Asada, M.
Osaka J. Math.
53 (2016), 321–330

ON SOME PROPERTIES OF GALOIS GROUPS OF UNRAMIFIED EXTENSIONS

MAMORU ASADA

(Received June 18, 2014, revised December 26, 2014)

Abstract

Let k be an algebraic number field of finite degree and k_∞ be the maximal cyclotomic extension of k. Let $\tilde{L}_k$ and L_k be the maximal unramified Galois extension and the maximal unramified abelian extension of k_∞ respectively. We shall give some remarks on the Galois groups $\mathrm{Gal}(\tilde{L}_k/k_\infty)$, $\mathrm{Gal}(L_k/k_\infty)$ and $\mathrm{Gal}(\tilde{L}_k/k)$. One of the remarks is concerned with non-solvable quotients of $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ when k is the rationals, which strengthens our previous result.

Introduction

Let k be an algebraic number field of finite degree in a fixed algebraic closure and ζ_n denote a primitive n-th root of unity ($n \geq 1$). Let k_∞ be the maximal cyclotomic extension of k, i.e., the field obtained by adjoining to k all ζ_n ($n \geq 1$). Let $\tilde{L}_k$ and L_k be the maximal unramified Galois extension and the maximal unramified abelian extension of k_∞ respectively. By the maximality, $\tilde{L}_k$ and L_k are both Galois extensions of k.

According to the analogy between finite algebraic number fields and function fields of one variable over finite constant fields, adjoining all ζ_n to a finite algebraic number field is one of the substitutes of extending the finite constant field of the function field to its algebraic closure. Therefore, the Galois group $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ may be regarded as an analogue of the algebraic fundamental group of a proper smooth geometrically connected curve over the algebraic closure of a finite field.

In this article, we shall give some remarks on the Galois groups $\mathrm{Gal}(\tilde{L}_k/k_\infty)$, $\mathrm{Gal}(L_k/k_\infty)$ and $\mathrm{Gal}(\tilde{L}_k/k)$.

It is known that the algebraic fundamental group of a smooth geometrically connected curve over an algebraically closed constant field has the following property (P) except for some special cases (cf. e.g. Tamagawa [8]).

(P) Every subgroup with finite index is centerfree.

This is one of the properties of algebraic fundamental groups of "anabelian" algebraic varieties (cf. e.g. Ihara–Nakamura [4]). Our first remark is that the Galois group

2010 Mathematics Subject Classification. 11R18, 11R23.

$\mathrm{Gal}(\tilde{L}_k/k_\infty)$ also has this property. This will be given in §1.

We shall next consider the Galois group $\Gamma = \mathrm{Gal}(k_\infty/k)$ and $X = \mathrm{Gal}(L_k/k_\infty)$. Then, Γ acts naturally on X, i.e., X is a Γ-module. As a profinite abelian group, X is isomorphic to the direct product of countable number of copies of $\hat{\mathbb{Z}}$, the profinite completion of the additive group of rational integers $\mathbb{Z}$. This follows from a more general result of Uchida [9] that the Galois group of the maximal unramified solvable extension of k_∞ over k_∞ is isomorphic to the free prosolvable group on countably infinite generators. However, the structure of X as a Γ-module does not seem to be well investigated. (Some partial and related results are obtained in Asada [2].)

Our second remark is that X is a faithful Γ-module. It follows from this and our first remark that the Galois group $\mathrm{Gal}(\tilde{L}_k/k)$ also has the property (P). This has been pointed out by Akio Tamagawa. The proofs of these will be given in §2.

Our final remark is about the inverse Galois problem on $\mathrm{Gal}(\tilde{L}_k/k_\infty)$. As noted above, the maximal prosolvable quotient of $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ is determined by Uchida, but not too much seems to be known for its non-solvable quotients. In our previous paper [1], when the ground field k is the rationals $\mathbb{Q}$, we have shown that there exist infinitely many unramified Galois extensions of $\mathbb{Q}_\infty$ having finite non-solvable group $\mathrm{PSL}_2(\mathbb{Z}/p^r\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})/\{\pm 1\}$ as the Galois group, where p is any prime greater than 3 and r is any positive integer. The method is to use the p^r-torsion points of certain elliptic curves over $\mathbb{Q}$. It is not difficult to see that all p-power torsion points of a single elliptic curve can not be used. Namely, by that method, profinite group $\mathrm{PSL}_2(\mathbb{Z}_p)$, which is not prosolvable, can not be realized as the Galois group of an unramified extension of $\mathbb{Q}_\infty$ ($\mathbb{Z}_p$: the ring of p-adic integers). Nevertheless, we can strengthen the result as the following theorem.

