<table>
<thead>
<tr>
<th>Title</th>
<th>ON SOME PROPERTIES OF GALOIS GROUPS OF UNRAMIFIED EXTENSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Asada, Mamoru</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 53(2) P.321–P.330</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2016-04</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/58906">https://doi.org/10.18910/58906</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/58906</td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
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 $k_{\infty}$ 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 $k_{\infty}$ respectively. We shall give some remarks on the Galois groups $\text{Gal}(\tilde{L}_k/k_{\infty})$, $\text{Gal}(L_k/k_{\infty})$ and $\text{Gal}(\tilde{L}_k/k)$. One of the remarks is concerned with non-solvable quotients of $\text{Gal}(\tilde{L}_k/k_{\infty})$ 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 $\zeta_n$ denote a primitive $n$-th root of unity ($n \geq 1$). Let $k_{\infty}$ be the maximal cyclotomic extension of $k$, i.e., the field obtained by adjoining to $k$ all $\zeta_n$ ($n \geq 1$). Let $\tilde{L}_k$ and $L_k$ be the maximal unramified Galois extension and the maximal unramified abelian extension of $k_{\infty}$ 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 $\zeta_n$ 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 $\text{Gal}(\tilde{L}_k/k_{\infty})$ 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 $\text{Gal}(\tilde{L}_k/k_{\infty})$, $\text{Gal}(L_k/k_{\infty})$ and $\text{Gal}(\tilde{L}_k/k)$.

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

We shall next consider the Galois group \(\Gamma = \text{Gal}(k_\infty/k)\) and \(X = \text{Gal}(L_k/k_\infty)\). Then, \(\Gamma\) acts naturally on \(X\), i.e., \(X\) is a \(\Gamma\)-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 \(k_\infty\) over \(k_\infty\) is isomorphic to the free prosolvable group on countably infinite generators. However, the structure of \(X\) as a \(\Gamma\)-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 \(\Gamma\)-module. It follows from this and our first remark that the Galois group \(\text{Gal}(\tilde{L}_k/k)\) 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 \(\text{Gal}(\tilde{L}_k/k_\infty)\). As noted above, the maximal prosolvable quotient of \(\text{Gal}(\tilde{L}_k/k_\infty)\) 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 \(\text{PSL}_2(\mathbb{Z}/p^r\mathbb{Z}) = \text{SL}_2(\mathbb{Z}/p^r\mathbb{Z})/\{\pm 1\}\) 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 \(\text{PSL}_2(\mathbb{Z}_p)\), 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 \(\text{Gal}(F/\mathbb{Q}_\infty)\) is isomorphic to \(\prod_{N=1}^{\infty} \text{SL}_2(\mathbb{Z}_p)\), the direct product of countable number of copies of \(\text{SL}_2(\mathbb{Z}_p)\).

We shall give the proof in §3. The arithmetic point of the proof is that the Galois group \(\text{Gal}(\tilde{L}_k/k_\infty)\) is projective, which is also due to Uchida [9]. The group-theoretical point of the proof is some properties of the group \(\text{SL}_2(\mathbb{Z}_p)\) 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 \(\text{Gal}(\tilde{L}_k/k_\infty)\) obtained so far are the following theorem of Uchida.

**Theorem 1.1** ([9]). (i) The cohomological dimension of the Galois group \(\text{Gal}(\tilde{L}_k/k_\infty)\) is less than or equal to 1.
(ii) The maximal prosolvable quotient of the Galois group \( \text{Gal}(\overline{L}_k/k_\infty) \) 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 15.9]). Recall that a profinite group \( G \) is called projective if for every surjective homomorphism \( \alpha : E \to H \) and for every surjective homomorphism \( \varphi : G \to H \), there exists a homomorphism \( \psi : G \to E \) 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 \( K^\text{ur} \) (resp. \( K^\text{ur}_\text{sol} \)) 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 \( \text{Gal}(K^\text{ur}/K) \) to be projective and those for the Galois group \( \text{Gal}(K^\text{ur}_\text{sol}/K) \) to be isomorphic to the free prosolvable group on countably infinite generators. Since the field \( k_\infty \) 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 \( \text{Gal}(\overline{L}_k/k_\infty) \) has the property (P).

