}(L_i/k_i))),\end{aligned}$$

Proposition 1 follows from the following:

Proposition 2. Assume that there exists an isomorphism

$$\psi : \mathrm{Gal}(L^{\mathrm{ab}}(K_1)/k_1) \simeq \mathrm{Gal}(L^{\mathrm{ab}}(K_2)/k_2)$$

of pro-finite groups. Then we have $k_1 \approx k_2$.

Our proof of the above proposition is based on the following fact:

Theorem C (Stuart-Perlis[7]). Let $g_F(l)$ be the number of primes of F lying over l for any number field F of finite degree and prime number l. Assume that $g_{k_1}(l) = g_{k_2}(l)$ holds for number fields k_1 and k_2 of finite degree and all but finitely many prime numbers l. Then we have $k_1 \approx k_2$.

In what follows, we will show that $g_{k_i}(l)$ is encoded in the group structure of $\mathrm{Gal}(L^{\mathrm{ab}}(K_i)/k_i)$. For simplicity, we write K and k for K_i and k_i, respectively.

We first analyze $\mathrm{Gal}(K/k)$ and its decomposition and inertia subgroups. We denote by $D_{\mathfrak{l}}(M/F)$ and $I_{\mathfrak{l}}(M/F)$ the decomposition and the inertia subgroup, respectively, of $\mathrm{Gal}(M/F)$ for a prime $\mathfrak{l}$ of k, M/F being any abelian extension of number fields.

Lemma 1. For any non-archimedean prime $\mathfrak{l}$ of k, we have

$$D_{\mathfrak{l}}(K/k) \simeq \hat{\mathbb{Z}} \times \mathbb{Z}_l \times \mathbb{Z}/d_{\mathfrak{l}}, \quad I_{\mathfrak{l}}(K/k) \simeq \mathbb{Z}_l \times \mathbb{Z}/d_{\mathfrak{l}},$$

where l is the rational prime below $\mathfrak{l}$ and $d_{\mathfrak{l}}$ is a certain divisor of $l-1$ (if $l \neq 2$) or 2 (if $l = 2$). Furthermore, we have $d_{\mathfrak{l}} = l - 1$ (if $l \neq 2$) or $d_{\mathfrak{l}} = 2$ (if $l = 2$)) if $\mathfrak{l}$ is unramified in $k/\mathbb{Q}$.

Proof. For any rational prime l, it is easy to see that

$$D_l(\tilde{\mathbb{Q}}/\mathbb{Q}) \simeq \hat{\mathbb{Z}} \times \mathbb{Z}_l \times \mathbb{Z}/b_l, \quad I_l(\tilde{\mathbb{Q}}/\mathbb{Q}) \simeq \mathbb{Z}_l \times \mathbb{Z}/b_l,$$

where $b_l = l - 1$ (if $l \neq 2$) or $b_l = 2$ (if $l = 2$).

The restriction $\mathrm{Gal}(\tilde{k}/k) \quad \mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$ induce injections $D_{\mathfrak{l}}(\tilde{k}/k) \quad D_l(\tilde{\mathbb{Q}}/\mathbb{Q})$ and $I_{\mathfrak{l}}(\tilde{k}/k) \quad I_l(\tilde{\mathbb{Q}}/\mathbb{Q})$ with finite cokernels. Hence we see that

$$D_{\mathfrak{l}}(\tilde{k}/k) \simeq \hat{\mathbb{Z}} \times \mathbb{Z}_l \times \mathbb{Z}/d_{\mathfrak{l}}, \quad I_{\mathfrak{l}}(\tilde{k}/k) \simeq \mathbb{Z}_l \times \mathbb{Z}/d_{\mathfrak{l}}, \tag{2}$$

for a certain divisor d_l of $l-1$ or 2, which equals $l-1$ or 2 if l is unramified in $k/\mathbb{Q}$. Because $K/\tilde{k}$ is unramified and every prime totally splits in it, we see that the restriction $\mathrm{Gal}(K/k) \quad \mathrm{Gal}(\tilde{k}/k)$ induces isomorphisms

$$D_{\mathfrak{l}}(K/k) \simeq D_{\mathfrak{l}}(\tilde{k}/k), \quad I_{\mathfrak{l}}(K/k) \simeq I_{\mathfrak{l}}(\tilde{k}/k).$$

Therefore the assertion of the lemma follows from (2). $\square$

Lemma 2. $I_{\mathfrak{l}_1}(K/k) \cap I_{\mathfrak{l}_2}(K/k) = 1$ for any non-archimedean primes $\mathfrak{l}_1$ and $\mathfrak{l}_2$ of k with $\mathfrak{l}_1 \neq \mathfrak{l}_2$.

Proof. We first note that K is the genus class field of $\tilde{k}/k$, namely, the maximal unramified abelian extension filed of $\tilde{k}$ which is abelian over k. Then, by using [2, Proposition 2], we see that the global resiprocity map induces the isomorphism

$$\rho : \mathcal{C}_k := J_k \Big/ \overline{k^\times \prod_{\mathfrak{p}:\ \text{primes of } k} U_{\mathfrak{p}}^0} \simeq \mathrm{Gal}(K/k), \tag{3}$$

where J_k is the idele group of k,

$$U_{\mathfrak{p}}^0 := \begin{cases} \ker(N_{k_{\mathfrak{p}}/\mathbb{Q}_p} : U_{\mathfrak{p}} \longrightarrow \mathbb{Z}_p^\times) \text{ if } \mathfrak{p} \text{ is a non-archimedean prime,} \\ \mathbb{R}_{>0}^\times \text{ if } \mathfrak{p} \text{ is a real arichimedean prime,} \\ \mathbb{C}^\times \text{ if } \mathfrak{p} \text{ is a complex archimedean prime,} \end{cases}$$

$U_{\mathfrak{p}}$ and p being the local unit group of $k_{\mathfrak{p}}$ and the prime number below $\mathfrak{p}$, respectively, and the "bar" means topological closure.

Assume that $I_{\mathfrak{l}_1}(K/k) \cap I_{\mathfrak{l}_2}(K/k) \neq 1$. Then it follows from (3) that there exists $u_{\mathfrak{l}_i} \in U_{\mathfrak{l}_i}$ $(i = 1, 2)$ such that $[(u_{\mathfrak{l}_1})] = [(u_{\mathfrak{l}_2})] \neq 1$, where $[(u_{\mathfrak{l}_i})] \in \mathcal{C}_k$ stands for the image of $u_{\mathfrak{l}_i} \in U_{\mathfrak{l}_i}$ under the composite of the natural maps

$$U_{\mathfrak{l}_i} \quad J_k \quad \mathcal{C}_k, \quad u_{\mathfrak{l}_i} \mapsto (u_{\mathfrak{l}_i}) \mapsto [(u_{\mathfrak{l}_i})].$$

Suppose that $\mathfrak{l}_1 \neq \mathfrak{l}_2$. Then we have

$$1 \neq (u_{\mathfrak{l}_1})(u_{\mathfrak{l}_2})^{-1} \in \overline{k^\times \prod_{\mathfrak{p}:\ \text{primes of } k} U_{\mathfrak{p}}^0}. \tag{4}$$