Theorem 0.1. *Let $p \geq 5$ be a prime. Then there exists an unramified Galois extension F of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(F/\mathbb{Q}_\infty)$ is isomorphic to $\prod_{N=1}^{\infty} \mathrm{SL}_2(\mathbb{Z}_p)$, the direct product of countable number of copies of $\mathrm{SL}_2(\mathbb{Z}_p)$.*

We shall give the proof in §3. The arithmetic point of the proof is that the Galois group $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ is projective, which is also due to Uchida [9]. The group-theoretical point of the proof is some properties of the group $\mathrm{SL}_2(\mathbb{Z}_p)$ due to Serre [6, 7]. Since our results are based on and related to Uchida's results, we shall summarize them in §1.

1. A result of Uchida and its consequence

(1-1) It seems that fundamental results about the Galois group $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ obtained so far are the following theorem of Uchida.

Theorem 1.1 ([9]). (i) *The cohomological dimension of the Galois group $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ is less than or equal to* 1.

(ii) *The maximal prosolvable quotient of the Galois group* $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ *is isomorphic to the free prosolvable group on countably infinite generators.*

It is known that the cohomological dimension of a profinite group G is less than or equal to 1 if and only if G is projective (cf. e.g. Serre [5, Chapter 1 5.9]). Recall that a profinite group G is called projective if for every surjective homomorphism of profinite groups $\alpha\colon E \to H$ and for every surjective homomorphism $\varphi\colon G \to H$, there exists a homomorphism $\psi\colon G \to E$ such that $\varphi = \alpha\psi$.

Actually, Uchida's result is more general. For an algebraic number field K, not necessarily of finite degree over the rationals, let K^{ur} (resp. K^{ur}_{sol}) be the maximal unramified Galois extension (resp. the maximal unramified prosolvable extension) of K. Uchida has given sufficient conditions on the ground field K for the Galois group $\mathrm{Gal}(K^{ur}/K)$ to be projective and those for the Galois group $\mathrm{Gal}(K^{ur}_{sol}/K)$ to be isomorphic to the free prosolvable group on countably infinite generators. Since the field k_∞ satisfies both conditions, the above theorem follows.

(1-2) The following is a consequence of Theorem 1.1, combined with a lemma of Tamagawa [8].

Proposition 1.2. *The Galois group* $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ *has the property* (*P*).

Proof. We first show that $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ itself is centerfree. By Lemma 1 in [8], it suffices to show that, for every open subgroup of $\mathrm{Gal}(\tilde{L}_k/k_\infty)$, its maximal pro-$l$ quotient is centerfree for every prime number l. Take an open subgroup U of $\mathrm{Gal}(\tilde{L}_k/k_\infty)$. Let $U = \mathrm{Gal}(\tilde{L}_k/K)$ with a finite extension K of k_∞. Then it is easy to see that there exists a finite algebraic number field F such that $K = F_\infty$ and that $\tilde{L}_k$ is also the maximal unramified Galois extension $\tilde{L}_F$ of F_∞. By Theorem 1.1 (ii), the maximal pro-l quotient of U is isomorphic to the free pro-l group on countably infinite generators, and hence is centerfree. Thus, $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ is centerfree.

Now, as stated above, any open subgroup of $\mathrm{Gal}(\tilde{L}_k/k_\infty)$ is of the form $\mathrm{Gal}(\tilde{L}_F/F_\infty)$ with a finite algebraic number field F. Hence, by the above arguments, it is centerfree. □

2. The faithfulness of the cyclotomic Galois action

(2-1) The cyclotomic Galois group $\Gamma = \mathrm{Gal}(k_\infty/k)$ acts naturally on $X = \mathrm{Gal}(L_k/k_\infty)$ and we have a homomorphism

$$\rho\colon \Gamma \to \mathrm{Aut}(X).$$

Then we have the following

Proposition 2.1. *The homomorphism ρ is injective, i.e., X is a faithful Γ-module.*

Before giving the proof, we shall verify the following corollary.

Corollary 2.2. *The Galois group* $\mathrm{Gal}(\tilde{L}_k/k)$ *has the property* (P).

Proof. We first verify that $\mathrm{Gal}(\tilde{L}_k/k)$ is centerfree. Let $\Omega = \mathrm{Gal}(\tilde{L}_k/k)$, $G = \mathrm{Gal}(\tilde{L}_k/k_\infty)$ and $N = \mathrm{Gal}(\tilde{L}_k/L_k)$, the commutator subgroup of G. We claim that the centralizer $C_\Omega(G)$ of G in Ω is trivial. In fact, let ω be an element of $C_\Omega(G)$ so that we have $\omega g \omega^{-1} = g$ for any element g of G. Reducing this equation modulo N, we see that the coset $\gamma = \omega G$, which is an element of $\Omega/G = \Gamma$, acts trivially on $G/N = X$. By Proposition 2.1, we have $\gamma = 1$, i.e., $\omega \in G$. Since G is centerfree by Proposition 1.2, we have $\omega = 1$, i.e. $C_\Omega(G) = \{1\}$. In particular, Ω is centerfree.