**Proof.** We first show that \( \text{Gal}(\overline{L}_k/k_\infty) \) itself is centerfree. By Lemma 1 in [8], it suffices to show that, for every open subgroup of \( \text{Gal}(\overline{L}_k/k_\infty) \), its maximal pro-

l quotient is centerfree for every prime number \( l \). Take an open subgroup \( U \) of \( \text{Gal}(\overline{L}_k/k_\infty) \). Let \( U = \text{Gal}(\overline{L}_k/K) \) with a finite extension \( K \) of \( k_\infty \). Then it is easy to see that there exists a finite algebraic number field \( F \) such that \( K = F_\infty \) and that \( \overline{L}_k \) is also the maximal unramified Galois extension \( \overline{L}_F \) of \( F_\infty \). 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, \( \text{Gal}(\overline{L}_k/k_\infty) \) is centerfree.

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

2. The faithfulness of the cyclotomic Galois action

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

\[ \rho : \Gamma \to \text{Aut}(X). \]

Then we have the following

**Proposition 2.1.** The homomorphism \( \rho \) is injective, i.e., \( X \) is a faithful \( \Gamma \)-module.
Before giving the proof, we shall verify the following corollary.

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

Proof. We first verify that $\text{Gal}(\bar{L}_k/k)$ is centerfree. Let $\Omega = \text{Gal}(\bar{L}_k/k)$, $G = \text{Gal}(\bar{L}_k/k_\infty)$ and $N = \text{Gal}(\bar{L}_k/L_k)$, the commutator subgroup of $G$. We claim that the centralizer $C_\Omega(G)$ of $G$ in $\Omega$ is trivial. In fact, let $\omega$ 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, $\Omega$ is centerfree.

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

(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 $\zeta_q$ be a primitive $q$-th root of unity, $e = [k(\zeta_q) : k]$, and $\Gamma_q = \text{Gal}(k(\zeta_q)/k)$. Let $p_1, \ldots, p_g$ 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 $\alpha$ of $k(\zeta_q)$ satisfying $\alpha \equiv 1 \mod p_i^{s_i}$ is locally a $q$-th power, i.e., $\alpha$ is a $q$-th power in the $p_i$-adic completion of $k(\zeta_q)$.

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

Let $l_1 (= l), \ldots, l_e$ be all prime ideals conjugate to $l$ over $k$. As $l$ is principal, all $l_i$ are principal: $l_i = (\alpha_i)$, $\alpha_i \in k(\zeta_q)$, $1 \leq i \leq e$. We may assume that $\alpha_1, \ldots, \alpha_e$ are all algebraic integers conjugate to $\alpha_1$ over $k$.

For each $\alpha_i$, $1 \leq i \leq e$, fix a $q$-th root $\alpha_i^{1/q}$ of $\alpha_i$. 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 $p_1, \ldots, p_g, l_1, \ldots, l_e$.

**Lemma 2.3.**

(i) The prime ideals $p_1, \ldots, p_g$ split completely in $E$. In particular, they are unramified in $E$.

(ii) Let $l = l \cap \mathbb{Q}$ and $\zeta_l$ be a primitive $l$-th root of unity. Then the prime ideals of $k(\zeta_l, \zeta_i)$ lying above $l_1, \ldots, l_e$ are unramified in the extension $E(\zeta_l)/k(\zeta_l, \zeta_l)$.

Proof. (i) Since $l$ belongs to the principal ray class modulo $m$, so do all $l_i$ ($1 \leq i \leq e$), because $m$ is invariant by the action of $\Gamma_q$. As $p_i^{s_i}$ divides $m$, we have $\alpha_i \equiv \zeta_q$ modulo
1 \mod p^i_j \ (1 \leq i \leq e, \ 1 \leq j \leq g). \ From \ this \ it \ follows \ that \ p_1, \ldots, p_g \ split \ completely \ in \ E.

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

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

(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 \ \tau_i \ (1 \leq i \leq e) \ of \ \text{Gal}(E/k(\zeta_q)) \ by

\[
\tau_i(\alpha_j^{1/q}) = \zeta_q \alpha_j^{1/q} \quad (j = i), \\
\tau_i(\alpha_j^{1/q}) = \alpha_j^{1/q} \quad (j \neq i).
\]

Each \ \tau_i \ is \ of \ order \ q \ and \ \text{Gal}(E/k(\zeta_q)) \ is \ the \ direct \ product \ of \ the \ cyclic \ subgroup \ generated \ by \ \tau_i \ (1 \leq i \leq e).

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

\[
\chi : \Gamma_q \to (\mathbb{Z}/q\mathbb{Z})^\ast
\]

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 \mod 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 \ \bar{\sigma} \tau_i \bar{\sigma}^{-1} = \tau_j^s, \ where \ \chi(\sigma) = s \mod q.

Let \ K = E \cap k_\infty. \ As \ the \ extension \ K/k(\zeta_q) \ is \ abelian, \ the \ commutator \ of \ \bar{\sigma} \ and \ \tau_i \ belongs \ to \ the \ subgroup \ \text{Gal}(E/K) \ of \ \text{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 \ \text{Gal}(E/K).