It follows from [1, Théorème 1] that for any given integer $m \geq 1$, there exists a finite set T_m of degree one primes of k such that $\mathfrak{l}_1, \mathfrak{l}_2 \notin T_m$ and

$$E_k \ni \varepsilon \equiv 1 \pmod{\prod_{\mathfrak{p} \in T_m} \mathfrak{p}} \Longrightarrow \varepsilon \in E_k^m$$

holds, E_k being the grobal unit group of k. Because $U_{\mathfrak{p}}^0 = 1$ for $\mathfrak{p} \in T_m$, we find that there exists an open neighberhood $U_k \supseteq H_m \ni (u_{\mathfrak{l}_1})(u_{\mathfrak{l}_2})^{-1}$, $U_k \subseteq J_k$ being the unit idele group of k, such that

$$H_m \cap k^\times \prod_{\mathfrak{p}:\ \text{primes of } k} U_{\mathfrak{p}}^0 \subseteq E_k^m \prod_{\mathfrak{p}:\ \text{primes of } k} U_{\mathfrak{p}}^0.$$

Hence, by (4), we see that for each $n \geq 1$, there exists $\varepsilon_n \in E_k$ and $w_{n,\mathfrak{l}_i} \in U^0_{\mathfrak{l}_i}$ such that

$$u_{\mathfrak{l}_1} \equiv \varepsilon_n^{\#(\mathcal{O}_{\mathfrak{l}_1}/\mathfrak{l}_1^n\mathcal{O}_{\mathfrak{l}_1})^\times} w_{n,\mathfrak{l}_1} \equiv w_{n,\mathfrak{l}_1} \pmod{\mathfrak{l}_1^n \mathcal{O}_{\mathfrak{l}_1}},$$

$\mathcal{O}_{\mathfrak{l}_1}$ being the integer ring of $k_{\mathfrak{l}_1}$, which implies $u_{\mathfrak{l}_1} \in U^0_{\mathfrak{l}_1}$ since $U^0_{\mathfrak{l}_1}$ is closed in $U_{\mathfrak{l}_1}$. This contradicts to $[(u_{\mathfrak{l}_1})] \neq 1$. Thus we conclude that $I_{\mathfrak{l}_1}(K/k) \cap I_{\mathfrak{l}_2}(K/k) \neq 1$ implies $\mathfrak{l}_1 = \mathfrak{l}_2$. □

Lemma 3. Let M be an intermediate field of K/k such that for each finite subextension F/k of M/k, there exist infinitely many degree one primes $\mathfrak{L}$ of F such that $\mu_l \subseteq M$, l being the rational prime below $\mathfrak{L}$. Then we have

$$\varprojlim_{k \subseteq F \subseteq M,\, [F:k]<\infty} E_F = 0,$$

where E_F denotes the global unit group of F and the projective limit is taken with respect to the norm maps.

Proof. It is enough to show that

$$\bigcap_{F \subseteq N \subseteq M,\ [N:F]<\infty} N_{N/F}(E_N) = 1$$

for each finite subextension F/k of M/k. Let $\mathfrak{L}$ be a degree one prime of F such that $\mu_l \subseteq M$, l being the rational prime below $\mathfrak{L}$, and $\mathfrak{L}$ is unramified in $F/\mathbb{Q}$. Then $F(\mu_l) \subseteq M$ and $N_{F(\mu_l)/F}(\varepsilon) \equiv 1 \pmod{\mathfrak{L}}$ holds for every $\varepsilon \in E_{F(\mu_l)}$. Since $F(\mu_l) \subseteq M$, we find that $\eta \equiv 1 \pmod{\mathfrak{L}}$ holds for any $\eta \in \bigcap_{F \subseteq N \subseteq M,\ [N:F]<\infty} N_{N/F}(E_N)$. Because there exists infinitely many such primes $\mathfrak{L}$, we conclude that $\eta = 1$ must hold. □

Lemma 4. Let p be an odd prime number and $\Delta = \langle \delta \rangle \subseteq \mathrm{Gal}(K/k)$ a subgroup of order p. Put

$$Y_\Delta^{(p)} := \mathrm{Gal}(L_p^{\mathrm{ab}}(K)/K^\Delta)/(\mathrm{Gal}(L_p^{\mathrm{ab}}(K)/K), \overline{\delta}),$$

where $L_p^{\mathrm{ab}}(K)/K$ is the maximal p-subextension of $L^{\mathrm{ab}}(K)/K$, and $\overline{\delta}$ is a lift of δ to $\mathrm{Gal}(L_p(K)/K^\Delta)$. Then

$$\mathrm{Tor}(Y_\Delta^{(p)}) \simeq \begin{cases} 0 & \text{if } \Delta \not\subseteq I_\mathfrak{l}(K/k) \text{ for any prime } \mathfrak{l} \text{ of } k, \\ \mathbb{F}_p[[\mathrm{Gal}(K/k)/D_\mathfrak{l}(K/k)]] & \text{if } \Delta \subseteq I_\mathfrak{l}(K/k) \text{ for some prime } \mathfrak{l} \text{ of } k, \end{cases}$$

as $\mathbb{F}_p[[\mathrm{Gal}(K/k)]]$-modules, where $\mathrm{Tor}(Y_\Delta^{(p)})$ means the torsion part of the pro-p abelian group $Y_\Delta^{(p)}$.

Proof. Let $M := L_p^{\mathrm{ab}}(K)^{(\mathrm{Gal}(L_p^{\mathrm{ab}}(K)/K), \overline{\delta})}$. Then M/K^Δ is the maximal abelian p-subextension of $L_p^{\mathrm{ab}}(K)/K^\Delta$, and $\mathrm{Gal}(K/k)$ acts on $Y_\Delta^{(p)} = \mathrm{Gal}(M/K^\Delta)$ via inner automorphisms of $\mathrm{Gal}(M/k)$.

Assume that $\Delta \not\subseteq I_\mathfrak{l}(K/k)$ for any prime $\mathfrak{l}$ of k. Then M is the maximal unramified abelian p-extension field over K^Δ since K/K^Δ is unramified.

Now we employ the following theorem:

Theorem D (Uchida[10])**.** For any integer $m \geq 1$ and prime number $l \equiv 1 \pmod{m}$, denote by $\mathbb{Q}(l,m)$ the subfield of the l-th cyclotomic field $\mathbb{Q}(\mu_l)$ such that $[\mathbb{Q}(\mu_l) : \mathbb{Q}(l,m)] = m$. We define $\mathbb{Q}^{(m)}$ to be the composite field of all the $\mathbb{Q}(l,m)$ for the primes $l \equiv 1 \pmod{m}$.

Let F a number field with $\mathbb{Q}^{(m)} \subseteq F$ for some $m \geq 1$. Furthermore we assume that F contains a subfield F_0 of finite degree over $\mathbb{Q}$ such that F is a subfield of the maximal nilpotent extension of F_0. Then the Galois group the maximal unramified pro-solvable extension over F is a free pro-solvable group of countably infinite rank.