Now, similar to the case of $\mathrm{Gal}(\tilde{L}_k/k_\infty)$, it is easy to see that any open subgroup of Ω is of the form $\mathrm{Gal}(\tilde{L}_F/F)$ with a finite algebraic number field F. Therefore, by the above arguments, it is centerfree. □

(2-2) In the rest of this section, we shall give the proof of Proposition 2.1. First we shall construct certain unramified abelian extensions of cyclotomic fields.

Let p be a fixed prime and q be a power of p: $q = p^r$ $(r \geq 1)$. Let ζ_q be a primitive q-th root of unity, $e = [k(\zeta_q) : k]$, and $\Gamma_q = \mathrm{Gal}(k(\zeta_q)/k)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ be all prime ideals of $k(\zeta_q)$ lying above p. For each i $(1 \leq i \leq g)$, fix a positive integer s_i such that every element α of $k(\zeta_q)$ satisfying $\alpha \equiv 1 \bmod \mathfrak{p}_i^{s_i}$ is locally a q-th power, i.e., α is a q-th power in the $\mathfrak{p}_i$-adic completion of $k(\zeta_q)$.

Let $\mathfrak{m}$ be an integral ideal of $k(\zeta_q)$ such that $\mathfrak{p}_i^{s_i}$ divides $\mathfrak{m}$ $(1 \leq i \leq g)$ and that $\mathfrak{m}$ is invariant by the action of Γ_q. By the density theorem, there exists a principal prime ideal $\mathfrak{l} = (\alpha)$ of $k(\zeta_q)$ which is unramified in the extension $k(\zeta_q)/\mathbb{Q}$, absolute degree one, and $\alpha \equiv 1 \bmod \mathfrak{m}$.

Let $\mathfrak{l}_1$ $(= \mathfrak{l})$, $\dots$, $\mathfrak{l}_e$ be all prime ideals conjugate to $\mathfrak{l}$ over k. As $\mathfrak{l}$ is principal, all $\mathfrak{l}_i$ are principal: $\mathfrak{l}_i = (\alpha_i)$, $\alpha_i \in k(\zeta_q)$, $1 \leq i \leq e$. We may assume that $\alpha_1, \dots, \alpha_e$ are all algebraic integers conjugate to α_1 over k.

For each α_i, $1 \leq i \leq e$, fix a q-th root $\alpha_i^{1/q}$ of α_i. Let E be the field obtained by adjoining to $k(\zeta_q)$ all $\alpha_i^{1/q}$, $1 \leq i \leq e$. Then E is a Kummer extension of $k(\zeta_q)$ with exponent q and is a Galois extension of k. The extension $E/k(\zeta_q)$ is unramified outside $\mathfrak{p}_1, \dots, \mathfrak{p}_g, \mathfrak{l}_1, \dots, \mathfrak{l}_e$.

Lemma 2.3. (i) *The prime ideals* $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ *split completely in* E. *In particular, they are unramified in* E.
(ii) *Let* $l = \mathfrak{l} \cap \mathbb{Q}$ *and* ζ_l *be a primitive* l*-th root of unity. Then the prime ideals of* $k(\zeta_q, \zeta_l)$ *lying above* $\mathfrak{l}_1, \dots, \mathfrak{l}_e$ *are unramified in the extension* $E(\zeta_l)/k(\zeta_q, \zeta_l)$.

Proof. (i) Since $\mathfrak{l}$ belongs to the principal ray class modulo $\mathfrak{m}$, so do all $\mathfrak{l}_i$ $(1 \leq i \leq e)$, because $\mathfrak{m}$ is invariant by the action of Γ_q. As $\mathfrak{p}_j^{s_j}$ divides $\mathfrak{m}$, we have $\alpha_i \equiv$

$1 \bmod \mathfrak{p}_j^{s_j}$ $(1 \le i \le e,\ 1 \le j \le g)$. From this it follows that $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ split completely in E.

(ii) We first note that $l \equiv 1 \bmod q$. Indeed, as the absolute degree of $\mathfrak{l}$ is one, so is that of $\mathfrak{l} \cap \mathbb{Q}(\zeta_q)$, which is a prime ideal of $\mathbb{Q}(\zeta_q)$ lying above l. This shows that l splits completely in $\mathbb{Q}(\zeta_q)$ so that $l \equiv 1 \bmod q$.