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

**Lemma 2.6.** The \ action \ of \ \Gamma_q \ on \ \text{Gal}(E/K) \ is \ faithful.
Proof. First, let us assume that $p > 2$. Then the group $\Gamma_q$ is cyclic. Let $\sigma$ be a generator of $\Gamma_q$ and $\chi(\sigma) = s \mod q$. We may assume, renumbering if necessary, that

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

Assume that $\sigma^m \,(m \geq 1)$ acts trivially on $\text{Gal}(E/K)$. Since $\tau^2_2 \tau^1_1$ belongs to $\text{Gal}(E/K)$ by Lemma 2.5, we have

$$\sigma^m \tau^x_2 \tau^1_1 = \tau^y_2 \tau^1_1,$$

and hence,

$$(\sigma^m \tau^y_2 \sigma^{-m})^2 (\sigma^m \tau^1_1 \sigma^{-m})^{-1} = \tau^y_2 \tau^1_1.$$ 

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

$$\tau^{x+1}_m \tau^{-m}_m = \tau^y_2 \tau^1_1.$$ 

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

We shall next assume that $p = 2$. In the case that $\Gamma_q$ is cyclic, the proof in the case of $p > 2$ remains valid. Assume that $\Gamma_q$ is not cyclic and let $e = 2^t$ ($t \geq 2$). Then $\Gamma_q$ 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 $\sigma_1$ and $\sigma_2$ 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

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

where $f = 2^{t-1}$. Then $\sigma_2(\alpha_1)$ belongs to the subset $\{\alpha_{f+1}, \ldots, \alpha_e\}$, because $\Gamma_q$ 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 $\Gamma_q$ is expressed uniquely as the following form:

$$\sigma^m_1 \sigma^n_2 \quad (0 \leq m < f, \, n = 0, 1)$$ 

Assume that $\sigma^m_1 \sigma^n_2$ acts trivially on $\text{Gal}(E/K)$. Let $\chi(\sigma_1) = s \mod q$. Since $\tau^2_2 \tau^1_1$ belongs to $\text{Gal}(E/K)$ by Lemma 2.5, we have

$$(1) \quad \sigma^m_1 \sigma^n_2 (\tau^2_2 \tau^1_1) \sigma^{-n}_2 \sigma^{-m}_1 = \tau^2_2 \tau^1_1.$$ 

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

$$\tau^{x+1}_m \tau^{-m}_m,$$
the index of $\tau$ being regarded as the residue class modulo $f$. If $n = 1$, the left hand side of (1) is

$$\tau^{f+m+1}_f,$$

the index of $\tau$ belongs to $\{f+1, \ldots, 2f\}$. Therefore, (1) holds if and only if $n = 0$ and $m \equiv 0 \mod f$. Hence we have $\sigma_1^m \sigma_2^n = 1$. \hfill \Box$

(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, $E_{k_{\infty}}$ is an unramified abelian extension of $k_{\infty}$ so that $k_{\infty} \subset E_{k_{\infty}} \subset L_k$. Let $X_E$ be the Galois group Gal($E_{k_{\infty}}$/$k_{\infty}$). Since $E_{k_{\infty}}$ is a Galois extension of $k$, $X_E$ is also a $\Gamma$-module, i.e., $X_E$ is a quotient of $\Gamma$-module $X$. By Lemma 2.6, the kernel of the action of $\Gamma$ on $X_E$ is Gal($k_{\infty}$/$k_{\infty}$). Therefore, Ker $\rho$ is contained in Gal($k_{\infty}$/$k_{\infty}$). Since $q$ is an arbitrary power of an arbitrary prime, it follows that Ker $\rho = \{1\}$, i.e., $\rho$ 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 $\text{PSL}_2(\mathbb{F}_p)$ 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 $\text{SL}_2(\mathbb{F}_p)$ as the Galois group such that $\mathbb{Q}_{\infty} \subset k \subset \tilde{k}$ and that the restriction Gal($\tilde{k}$/$\mathbb{Q}_{\infty}$) $\to$ Gal($k$/$\mathbb{Q}_{\infty}$) corresponds to the projection $\text{SL}_2(\mathbb{F}_p) \to \text{PSL}_2(\mathbb{F}_p)$.

(ii) There exists an unramified Galois extension $K$ of $\mathbb{Q}_{\infty}$ having $\text{SL}_2(\mathbb{Z}_p)$ 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 Gal($K$/$\mathbb{Q}_{\infty}$) $\to$ Gal($\tilde{k}$/$\mathbb{Q}_{\infty}$) corresponds to $\text{SL}_2(\mathbb{Z}_p) \to \text{SL}_2(\mathbb{F}_p)$, the reduction modulo $p$.