It follows from Theorem D that $Y_\Delta^{(p)}$ is a free pro-p abelian group since $\mathbb{Q}^{(p)} \subseteq K^\Delta$ and K^Δ/k is abelian. Hence $\mathrm{Tor}(Y_\Delta^{(p)}) = 0$ in this case.

Assume that $\Delta \subseteq I_{\mathfrak{l}}(K/k)$ for a certain non-archimedean prime $\mathfrak{l}$ of k. Then such a prime $\mathfrak{l}$ is unique by Lemma 2, and the prime number l below $\mathfrak{l}$ satisfies $l \equiv 1 \pmod{p}$ by Lemma 1, especially, K/K^Δ is tamely ramified. We get the exact sequence

$$1 \longrightarrow \langle I_{\mathfrak{L}}(M/K^\Delta) \mid \mathfrak{L}|\mathfrak{l} \rangle \longrightarrow \mathrm{Gal}(M/K^\Delta) \longrightarrow \mathrm{Gal}(L_p^{\mathrm{ab}}(K^\Delta)/K^\Delta) \longrightarrow 1$$

of abelian pro-p-groups, where $\mathfrak{L}$ runs over all the primes of K^Δ lying over $\mathfrak{l}$. Here we note that exactly all the primes lying over $\mathfrak{l}$ ramify in M/K^Δ, and that $L^{\mathrm{ab}}(K^\Delta)K \subseteq M$ because M/K is the maximal unramified abelian p-extension which is abelian over K^Δ.

It follows from Theorem D that $\mathrm{Gal}(L^{\mathrm{ab}}(K^\Delta)/K^\Delta)$ is free pro-p abelian group since $\mathbb{Q}^{(p)} \subseteq K^\Delta$, hence the above exact sequence splits. Thetrefore we obtain

$$\mathrm{Tor}(Y_\Delta^{(p)}) = \langle I_{\mathfrak{L}}(M/K^\Delta) \mid \mathfrak{L}|\mathfrak{l} \rangle. \tag{5}$$

Denote by $U_{F,\mathfrak{L}}(p)$ be the pro-p-part of the local unit group at the prime $\mathfrak{L}$ of a number field F of finite degree. Define

$$\mathcal{U}_{K^\Delta,\mathfrak{l}}(p) := \varprojlim_{k \subseteq F \subseteq K^\Delta, [F:\mathbb{Q}] < \infty} \prod_{\mathfrak{L} \in S_{\mathfrak{l}}(F)} U_{F,\mathfrak{L}}(p) \tag{6}$$

to be the projective limit of the pro-p-part of the semi-local unit groups of F at $\mathfrak{l}$ with respect to the norm maps, where $S_{\mathfrak{l}}(F)$ stands for the set of all the primes of F lying over $\mathfrak{l}$ and F runs over all the subfields of K^Δ with $k \subseteq F$ and $[F:\mathbb{Q}] < \infty$.

Denote by $L_{p,\{\mathfrak{l}\}}^{\mathrm{ab}}(K^\Delta)/K^\Delta$ the maximal abelian p-extension unramified outside $\mathfrak{l}$. Then class field theory gives the exact sequence

$$\varprojlim_{F \subseteq K^\Delta, [F:\mathbb{Q}] < \infty} E_F \longrightarrow \mathcal{U}_{K^\Delta,\mathfrak{l}}(p) \longrightarrow \mathrm{Gal}(L_{p,\{\mathfrak{l}\}}^{\mathrm{ab}}(K^\Delta)/L_p^{\mathrm{ab}}(K^\Delta)) \longrightarrow 1.$$

Here it follows from Lemma 3 that $\varprojlim_{F \subseteq K^\Delta, [F:\mathbb{Q}] < \infty} E_F = 0$. Hence we get the isomorphism

$$\mathcal{U}_{K^\Delta,\mathfrak{l}}(p) \simeq \mathrm{Gal}(L_{p,\{\mathfrak{l}\}}^{\mathrm{ab}}(K^\Delta)/L_p^{\mathrm{ab}}(K^\Delta)). \tag{7}$$

On the other hand, we see that

$$L_p^{\mathrm{ab}}(K^\Delta) \subseteq M \subseteq L_{p,\{\mathfrak{l}\}}^{\mathrm{ab}}(K^\Delta),$$

and $M/L_p^{\mathrm{ab}}(K^\Delta)$ is the maximal subextenion of $L_{p,\{\mathfrak{l}\}}^{\mathrm{ab}}(K^\Delta)/L_p^{\mathrm{ab}}(K^\Delta)$ such that every ramified prime in $M/L_p(K^\Delta)$ has ramification index p. Hence we see that

$$\text{(8)}\qquad \mathrm{Tor}(Y_\Delta^{(p)}) = \langle I_{\mathfrak{L}}(M/K^\Delta) \mid \mathfrak{L}|\mathfrak{l}\rangle = \mathrm{Gal}(M/L_p^{\mathrm{ab}}(K^\Delta)) \simeq \mathcal{U}_{K^\Delta,\mathfrak{l}}(p)/p$$

by using (5) and (7).

$U_{F,\mathfrak{L}}(p)/p$ is a cyclic group of oder p on which $D_{\mathfrak{l}}(K/k)$ acts on trivially since $N(\mathfrak{l}) \equiv 1 \pmod p$. Hence it follows from (6) that

$$\mathcal{U}_{K^\Delta,\mathfrak{l}}(p)/p \simeq \mathbb{F}_p[[\mathrm{Gal}(\mathrm{Gal}(K^\Delta/k)/D_{\mathfrak{l}}(K^\Delta/k))]] \simeq \mathbb{F}_p[[\mathrm{Gal}(K/k)/D_{\mathfrak{l}}(K/k))]]$$

as $\mathrm{Gal}(K/k)$-modules, noting that $\Delta \subseteq D_{\mathfrak{l}}(K/k)$. Thus the assetion of the lemma follows from (8). $\square$

Proof of Proposition 2 Let $N/\mathbb{Q}$ be the Galois closure of $k_1k_2/\mathbb{Q}$. We choose an odd prime number p such that $\mathbb{Q}(\mu_p) \cap N = \mathbb{Q}$. For any given prime number $q \neq p$ unramified in N, there exists a prime number l such that $[l, N/\mathbb{Q}] = [q, N/\mathbb{Q}]$, $l \equiv 1 \pmod p$, and l is unramified in k_1k_2 by the Čebotarev density theorem, where $[r, N/\mathbb{Q}]$ stands for the Frobenius conjugacy class of r in $\mathrm{Gal}(N/\mathbb{Q})$ for any prime number r. Then we have

$$g_{k_1}(q) = g_{k_1}(l),\ g_{k_2}(q) = g_{k_2}(l).$$

Hence if $g_{k_1}(l) = g_{k_2}(l)$ holds for all the prime numbers $l \equiv 1 \pmod p$ unramified in $k_1k_2/\mathbb{Q}$, then $g_{k_1}(q) = g_{k_2}(q)$ for all but finitely many prime numbers q, which in turn implies $k_1 \approx k_2$ by Theorem C.