Now since $\mathfrak{l}$, hence all $\mathfrak{l}_i$, are unramified in the extension $k(\zeta_q)/\mathbb{Q}$, it follows that $\mathbb{Q}(\zeta_l) \cap k(\zeta_q) = \mathbb{Q}$ and every $\mathfrak{l}_i$ is totally ramified in $k(\zeta_q, \zeta_l)/k(\zeta_q)$ with ramification index $l - 1$. On the other hand, the ramification index of $\mathfrak{l}_i$ in $E/k(\zeta_q)$ is obviously q. Since q divides $l - 1$ as noted above, (ii) follows by Abhyankar's lemma (cf. e.g. Cornell [3]). $\square$

(2-3) We shall next investigate cyclotomic Galois actions on the Galois group of E over $E \cap k_\infty$.

Let us define the element τ_i $(1 \le i \le e)$ of $\mathrm{Gal}(E/k(\zeta_q))$ by

$$\tau_i(\alpha_j^{1/q}) = \zeta_q \alpha_j^{1/q} \quad (j = i),$$
$$\tau_i(\alpha_j^{1/q}) = \alpha_j^{1/q} \quad (j \ne i).$$

Each τ_i is of order q and $\mathrm{Gal}(E/k(\zeta_q))$ is the direct product of the cyclic subgroup generated by τ_i $(1 \le i \le e)$.

For each $\sigma \in \Gamma_q$, we define its extension $\tilde{\sigma} \in \mathrm{Gal}(E/k)$ in such a way that $\tilde{\sigma}(\alpha_i^{1/q}) = \alpha_j^{1/q}$ if $\sigma(\alpha_i) = \alpha_j$ $(1 \le i, j \le e)$. Let

$$\chi : \Gamma_q \to (\mathbb{Z}/q\mathbb{Z})^*$$

denote the cyclotomic character, i.e., if $\sigma(\zeta_q) = \zeta_q^s$ $(\sigma \in \Gamma_q,\ s \in \mathbb{Z})$, then $\chi(\sigma) = s \bmod q$. The following lemma will be easily verified.

Lemma 2.4. *Assume that $\sigma \in \Gamma_q$ satisfies $\sigma(\alpha_i) = \alpha_j$. Then we have $\tilde{\sigma}\tau_i\tilde{\sigma}^{-1} = \tau_j^s$, where $\chi(\sigma) = s \bmod q$.*

Let $K = E \cap k_\infty$. As the extension $K/k(\zeta_q)$ is abelian, the commutator of $\tilde{\sigma}$ and τ_i belongs to the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/k(\zeta_q))$. Thus we have the following

Lemma 2.5. *Assumptions being as in* Lemma 2.4, *$\tau_j^s\tau_i^{-1}$ belongs to* $\mathrm{Gal}(E/K)$.

The group Γ_q acts naturally on the abelian group $\mathrm{Gal}(E/k(\zeta_q))$ and, since K is a Galois extension of k, on the subgroup $\mathrm{Gal}(E/K)$.

Lemma 2.6. *The action of Γ_q on* $\mathrm{Gal}(E/K)$ *is faithful.*

Proof. First, let us assume that $p > 2$. Then the group Γ_q is cyclic. Let σ be a generator of Γ_q and $\chi(\sigma) = s \bmod q$. We may assume, renumbering if necessary, that

$$\sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, \ldots, \sigma(\alpha_e) = \alpha_1.$$

Assume that σ^m ($m \geq 1$) acts trivially on $\mathrm{Gal}(E/K)$. Since $\tau_2^s \tau_1^{-1}$ belongs to $\mathrm{Gal}(E/K)$ by Lemma 2.5, we have

$$\tilde{\sigma}^m \tau_2^s \tau_1^{-1} \tilde{\sigma}^{-m} = \tau_2^s \tau_1^{-1},$$

and hence,

$$(\tilde{\sigma}^m \tau_2 \tilde{\sigma}^{-m})^s (\tilde{\sigma}^m \tau_1 \tilde{\sigma}^{-m})^{-1} = \tau_2^s \tau_1^{-1}.$$

By Lemma 2.4, the left hand side is $(\tau_{m+2}^{s^{m+1}})(\tau_{m+1}^{-s^m})$, the index of τ being regarded as the residue class modulo e. Thus we have

$$\tau_{m+2}^{s^{m+1}} \tau_{m+1}^{-s^m} = \tau_2^s \tau_1^{-1}.$$

Since $\mathrm{Gal}(E/k(\zeta_q))$ is the direct product of the cyclic subgroup generated by τ_i ($1 \leq i \leq e$), this holds if and only if $m \equiv 0 \bmod e$ and $s^m \equiv 1 \bmod q$. Hence, we have $\sigma^m = 1$.

We shall next assume that $p = 2$. In the case that Γ_q is cyclic, the proof in the case of $p > 2$ remains valid. Assume that Γ_q is not cyclic and let $e = 2^t$ ($t \geq 2$). Then Γ_q is the direct product of a cyclic subgroup H_1 of order 2^{t-1} and a cyclic subgroup H_2 of order 2. Let σ_1 and σ_2 be generators of H_1 and H_2 respectively. Since H_1 is cyclic and is of index 2, we may assume, renumbering if necessary, that

$$\sigma_1(\alpha_1) = \alpha_2, \ldots, \sigma_1(\alpha_f) = \alpha_1, \sigma_1(\alpha_{f+1}) = \alpha_{f+2}, \ldots, \sigma_1(\alpha_e) = \alpha_{f+1},$$

where $f = 2^{t-1}$. Then $\sigma_2(\alpha_1)$ belongs to the subset $\{\alpha_{f+1}, \ldots, \alpha_e\}$, because Γ_q acts on the set $\{\alpha_1, \ldots, \alpha_e\}$ transitively. We may also assume that $\sigma_2(\alpha_1) = \alpha_{f+1}$ and then it is easy to see that

$$\sigma_2(\alpha_2) = \alpha_{f+2}, \ldots, \sigma_2(\alpha_f) = \alpha_e.$$

Now, each element of Γ_q is expressed uniquely as the following form:

$$\sigma_1^m \sigma_2^n \quad (0 \leq m < f,\ n = 0, 1)$$

Assume that $\sigma_1^m \sigma_2^n$ acts trivially on $\mathrm{Gal}(E/K)$. Let $\chi(\sigma_1) = s \bmod q$. Since $\tau_2^s \tau_1^{-1}$ belongs to $\mathrm{Gal}(E/K)$ by Lemma 2.5, we have

$$\tilde{\sigma}_1^m \tilde{\sigma}_2^n (\tau_2^s \tau_1^{-1}) \tilde{\sigma}_2^{-n} \tilde{\sigma}_1^{-m} = \tau_2^s \tau_1^{-1}. \tag{1}$$

If $n = 0$, similarly as in the case that $p > 2$, the left hand side of (1) is

$$\tau_{m+2}^{s^{m+1}} \tau_{m+1}^{-s^m},$$

the index of τ being regarded as the residue class modulo f. If $n = 1$, the left hand side of (1) is

$$\tau_{f+m+2}^{-s^{m+1}} \tau_{f+m+1}^{s^m},$$

the index of τ belongs to $\{f+1, \dots, 2f\}$. Therefore, (1) holds if and only if $n = 0$ and $m \equiv 0 \bmod f$. Hence we have $\sigma_1^m \sigma_2^n = 1$. □

(2-4) Now we shall complete the proof of Proposition 2.1.

Let p be a prime and q be a power of p. Let E be the field defined in (2-2). By Lemma 2.3, Ek_∞ is an unramified abelian extension of k_∞ so that $k_\infty \subset Ek_\infty \subset L_k$. Let X_E be the Galois group $\mathrm{Gal}(Ek_\infty/k_\infty)$. Since Ek_∞ is a Galois extension of k, X_E is also a Γ-module, i.e., X_E is a quotient of Γ-module X. By Lemma 2.6, the kernel of the action of Γ on X_E is $\mathrm{Gal}(k_\infty/k(\zeta_q))$. Therefore, $\mathrm{Ker}\,\rho$ is contained in $\mathrm{Gal}(k_\infty/k(\zeta_q))$. Since q is an arbitrary power of an arbitrary prime, it follows that $\mathrm{Ker}\,\rho = \{1\}$, i.e., ρ is injective.

3. Proof of Theorem 0.1

(3-1) In this section, we shall give the proof of Theorem 0.1.

We first verify the following

Lemma 3.1. *Let $p \geq 5$ be a prime and k be an unramified Galois extension of $\mathbb{Q}_\infty$ having $\mathrm{PSL}_2(\mathbb{F}_p)$ as the Galois group ($\mathbb{F}_p$: the prime field of characteristic p). Then the following assertions hold.*

(i) *There exists an unramified Galois extension $\tilde{k}$ of $\mathbb{Q}_\infty$ having $\mathrm{SL}_2(\mathbb{F}_p)$ as the Galois group such that $\mathbb{Q}_\infty \subset k \subset \tilde{k}$ and that the restriction $\mathrm{Gal}(\tilde{k}/\mathbb{Q}_\infty) \to \mathrm{Gal}(k/\mathbb{Q}_\infty)$ corresponds to the projection $\mathrm{SL}_2(\mathbb{F}_p) \to \mathrm{PSL}_2(\mathbb{F}_p)$.*