We write k and K for k_i and K_i, respectively. Let $l \equiv 1 \pmod p$ be a prime number unramified in $k/\mathbb{Q}$ and $\mathfrak{l}$ a prime of k lying over l. Then it follows from Lamma 1 that $I_{\mathfrak{l}}(K/k)$ has the subgroup $\Delta_{\mathfrak{l}}$ of order p. Then it follows from Lemma 4 that

(9)

$$\mathrm{Stab}_{\mathrm{Gal}(K/k)}(\mathrm{Tor}(Y_{\Delta_{\mathfrak{l}}}^{(p)})) := \{\alpha \in \mathrm{Gal}(K/k) \mid \alpha y = y \text{ for all } y \in Y_{\Delta_{\mathfrak{l}}}\} = D_{\mathfrak{l}}(K/k).$$

We note that the $\mathrm{Gal}(K/k)$-module structure of $Y_\Delta^{(p)}$ is determined only by the group structure of $\mathrm{Gal}(L^{\mathrm{ab}}(K)/k)$ and the subgroup $\Delta \subseteq \mathrm{Gal}(K/k)$. The prime number l is charactelized from the structure of $D_{\mathfrak{l}}(K/k)$ by the unique prime number l such that $\mathrm{rank}_{\mathbb{Z}_l} D_{\mathfrak{l}}(K/k) = 2$ by Lemma 1. Hence we find from Lemmas 2, 4 and (9) that

$$g_k(l)$$
$$= \#\{\Delta \subseteq \mathrm{Gal}(K/k) \mid \Delta \simeq \mathbb{Z}/p,\ \mathrm{Tor}(Y_\Delta^{(p)}) \neq 0,\ \mathrm{rank}_{\mathbb{Z}_l}\mathrm{Stab}_{\mathrm{Gal}(K/k)}(\mathrm{Tor}(Y_\Delta^{(p)})) = 2\}$$

for every prime number $l \equiv 1 \pmod p$ which is unramified in $k/\mathbb{Q}$. This means $g_k(l)$ is determined by the group structure of $\mathrm{Gal}(L^{\mathrm{ab}}(K)/k)$.

Therefore, it follows from the isomorphism $\mathrm{Gal}(L^{\mathrm{ab}}(K_1)/k_1) \simeq \mathrm{Gal}(L^{\mathrm{ab}}(K_2)/k_2)$ that $g_{k_1}(l) = g_{k_2}(l)$ holds for every prime number $l \equiv 1 \pmod p$, unramified in $k_1k_2/\mathbb{Q}$, from which we deduce $g_{k_1}(q) = g_{k_2}(q)$ for all but finitely many prime numbers q as we have seen.

Now, by using Theorem C, we conclude that $k_1 \approx k_2$. Thus we have proved Proposition 2, from which Proposition 1 follows. $\square$

3. Construction of field isomorphisms

Let k_i be a number field of finite degree, and put $\tilde{k_i} = k_i(\mu_\infty)$ for $i = 1, 2$. Denote by L_i the maximal unramified extension field of $\tilde{k}_i$.

In this section, assuming the existence of an isomorphism $\varphi : \mathrm{Gal}(L_1/k_1) \simeq \mathrm{Gal}(L_2/k_2)$ of pro-finite groups, we construct a field isomorphism

$$\tau : L_1 \simeq L_2$$

such that $\tau(k_1) = k_2$ and $\varphi(x) = \tau x \tau^{-1}$ for every $x \in \mathrm{Gal}(L_1/k_1)$. We are based on Proposition 1 given in the precedent section and the method of Uchida[9] to construct a field isomorphism τ.

We first recall the following facts on arithmetically equivalence:

Theorem E. (cf.[3, Theorems (1.3),(1.4),(1.6)]) Let F_1 and F_2 be number fields of finite degree such that $F_1 \approx F_2$. Then the followings holds:

(1) F_1 and F_2 has the common Galois closure over $\mathbb{Q}$.

(2) For any finite Galois extension $F_0/\mathbb{Q}$, we have $F_0F_1 \approx F_0F_2$.

(3) Let $N/\mathbb{Q}$ be a finite Galois extension with $F_1F_2 \subseteq N$. Then there exists a bijection

$$\gamma : \mathrm{Gal}(N/F_1) \longrightarrow \mathrm{Gal}(N/F_2)$$

such that $\gamma(x) = \tau_x x \tau_x^{-1}$ for each $x \in \mathrm{Gal}(N/F_1)$ with some $\tau_x \in \mathrm{Gal}(N/\mathbb{Q})$.

Let K_1/k_1 be any finite Galois subextension of L_1/k_1, and K_2 is the corresponding intermediate field of L_2/k_2 by φ, namely, $K_2 = L_2^{\varphi(\mathrm{Gal}(L_1/K_1))}$. Then K_2/k_2 is also a Galois extension and φ induces the isomorphism

$$\varphi_{K_1} : \mathrm{Gal}(K_1/k_1) \simeq \mathrm{Gal}(K_2/k_2).$$

Let $K/\mathbb{Q}$ be a finite Galois extension containing K_1K_2 and put $G := \mathrm{Gal}(K/k)$

Lemma 5. Let p be a prime number with $p \nmid \#G$ and r a positive integer. Then there exists a Galois extension $M/\mathbb{Q}$ containing K such that $\mathrm{Gal}(M/K) \simeq \mathbb{F}_p[G]^{\oplus r}$ as G-modules when we define the G-action on $\mathrm{Gal}(M/K)$ via inner automorphisms of $\mathrm{Gal}(M/\mathbb{Q})$, and that the maximal abelian p-subextension M_1/K_1 of M/K_1 is a subextension of L_1/K_1.

Proof. By the Čebotarev density theorem, there exist degree one principal prime ideals (Λ_i) $(1 \leq i \leq r)$ of $K(\mu_p)$ such that $\Lambda_i \equiv 1 \pmod{p^2}$ and totally positive, and that (Λ_i)'s are unramified in $K/\mathbb{Q}$ and lying over distinct rational primes l_i's with $l_i \equiv 1 \pmod p$. Define M/K to be the maximal abelian p-subextension of $M' := K(\mu_p, \sqrt[p]{\sigma\Lambda_i} \,|\, \sigma \in \mathrm{Gal}(K(\mu_p)/\mathbb{Q}),\ 1 \leq i \leq r)/K$. Then we have

$$\begin{aligned} \mathrm{Gal}(M'/K(\mu_p)) &\simeq \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/\mathbb{Q})]^{\oplus r}, \mu_p) \\ &\simeq \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/\mathbb{Q})](-1), \mathbb{F}_p)^{\oplus r} \end{aligned}$$

as $\mathrm{Gal}(K(\mu_p)/\mathbb{Q})$-modules by Kummer duality, (-1) denoting the Tate twist. Hence we see that

$$\begin{aligned} \mathrm{Gal}(M/K) &\simeq \mathrm{Gal}(M(\mu_p)/K(\mu_p)) \simeq \mathrm{Gal}(M'/K(\mu_p))_{\mathrm{Gal}(K(\mu_p)/K)} \\ &\simeq \mathrm{Hom}_{\mathbb{F}_p}((\mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/\mathbb{Q})](-1))^{\mathrm{Gal}(K(\mu_p)/K)}, \mathbb{F}_p)^{\oplus r}. \end{aligned}$$

Here,

$$(\mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/\mathbb{Q})](-1))^{\mathrm{Gal}(K(\mu_p)/K)} = \mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/\mathbb{Q})]\varepsilon \simeq \mathbb{F}_p[G]$$

as G-modules holds for

$$\varepsilon := \sum_{\delta \in \mathrm{Gal}(K(\mu_p)/K)} \chi(\delta)\delta^{-1} \in \mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/\mathbb{Q})](-1),$$

where $\chi : \mathrm{Gal}(K(\mu_p)/K) \longrightarrow \mathbb{F}_p^{\times}$ stands for the cyclotomic character.