(ii) *There exists an unramified Galois extension K of $\mathbb{Q}_\infty$ having $\mathrm{SL}_2(\mathbb{Z}_p)$ as the Galois group such that $\mathbb{Q}_\infty \subset \tilde{k} \subset K$, $\tilde{k}$ being the extension given in (i), and that the restriction $\mathrm{Gal}(K/\mathbb{Q}_\infty) \to \mathrm{Gal}(\tilde{k}/\mathbb{Q}_\infty)$ corresponds to $\mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$, the reduction modulo p.*

Proof. By the assumption, there exists a surjective homomorphism

$$\varphi\colon \mathrm{Gal}(\tilde{L}_{\mathbb{Q}}/\mathbb{Q}_\infty) \to \mathrm{PSL}_2(\mathbb{F}_p)$$

such that $\mathrm{Ker}\,\varphi$ corresponds to k.

Consider the surjective homomorphism $\alpha\colon \mathrm{SL}_2(\mathbb{F}_p) \to \mathrm{PSL}_2(\mathbb{F}_p)$. Then, by the projectivity of $\mathrm{Gal}(\tilde{L}_{\mathbb{Q}}/\mathbb{Q}_\infty)$ (Theorem 1.1 (i)), there exists a homomorphism

$$\psi\colon \mathrm{Gal}(\tilde{L}_{\mathbb{Q}}/\mathbb{Q}_\infty) \to \mathrm{SL}_2(\mathbb{F}_p)$$

such that $\varphi = \alpha\psi$. Then ψ is surjective, because no proper subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ maps onto $\mathrm{PSL}_2(\mathbb{F}_p)$ (cf. e.g. Serre [6, Chapter IV 3.4 Lemma 2]). Then, the extension $\tilde{k}$ of $\mathbb{Q}_\infty$ corresponding to $\mathrm{Ker}\,\psi$ satisfies the condition (i).

Consider the surjective homomorphism $r\colon \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$, the reduction modulo p. Again, there exists a homomorphism

$$\omega\colon\ \mathrm{Gal}(\tilde{L}_{\mathbb{Q}}/\mathbb{Q}_\infty) \to \mathrm{SL}_2(\mathbb{Z}_p)$$

such that $\psi = r\omega$. Then ω is also surjective, because no proper subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ maps onto $\mathrm{SL}_2(\mathbb{F}_p)$ ([6, Chapter IV 3.4 Lemma 3]). Then, the extension K of $\mathbb{Q}_\infty$ corresponding to $\mathrm{Ker}\,\omega$ satisfies the condition (ii). □

(3-2) We need some group-theoretical lemmas.

Lemma 3.2. *Let G be a non-abelian finite simple group and $G_1, G_2, \dots, G_n$ $(n \geq 1)$ be finite groups all isomorphic to G. Then every normal subgroup of the direct product $G_1 \times G_2 \times \cdots \times G_n$ is of the form*

$$G_{i_1} \times G_{i_2} \times \cdots \times G_{i_k} \quad (1 \leq i_1 < i_2 < \cdots < i_k \leq n).$$

The proof of Lemma 3.2 is an exercise of group theory, and hence is omitted.

Lemma 3.3. (i) *Let $p \geq 5$ be a prime and H be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)^n$, the direct product of n copies of $\mathrm{SL}_2(\mathbb{Z}_p)$ $(n \geq 1)$. Assume that the image of H in $\mathrm{SL}_2(\mathbb{F}_p)^n$ by the reduction modulo p coincides with $\mathrm{SL}_2(\mathbb{F}_p)^n$. Then H coincides with $\mathrm{SL}_2(\mathbb{Z}_p)^n$.*
(ii) *Let $p \geq 5$ be a prime and H be a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)^n$, the direct product of n copies of $\mathrm{SL}_2(\mathbb{F}_p)$ $(n \geq 1)$. Assume that the image of H in $\mathrm{PSL}_2(\mathbb{F}_p)^n$ coincides with $\mathrm{PSL}_2(\mathbb{F}_p)^n$. Then H coincides with $\mathrm{SL}_2(\mathbb{F}_p)^n$.*

Proof. (i) If $n = 1$, this is one of the lemmas quoted in the proof of Lemma 3.1 ([6, Chapter IV 3.4 Lemma 3]). If $n = 2$, this lemma follows from Lemma 10 in Serre [7], where the case of $n = 2$ is reduced to the case of $n = 1$ by using projections to each component of $\mathrm{SL}_2(\mathbb{Z}_p) \times \mathrm{SL}_2(\mathbb{Z}_p)$. In this reduction process, the points are that the kernel of the reduction modulo $p\colon \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ is a pro-p group and that $\mathrm{SL}_2(\mathbb{F}_p)$ does not have non-trivial normal subgroups with p-power indices. If $n \geq 3$, by decomposing $\mathrm{SL}_2(\mathbb{Z}_p)^n = \mathrm{SL}_2(\mathbb{Z}_p)^{n-1} \times \mathrm{SL}_2(\mathbb{Z}_p)$, $\mathrm{SL}_2(\mathbb{Z}_p) \times \mathrm{SL}_2(\mathbb{Z}_p)^{n-1}$, the same method can also be applied and the lemma is proved by induction on n. We omit the details.

(ii) If $n = 1$, again this is one of the lemmas quoted in the proof of Lemma 3.1 ([6, Chapter IV 3.4 Lemma 2]). If $n \geq 2$, the proof will be done, in the same way as that of (i), by induction on n, and hence is omitted. We note that, here, the points are that the kernel of the projection $SL_2(\mathbb{F}_p) \to PSL_2(\mathbb{F}_p)$ is a cyclic group of order 2 and that $PSL_2(\mathbb{F}_p)$ does not have normal subgroups with index 2. $\square$

(3-3) Now we shall prove Theorem 0.1. By the result of [1], there exist unramified Galois extensions k_n $(n \geq 1)$ of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(k_n/\mathbb{Q}_\infty)$ is isomorphic to $PSL_2(\mathbb{F}_p)$ and that $k_n \neq k_m$ for $n \neq m$. Applying Lemma 3.1 to $k = k_n$, we obtain unramified Galois extensions $\tilde{k}_n$ and K_n of $\mathbb{Q}_\infty$ satisfying the following conditions:
(a) $\mathbb{Q}_\infty \subset k_n \subset \tilde{k}_n \subset K_n$.
(b) $\mathrm{Gal}(K_n/\mathbb{Q}_\infty)$ is isomorphic to $SL_2(\mathbb{Z}_p)$, $\tilde{k}_n$ and k_n corresponding to the kernels of homomorphisms $SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p)$ and $SL_2(\mathbb{Z}_p) \to PSL_2(\mathbb{F}_p)$ respectively.

Let F be the composite field of all K_n $(n \geq 1)$. Then F is an unramified Galois extension of $\mathbb{Q}_\infty$. We shall show that $\mathrm{Gal}(F/\mathbb{Q}_\infty)$ is isomorphic to $\prod_{N=1}^{\infty} SL_2(\mathbb{Z}_p)$. For that purpose, it suffices to show that

$$(*) \qquad \begin{array}{l}\mathrm{Gal}(K_1 \cdots K_n/\mathbb{Q}_\infty) \text{ is isomorphic to } \mathrm{Gal}(K_1/\mathbb{Q}_\infty) \times \cdots \times \mathrm{Gal}(K_n/\mathbb{Q}_\infty) \\ \text{for all } n \geq 1.\end{array}$$

We first verify that

$$(*)_k \qquad \begin{array}{l}\mathrm{Gal}(k_1 \cdots k_n/\mathbb{Q}_\infty) \text{ is isomorphic to } \mathrm{Gal}(k_1/\mathbb{Q}_\infty) \times \cdots \times \mathrm{Gal}(k_n/\mathbb{Q}_\infty) \\ \text{for all } n \geq 1.\end{array}$$

This will be proved by induction on n. For $n = 1$, this holds trivially. Assume that this holds for $n = m$, so that $\mathrm{Gal}(k_1 \cdots k_m/\mathbb{Q}_\infty)$ is isomorphic to $PSL_2(\mathbb{F}_p)^m$. As $\mathrm{Gal}(k_{m+1}/\mathbb{Q}_\infty)$ is simple, we have $k_1 \cdots k_m \cap k_{m+1} = \mathbb{Q}_\infty$ or k_{m+1}. But Lemma 3.2 shows, in particular, that a Galois subextension of $k_1 \cdots k_m/\mathbb{Q}_\infty$ having $PSL_2(\mathbb{F}_p)$ as the Galois group is one of k_i $(i = 1, 2, \ldots, m)$. Hence the latter cannot occur and it follows that $(*)_k$ holds for $n = m + 1$.