Then we see that $\mathrm{Gal}(M/K) \simeq \mathbb{F}_p[G]^{\oplus r}$ as G-modules, and that the ramified primes in M/K are exactly the primes lying over l_i's whose ramification indexes equal p. Hence, if we denote by M_1/K_1 the maximal abelian p-subextension of M/K_1, then the ramified primes in M_1/K_1 are lying over l_i's, whose ramification indexes are p because $p \nmid [K : K_1]$. Since the prime l_i is unramified in $k_1/\mathbb{Q}$ and $l_i \equiv 1 \pmod p$, the primes lying over l_i's are unramified in $M_1(\mu_{l_i})/K_1(\mu_{l_i})$. Therefore we see that $M_1(\mu_\infty)/K_1(\mu_\infty)$ is unramified abelian p-extension. Because $K_1(\mu_\infty) \subseteq L_1$, we conclude that $M_1 \subseteq L_1$. □

Let $H_i := \mathrm{Gal}(K_i/k_i)$ $(i = 1, 2)$ and M/K an extension given by Lemma 5 such that

$$A := \mathrm{Gal}(M/K) \simeq \bigoplus_{h \in H_1} \mathbb{F}_p[G]u_h, \tag{10}$$

as G-modules, where the right hand side is the free $\mathbb{F}_p[G]$-modules with basis $\{u_h \,|\, h \in H_1\}$.

For each $h \in H_1$, let M_h/K be the subextension of M/K such that

$$\mathrm{Gal}(M/M_h) \simeq \bigoplus_{h \neq h' \in H_1} \mathbb{F}_p[G]u_{h'}$$

under isomorphism (10). We note that $M_h/\mathbb{Q}$ is a Galois extension.

Define $M_{1,h}/K_1$ to be the maximal abelian p-subextension of M_h/K_1 which is abelian over $K_1^{\langle h \rangle}$ for each $h \in H_1$. By our choice of M, we see that $M_{1,h} \subseteq L_1$. Let $M_{2,h}$ be the field coresponding to $M_{1,h}$ by φ_{K_1} for each $h \in H_1$. Then it follows from Proposition 1 that $M_{1,h} \approx M_{2,h}$. This means $M_{2,h}$ is a subfield of the Galois closure of $M_{1,h}$ over $\mathbb{Q}$ by Theorem E (1), which is a subfield of M_h since $M_h/\mathbb{Q}$ is Galois. Hence we see that $K_2 \subseteq M_{2,h} \subseteq M_h$ and that φ induces $\mathrm{Gal}(M_{2,h}/K_2) \simeq \mathrm{Gal}(M_{1,h}/K_1)$, which are abelian p-groups, and $\mathrm{Gal}(M_{2,h}/K_2^{\langle \varphi_{K_1}(h) \rangle}) \simeq \mathrm{Gal}(M_{1,h}/K_1^{\langle h \rangle})$, which is abelian.

Furthemere, for any abelian p-subextension F_2/K_2 of M_h/K_2 which is abelian over $K_2^{\langle \varphi_{K_1}(h) \rangle}$, we see that the corresponding field F_1 to F_2 by φ^{-1} is an intermediate field of M_h/K_1 by a similar argument above, which is p-abelian over K_1, and $\mathrm{Gal}(F_1/K_1^{\langle h \rangle}) \simeq \mathrm{Gal}(F_2/K_2^{\langle \varphi_{K_1}(h) \rangle})$ is abelian. Hence we have $F_1 \subseteq M_{1,h}$, which implies $F_2 \subseteq M_{2,h}$. Therefore we conclude that $M_{2,h}/K_2$ is the maximal abelian p-subextension of M_h/K_2 which is abelian over $K_2^{\langle \varphi_{K_1}(h) \rangle}$.

Lemma 6. (1) We have

$$K \prod_{h \in H_1} M_{1,h} \approx K \prod_{h \in H_1} M_{2,h}.$$

(2) Let $N_i := \mathrm{Gal}(K/K_i)$ $(i = 1, 2)$. Then we have

$$A_1 := \mathrm{Gal}(M/K \prod_{h \in H_1} M_{1,h}) \simeq \bigoplus_{h \in H_1} (I_{N_1} + (\overline{h} - 1)\mathbb{F}_p[G])u_h,$$
$$A_2 := \mathrm{Gal}(M/K \prod_{h \in H_1} M_{2,h}) \simeq \bigoplus_{h \in H_1} (I_{N_2} + (\overline{\varphi_{K_1}(h)} - 1)\mathbb{F}_p[G])u_h,$$

where $I_{N_i} := \sum_{n \in N_i}(n-1)\mathbb{F}_p[G]$, $\overline{h} \in \mathrm{Gal}(K/k_1)$ and $\overline{\varphi_{K_1}(h)} \in \mathrm{Gal}(K/k_2)$ are lifts of h and $\varphi_{K_1}(h)$, respectively.

Proof. (1) Because $M_{2,h}$ is corresponding to $M_{1,h}$ by φ for each $h \in H_1$, the coposite field $\prod_{h \in H_1} M_{2,h}$ is corresponding to $\prod_{h \in H_1} M_{1,h}$ by φ. Then it follows from Proposition 1 that $\prod_{h \in H_1} M_{1,h} \approx \prod_{h \in H_1} M_{2,h}$. Hence the assertion follows from Theorem E(2) since $K/\mathbb{Q}$ is Galois.

(2) Recall that $M_{1,h}/K_1$ and $M_{2,h}/K_2$ are the maximal abelian p-subextensions of M_h/K_1 and M_h/K_2 such that h and $\varphi_{K_1}(h)$ act trivially on $\mathrm{Gal}(M_{1,h}/K_1)$ and $\mathrm{Gal}(M_{2,h}/K_2)$, respectively. Hence we find that N_1 and $\overline{h}$ acts trivially on $\mathrm{Gal}(M/K)/\mathrm{Gal}(M/KM_{1,h}) \simeq \mathrm{Gal}(KM_{1,h}/K) \simeq \mathrm{Gal}(M_{1,h}/K_1)$, which implies

$$J_h := \bigoplus_{h \neq h' \in H_1} \mathbb{F}_p[G]u_{h'} \oplus (I_{N_1} + (\overline{h} - 1)\mathbb{F}_p[G])u_h \subseteq \mathrm{Gal}(M/KM_{1,h})$$