Now let $H = \mathrm{Gal}(K_1 \cdots K_n/\mathbb{Q}_\infty)$ and consider the commutative diagram

$$\begin{array}{ccc} H & \xrightarrow{r_1} & \mathrm{Gal}(K_1/\mathbb{Q}_\infty) \times \cdots \times \mathrm{Gal}(K_n/\mathbb{Q}_\infty) = SL_2(\mathbb{Z}_p)^n \\ \downarrow & & \downarrow \\ \mathrm{Gal}(k_1 \cdots k_n/\mathbb{Q}_\infty) & \xrightarrow{r_2} & \mathrm{Gal}(k_1/\mathbb{Q}_\infty) \times \cdots \times \mathrm{Gal}(k_n/\mathbb{Q}_\infty) = PSL_2(\mathbb{F}_p)^n \end{array}$$

where r_1 and r_2 are restrictions and vertical homomorphisms are projections.

Then, by $(*)_k$, r_2 is an isomorphism so that the image of H in $PSL_2(\mathbb{F}_p)^n$ coincides with $PSL_2(\mathbb{F}_p)^n$. Hence, by Lemma 3.3 (i) and (ii), r_1 is surjective, i.e., $(*)$ holds.

REMARK. In our previous paper [1], we have considered certain subextension M_0 of $\tilde{L}_{\mathbb{Q}}/\mathbb{Q}_\infty$ and have shown that the unramified Galois extension $k_n M_0/M_0$ $(n \geq 1)$ has also $PSL_2(\mathbb{F}_p)$ as the Galois group and that they are mutually distinct. Here, M_0 is the composite of $\mathbb{Q}_\infty$ and the maximal tamely ramified subextension M^t of $\tilde{L}_{\mathbb{Q}}/\mathbb{Q}$. The above arguments for determining the Galois group H can be also applied to the Galois group $\mathrm{Gal}(K_1 \cdots K_n M_0/M_0)$. Hence we have that the extension FM_0/M_0 is unramified and that it has $\prod_{N=1}^{\infty} \mathrm{SL}_2(\mathbb{Z}_p)$ as the Galois group.

Further, let γ be an element of $\mathrm{Gal}(M_0/M^t)$ and $\tilde{\gamma} \in \mathrm{Gal}(\tilde{L}_{\mathbb{Q}}/M^t)$ be any extension of γ. Then, for $n \geq 1$, $\tilde{\gamma}$ transforms the field $K_n M_0$ to the subextension $\tilde{\gamma}(K_n M_0)$ of $\tilde{L}_{\mathbb{Q}}/M^t$, which also has $\mathrm{SL}_2(\mathbb{Z}_p)$ as the Galois group. This may be different from $K_n M_0$ because $K_n M_0$ is not necessarily Galois over M^t. However, $\tilde{\gamma}(K_n M_0)$ does not coincide with $K_m M_0$ for any $m \neq n$.

To see this, first note that the subextension $k_n M_0$ of $K_n M_0/M_0$ is Galois over M^t (in fact Galois over $\mathbb{Q}$) so that $\tilde{\gamma}(k_n M_0) = k_n M_0$. Then, since $k_n M_0 \cap k_m M_0 = M_0$ for $m \neq n$, by the same arguments for determining the Galois group H, we have $\tilde{\gamma}(K_n M_0) \cap K_m M_0 = M_0$. In particular, $\tilde{\gamma}(K_n M_0) \neq K_m M_0$.

ACKNOWLEDGEMENTS. The author expresses his gratitudes to Akio Tamagawa for valuable comments, especially for pointing out that the Galois group $\mathrm{Gal}(\tilde{L}_k/k)$ has the property (P).

References

[1] M. Asada: *Construction of certain non-solvable unramified Galois extensions over the total cyclotomic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **32** (1985), 397–415.

[2] M. Asada: *On Galois groups of abelian extensions over maximal cyclotomic fields*, Tôhoku Math. J. (2) **60** (2008), 135–147.

[3] G. Cornell: *Abhyankar's lemma and the class group*; in Number Theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., 751, Springer, Berlin, 1979, 82–88.

[4] Y. Ihara and H. Nakamura: *Some illustrative examples for anabelian geometry in high dimensions*; in Geometric Galois Actions, **1**, London Math. Soc. Lecture Note Ser. **242**, Cambridge Univ. Press, Cambridge, 1997, 127–138.

[5] J.-P. Serre: Cohomologie Galoisienne, fifth edition, Lecture Notes in Mathematics **5**, Springer, Berlin, 1994.

[6] J.-P. Serre: Abelian l-Adic Representations and Elliptic Curves, W.A. Benjamin, Inc., New York, 1968.

[7] J.-P. Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[8] A. Tamagawa: *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), 135–194.

[9] K. Uchida: *Galois groups of unramified solvable extensions*, Tôhoku Math. J. (2) **34** (1982), 311–317.

Faculty of Arts and Sciences
Kyoto Institute of Technology
Matsugasaki, Kyoto 606-8585
Japan