It follows from the definition of J_h that $\mathrm{Gal}(M^{J_h}/K_1)$ has a direct factor naturally isomorphic to $N_1 = \mathrm{Gal}(K/K_1)$ since $p \nmid \#N_1$. Hence there is an abelian p-subextension F/K_1 such that $KF = M^{j_h}$ and $F \cap K = K_1$, and we see that $F/K_1^{\langle h \rangle}$ is abelian by the definition of J_h. This means $F \subseteq M_{1,h}$ and $\mathrm{Gal}(M/KM_{1,h}) \subseteq J_h$. Thus we conclude that $J_h = \mathrm{Gal}(M/KM_{1,h})$ and

$$\mathrm{Gal}(M/K \prod_{h \in H_1} M_{1,h}) = \bigcap_{h \in H_1} J_h = \bigoplus_{h \in H_1} (I_{N_1} + (\overline{h} - 1)\mathbb{F}_p[G])u_h.$$

We obtain the assertion also for A_2 by the similar way. □

Lemma 7. There exists $\tau_0 \in G$ and $m_h \in \mathbb{Z}$ for each $h \in H_1$ such that $\tau_0 N_1 \tau_0^{-1} = N_2$, and

$$(\tau_0 \overline{h} \tau_0^{-1})|_{K_2} = \varphi_{K_1}(h)^{m_h} \in \mathrm{Gal}(K_2/k_2)$$

holds for every $h \in H_1$, where $\overline{h} \in \mathrm{Gal}(K/k_1)$ is a lift of h.

Proof. By using Lemma 6 (2), we define

$$\alpha := \sum_{n \in N_1}(n-1)u_1 + \sum_{h \in H_1 - \{1\}} (\overline{h} - 1)u_h \in A_1.$$

Then it follows from Lemma 6 (1) and Theorem E (3) that there exists $\tau_0 \in G$ such that

$$\tau_0 \cdot \alpha \in A_2, \tag{11}$$

where " $\cdot$ " denotes the G-action on A. We derive from (11) and Lemma 6 (2) that

$$\tau_0 \sum_{n \in N_1}(n-1) \in I_{N_2}, \tag{12}$$

and

$$\tau_0(\overline{h}-1) \in I_{N_2} + (\overline{\varphi_{K_1}(h)}-1)\mathbb{F}_p[G], \tag{13}$$

for $h \in H_1 - \{1\}$.

By operating $T_{N_2} := \sum_{n\in N_2} n \in \mathbb{F}_p[G]$ on (12), we obtain the equality

$$T_{N_2}\tau_0 \sum_{n\in N_1} n = (\#N_1)T_{N_2}\tau_0,$$

from which we see that for each $n_1 \in N_1$, there exists $n_2 \in N_2$ such that $\tau_0 n_1 = n_2\tau_0$. This implies $\tau_0 N_1 \tau_0^{-1} \subseteq N_2$. Since $K_1 \approx K_2$ by Proposition 1, we find that $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$ by Theorem E (3), which implies $\#N_1 = \#N_2$. Thus we conclude that $\tau_0 N_1 \tau_0^{-1} = N_2$.

By operating $T := \sum_{t\in\langle N_2, \overline{\varphi_{K_1}(h)}\rangle} t \in \mathbb{F}_p[G]$ on (13), we get

$$T\tau_0\overline{h} = T\tau_0,$$

from which we see that there exists $t \in \langle N_2, \overline{\varphi_{K_1}(h)}\rangle$ such that $\tau_0\overline{h} = t\tau_0$. Then we conclude that

$$(\tau_0\overline{h}\tau_0^{-1})N_2 = \overline{\varphi_{K_1}(h)}^{m_h}N_2,$$

which means

$$\tau_0\overline{h}\tau_0^{-1}|_{K_2} = \varphi_{K_1}(h)^{m_h},$$

for a certain $m_h \in \mathbb{Z}$ for each $h \in H_1$. □

We note that $\mathrm{Gal}(K/\tau_0(k_1)) = \tau_0\mathrm{Gal}(K/k_1)\tau_0^{-1} \subseteq \mathrm{Gal}(K/k_2)$ holds by the above Lemma, which in turn implies

$$\tau_0(k_1) = k_2,\ \tau_0\mathrm{Gal}(K/k_1)\tau_0^{-1} = \mathrm{Gal}(K/k_2), \tag{14}$$

because $[K : k_1] = [K : k_2]$ holds by $k_1 \approx k_2$ and Theorem E. Hence $k_1 \simeq k_2$ holds.

In what follows we will show that the assertion of Lemma 7 holds for $m_h = 1$ in fact.

Lemma 8. Let K_1/k_1 be any finite Galois subextension of L_1/k_1 and p a prime number. Then there exists a Galois subextension M_1/k_1 of L_1/k_1 with $K_1 \subseteq M_1$ such that

$$\mathrm{Gal}(M_1/K_1) \simeq \mathbb{F}_p[H_1]$$

as $H_1 = \mathrm{Gal}(K_1/k_1)$-modules, where the H_1-acsion on $\mathrm{Gal}(M_1/K_1)$ is defined via inner automorphisms of $\mathrm{Gal}(M_1/k_1)$.

Proof. We can show the existence of M_1 in a similar way to the proof of Lemma 5. Choose a principal degree one prime ideal (Λ) of $K_1(\mu_p)$ such that $\Lambda \equiv 1 \pmod{p^2}$ and totally positive, and that the rational prime l below (Λ) is unramified in $k_1/\mathbb{Q}$. Then the maximal abelian p-subextension M_1/K_1 of $K_1(\mu_p)(\sqrt[p]{\sigma\Lambda} \mid \sigma \in \mathrm{Gal}(K_1(\mu_p)/k_1))/K_1$ satisfies our requirement. □

Now we will give the following crucial proposition:

Proposition 3. Let K_1/k_1 be a finite Galois subextension of L_1/k_1, and $K_2 \subseteq L_2$ the corresponding field to K_1 by φ. Then there exists a field isomorphism $\tau_{K_1} : K_1 \simeq K_2$ such that $\tau_{K_1}(k_1) = k_2$ and

$$\varphi_{K_1}(x) = \tau_{K_1} x \tau_{K_1}^{-1}$$

for every $x \in \mathrm{Gal}(K_1/k_1)$.

Proof. M_1/K_1 be a subextension of L_1/K_1 given by Lemma 8. Let K_2 and M_2 be the fields corresponding to K_1 and M_1 by φ, respectively. Then φ induces the isomorphism

$$\varphi_{M_1} : \mathrm{Gal}(M_1/k_1) \simeq \mathrm{Gal}(M_2/k_2) \tag{15}$$

with $\varphi_{M_2}(\mathrm{Gal}(M_1/K_1)) = \mathrm{Gal}(M_2/K_2)$. Let $M/\mathbb{Q}$ be a finite Galois extension containing M_1M_2. Then by applying Lemma 7 to M_1, M_2, and M as K_1, K_2, and K, respectively, we get $\tau_0 \in \mathrm{Gal}(M/\mathbb{Q})$ such that

$$\tau_0 \mathrm{Gal}(M/M_1)\tau_0^{-1} = \mathrm{Gal}(M/M_2) \tag{16}$$

and

$$(\tau_0 \overline{x} \tau_0^{-1})|_{M_2} = \varphi_{M_1}(x)^{m_x} \tag{17}$$

holds for each $x \in \mathrm{Gal}(M_1/k_1)$ with a certain $m_x \in \mathbb{Z}$, where $\overline{x} \in \mathrm{Gal}(M/k_1)$ is a lift of x. Here we note that $\tau_0 \mathrm{Gal}(M/k_1)\tau_0^{-1} = \mathrm{Gal}(M/k_2)$ holds by (14). Put $A := \mathrm{Gal}(M_1/K_1) = \mathbb{F}_p[\mathrm{Gal}(K_1/k_1)]u$, u being a basis of the free $\mathbb{F}_p[\mathrm{Gal}(K_1/k_1)]$-module A. Then we have

$$\mathrm{Gal}(M_2/K_2) = \varphi_{M_1}(\mathrm{Gal}(M_1/K_1)) = \mathbb{F}_p[\mathrm{Gal}(K_2/k_2)]\varphi_{M_1}(u) \simeq \mathbb{F}_p[\mathrm{Gal}(K_2/k_2)],$$

as $\mathrm{Gal}(K_2/k_2)$-modules by (15).

Let $x \in \mathrm{Gal}(M_1/k_1)$ be any element. Then we have

$$\begin{aligned} &\varphi_{M_1}(xux^{-1})^{m_u} \\ &= \varphi_{M_1}(x)\varphi_{M_1}(u)^{m_u}\varphi_{M_1}(x)^{-1} \\ &= \varphi_{M_1}(x)\left((\tau_0\overline{u}\tau_0^{-1})|_{M_2}\right)\varphi_{M_1}(x)^{-1}, \end{aligned} \tag{18}$$

where $u \in A$ is the free basis, by (17).

We also get

$$\begin{aligned} &\varphi_{M_1}(xux^{-1})^{m_{xux^{-1}}} \\ &= \left(\tau_0(\overline{xux^{-1}})\tau_0^{-1}\right)|_{M_2} \\ &= (\tau_0\overline{x}\tau_0^{-1})|_{M_2}(\tau_0\overline{u}\tau_0^{-1})|_{M_2}(\tau_0 x\tau_0^{-1})^{-1}|_{M_2} \end{aligned} \tag{19}$$

Because we have $\tau_0\overline{u}\tau_0^{-1}|_{M_2} \neq 1$ by (16) and $\varphi_{M_1}(xux^{-1}) \in \mathrm{Gal}(M_2/K_2) \simeq \mathbb{F}_p[\mathrm{Gal}(K_2/k_2)]$, we see that m_u and $m_{xux^{-1}}$ is prime to p by (18) and (19). Furthermore, since we have $\varphi_{M_1}(u)^{m_u} = (\tau_0\overline{u}\tau_0^{-1})|_{M_2}$ from (17), and $p \nmid m_u$. we see that

$$(\tau_0\overline{u}\tau_0^{-1})|_{M_2} \in \mathrm{Gal}(M_2/K_2) = \mathbb{F}_p[\mathrm{Gal}(K_2/k_2)](\varphi_{M_1}(u))$$

is a free $\mathbb{F}_p[\mathrm{Gal}(K_2/k_2)]$-basis of $\mathrm{Gal}(M_2/K_2)$.

We derive from (18) and (19) that

$$m_{xux^{-1}}\varphi_{M_1}(x)|_{K_2} \cdot (\tau_0\overline{u}\tau_0^{-1})|_{M_2} = m_u(\tau_0\overline{x}\tau_0^{-1})|_{K_2} \cdot (\tau_0\overline{u}\tau_0^{-1})_{M_2} \in \mathrm{Gal}(M_2/K_2),$$

where " $\cdot$ " stands for the $\mathbb{F}_p[\mathrm{Gal}(K_2/k_2)]$-action on $\mathrm{Gal}(M_2/K_2)$.

Because $(\tau_0\overline{u}\tau_0^{-1})_{M_2} \in \mathrm{Gal}(M_2/K_2) \simeq \mathbb{F}_p[\mathrm{Gal}(K_2/k_2)]$ is a free $\mathbb{F}_p[\mathrm{Gal}(K_2/k_2)]$-basis of $\mathrm{Gal}(M_2/K_2)$ and $p \nmid m_u m_{xux^{-1}}$, we conclude that

$$\varphi_{K_1}(x|_{K_1}) = \varphi_{M_1}(x)|_{K_2} = (\tau_0\overline{x}\tau_0^{-1})|_{K_2} \in \mathrm{Gal}(K_2/k_2) \tag{20}$$

for every $x \in \mathrm{Gal}(M_1/k_1)$.

It follows from (20) that $\tau_0 \mathrm{Gal}(M/K_1)\tau_0^{-1} \subseteq \mathrm{Gal}(M/K_2)$, from which we have

$$\tau_0 \mathrm{Gal}(M/K_1)\tau_0^{-1} = \mathrm{Gal}(M/K_2),$$

since $\#\mathrm{Gal}(M/K_1) = \#\mathrm{Gal}(M/K_2)$ by Proposition 1 and Theorem E (3). This means $\tau_0(K_1) = K_2$. Furthermore, $\tau_0(k_1) = k_2$ also holds by (14).

Now we define the field isomorphism $\tau_{K_1} : K_1 \simeq K_2$ by $\tau_{K_1}(\alpha) := \tau_0(\alpha)$ for $\alpha \in K_1$. Then $\tau_{K_1}(k_1) = k_2$ and

$$\varphi_{K_1}(x) = \tau_{K_1} x \tau_{K_1}^{-1}$$

for every $x \in \mathrm{Gal}(K_1/k_1)$ holds by (20). This completes the proof of the proposition. □

4. Proof of Theorem 1

Now we will giva a proof of Theorem 1. Let k_i be number field of finite degree and L_i the maximal unramified extension of $\tilde{k_i} = k_i(\mu_\infty)$ $(i = 1, 2)$. Assume that

$$\varphi : \mathrm{Gal}(L_1/k_1) \simeq \mathrm{Gal}(L_2/k_2)$$

is an isomorphism of pro-finite groups. We will show that there exists the unique field isomorphism

$$\tau : L_1 \simeq L_2$$

such that

$$\tau(k_1) = k_2, \quad \varphi(x) = \tau x \tau^{-1} \tag{21}$$

holds for every $x \in \mathrm{Gal}(L_1/k_1)$. This implies the assertion of Theorem 1.

For a finite Galois subextension K_1/k_1 of L_1/k_1, let K_2 be the intermediate field of L_2/k_2 corresponding to K_1 by φ, and define T_{K_1} to be the set of all the field isomorphisms

$$\tau_{K_1} : K_1 \simeq K_2$$

such that

$$\tau_{K_1}(k_1) = k_2, \quad \varphi_{K_1}(x) = \tau_{K_1} x \tau_{K_1}^{-1} \tag{22}$$

holds for every $x \in \mathrm{Gal}(K_1/k_1)$, where $\varphi_{K_1} : \mathrm{Gal}(K_1/k_1) \simeq \mathrm{Gal}(K_2/k_1)$ is the isomorphism inducedc by φ.

Then it follows from Proposition 3 that $T_{K_1} \neq \emptyset$ for each K_1. Furhermore, if $k_1 \subseteq K_1 \subseteq K_1' \subseteq L_1$ are inermediate fields finite Galois over k_1, we obtain the map

$$T_{K_1'} \longrightarrow T_{K_1}$$

by $\tau_{K_1'} \mapsto \tau_{K_1'}|_{K_1}$. Since T_{K_1} is a non-empty finite set, we see that the projective limit T of T_{K_1}'s with respect to the above maps is not empty, where K_1 runs over all the intermediate fields of L_1/k_1 such that K_1/k_1 is finite Galois. Take $(\tau_{K_1})_{K_1} \in T$ and define the map

$$\tau : L_1 \longrightarrow L_2$$

by $\tau(\alpha) := \tau_{K_1}(\alpha)$ for each $\alpha \in L_1$ and finite Galois subextension K_1/k_1 of L_1/k_1 with $\alpha \in K_1$. We see that τ is a well-defined field isomorphism $L_1 \simeq L_2$ and satisfies our requirement (21) by (22). Thus we have proved the existence of $\tau : L_1 \simeq L_2$ with (21).

Finally we will show the uniqness of τ with (21) in what follows. We need the following:

Lemma 9. Let $k_0 \subseteq k_1$ be a subfield such that L_1/k_0 is a Galois extension. Then the centralizer $Z_{\mathrm{Gal}(L_1/k_0)}(\mathrm{Gal}(L_1/k_1))$ of $\mathrm{Gal}(L_1/k_1)$ in $\mathrm{Gal}(L_1/k_0)$ is trivial.

Proof. Assume that $z \in Z_{\mathrm{Gal}(L_1/k_0)}(\mathrm{Gal}(L_1/k_1))$. Let K_1/k_0 be a finite Galois subextension of L_1/k_0 By a similar way to the proof of Lemma 8, we see that there exists finite Galois subextension M_1/k_0 of L_1/k_0 containing K_1 such that $\mathrm{Gal}(M_1/K_1) \simeq \mathbb{F}_p[\mathrm{Gal}(K_1/k_0)]$ as $\mathrm{Gal}(K_1/k_0)$-modules, where the $\mathrm{Gal}(K_1/k_0)$-action on $\mathrm{Gal}(M_1/K_1)$ is given via inner automorphisms of $\mathrm{Gal}(M_1/k_0)$. Then $z|_{K_1} \in \mathrm{Gal}(K_1/k_0)$ acts on $\mathrm{Gal}(M_1/K_1)$ trivially, which implies $z|_{K_1} = 1$ since the $\mathrm{Gal}(K_1/k_0)$-action on $\mathrm{Gal}(M_1/K_1)$ is faithful. Because K_1 can be arbitral finite Galois subextension of L_1/k_0, we conclude that $z = 1$. $\square$

Assume taht $\tau_1, \tau_2 : L_1 \simeq L_2$ are field isomorphisms satisfying (21) for $\tau = \tau_1, \tau_2$. Put $z := \tau_1^{-1}\tau_2 \in \mathrm{Gal}(L_1/k_0)$, where k_0 be the minimal subfield of L_1 such that L_1/k_0 is Galois. Then we have

$$zxz^{-1} = \tau_1^{-1}(\tau_2 x \tau_2^{-1})\tau_1 = \tau_1^{-1}\varphi(x)\tau_1 = \varphi^{-1}\varphi(x) = x$$

for any $x \in \mathrm{Gal}(L_1/k_1)$ by our assumption. Hence we conclude that

$$z \in Z_{\mathrm{Gal}(L_1/k_0)}(\mathrm{Gal}(L_1/k_1)) = 1$$

by Lemma 9, which implies $\tau_1 = \tau_2$. Thus we have shown the uniqueness of τ with (21). This completes the proof of Theorem 1. $\square$

5. Remarks

1. In the case of a curve C over a finite field $\mathbb{F}$, it is known that $\mathrm{Gal}(L(C)/\overline{\mathbb{F}}(C))$ is a characteristic subgroup of $\mathrm{Gal}(L(C)/\mathbb{F}(C))$ (see [8, Proposition(3.3)]). Furthermore, for every $\varphi \in \mathrm{Aut}(\mathrm{Gal}(L(C)/F(C)))$, the induced automorphism of $G_{\mathbb{F}} \simeq \mathrm{Gal}(\overline{\mathbb{F}}(C)/\mathbb{F}(C))$ by φ is the identity (see [8, Proposition(3.4)]).

In the case of a number field k, analogous assertions also hold, namely, it follows from Theorem 1 that $\mathrm{Gal}(L(\tilde{k})/\tilde{k})$ is a characteristic subgroup of $\mathrm{Gal}(L(\tilde{k})/k)$ and that for every $\varphi \in \mathrm{Aut}(\mathrm{Gal}(L(\tilde{k})/k))$, the induced automorphism of $\mathrm{Gal}(\tilde{k}/k)$ by φ is the identity.

2. The assertion of Theorem 1 holds even if we replace $L_i = L(\tilde{k}_i)$ with any solvably closed unraramified extension field L_i' over $\tilde{k}_i$ which is Galois over k_i, namely, there is no non-trivial unramified abelian extensions over L_i'. The maximal unramified solvable extension over $\tilde{k}_i$ is an example of such L_i'.

Indeed, because the maximal abelian subextenions of L_i/k_i and L_i'/k_i coincide, and $L^{\mathrm{ab}}(F) \subseteq L_i'$, holds for any $k_i \subseteq F \subseteq L_i'$, the assertion of Proposition 1 holds even if we replace L_i with L_i'. Furthemore, for a finite Galois subextension K_1/k_1 of L_1'/k_1, if an abelian extension M_1/K_1 satisfies that $\tilde{M}_1/\tilde{K}_1$ is unramified, then $M_1 \subseteq L_1'$ holds. Therefore, the arguments of sections 3 and 4 work for L_i'/k_i.

References

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

[2] Y.Furuta, The genus field and genus number in algebraic number fields, Nagoya Math. J. **29** (1967), 281–285.

[3] N.Klingen, Arithmetical similarities. Prime decomposition and finite group theory, Oxford Math. Monogr. Oxford Sci. Publ. The Clarendon Press, Oxford University Press, New York, 1998

[4] S.Mochizuki, The local pro-p anabelian geometry of curves, Invent. Math. **138** (1999), 319–423.

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

[6] J.Neukirch, A.Schmidt, K.Wingberg, Cohomology of Number Fields. Grundlehren Math. Wiss. **323** Springer-Verlag, Berlin, 2008

[7] D. Stuart and R. Perlis, A new characterization of arithmetic equivalence. J. Number Theory **53** (1995), no. 2, 300–308.

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

[9] K.Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions. Tohoku Math. J.(2)**31** (1979), no.3, 359–362.

[10] K.Uchida, Galois groups of unramified solvable extensions. Tohoku Math. J.(2) **34** (1982), no.2, 311–317.

Manabu Ozaki,
Department of Mathematics,
School of Fundamental Science and Engineering,
Waseda University,
Ohkubo 3-4-1, Shinjuku-ku, Tokyo, 169-8555, Japan
e-mail: `ozaki@waseda.jp`