Proof. By the assumption, there exists a surjective homomorphism

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

such that Ker $\varphi$ corresponds to $k$.

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

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

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

\[
\omega: \text{Gal}(\bar{L}_Q/\mathbb{Q}_\infty) \to \text{SL}_2(\mathbb{Z}_p)
\]

such that \( \psi = r \omega \). Then \( \omega \) is also surjective, because no proper subgroup of \( \text{SL}_2(\mathbb{Z}_p) \) maps onto \( \text{SL}_2(\mathbb{F}_p) \) ([6, Chapter IV 3.4 Lemma 3]). Then, the extension \( K \) of \( \mathbb{Q}_\infty \) corresponding to \( \text{Ker} \omega \) 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 \( G_1, G_2, \ldots, G_n \) \((n \geq 1)\) 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 \( \text{SL}_2(\mathbb{Z}_p)^n \), the direct product of \( n \) copies of \( \text{SL}_2(\mathbb{Z}_p) \) \((n \geq 1)\). Assume that the image of \( H \) in \( \text{SL}_2(\mathbb{F}_p)^n \) by the reduction modulo \( p \) coincides with \( \text{SL}_2(\mathbb{F}_p)^n \). Then \( H \) coincides with \( \text{SL}_2(\mathbb{Z}_p)^n \).

(ii) Let \( p \geq 5 \) be a prime and \( H \) be a subgroup of \( \text{SL}_2(\mathbb{F}_p)^n \), the direct product of \( n \) copies of \( \text{SL}_2(\mathbb{F}_p) \) \((n \geq 1)\). Assume that the image of \( H \) in \( \text{PSL}_2(\mathbb{F}_p)^n \) coincides with \( \text{PSL}_2(\mathbb{F}_p)^n \). Then \( H \) coincides with \( \text{SL}_2(\mathbb{F}_p)^n \).

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 \( \text{SL}_2(\mathbb{Z}_p) \times \text{SL}_2(\mathbb{Z}_p) \). In this reduction process, the points are that the kernel of the reduction modulo \( p: \text{SL}_2(\mathbb{Z}_p) \to \text{SL}_2(\mathbb{F}_p) \) is a pro-\( p \) group and that \( \text{SL}_2(\mathbb{F}_p) \) does not have non-trivial normal subgroups with pro-\( p \)-power indices. If \( n \geq 3 \), by decomposing \( \text{SL}_2(\mathbb{Z}_p)^n = \text{SL}_2(\mathbb{Z}_p)^{n-1} \times \text{SL}_2(\mathbb{Z}_p) \), \( \text{SL}_2(\mathbb{Z}_p) \times \text{SL}_2(\mathbb{Z}_p)^{n-1} \), 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 \( \text{SL}_2(\mathbb{F}_p) \to \text{PSL}_2(\mathbb{F}_p) \) is a cyclic group of order 2 and that \( \text{PSL}_2(\mathbb{F}_p) \) does not have normal subgroups with index 2.

(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 \( \text{Gal}(k_n/\mathbb{Q}_\infty) \) is isomorphic to \( \text{PSL}_2(\mathbb{F}_p) \) and that \( k_n \neq k_m \) for \( n \neq m \). Applying Lemma 3.1 to \( k = k_n \), we obtain unramified Galois subextensions \( \tilde{k}_n \) 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) \( \text{Gal}(K_n/\mathbb{Q}_\infty) \) is isomorphic to \( \text{SL}_2(\mathbb{Z}_p) \), \( \tilde{k}_n \) and \( k_n \) corresponding to the kernels of homomorphisms \( \text{SL}_2(\mathbb{Z}_p) \to \text{SL}_2(\mathbb{F}_p) \) and \( \text{SL}_2(\mathbb{Z}_p) \to \text{PSL}_2(\mathbb{F}_p) \) 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 \( \text{Gal}(F/\mathbb{Q}_\infty) \) is isomorphic to \( \prod_{n=1}^{\infty} \text{SL}_2(\mathbb{Z}_p) \). For that purpose, it suffices to show that

\[
(*) \quad \text{Gal}(K_1 \cdots K_n/\mathbb{Q}_\infty) \text{ is isomorphic to } \text{Gal}(K_1/\mathbb{Q}_\infty) \times \cdots \times \text{Gal}(K_n/\mathbb{Q}_\infty)
\]

for all \( n \geq 1 \).

We first verify that

\[
(*)_k \quad \text{Gal}(k_1 \cdots k_n/\mathbb{Q}_\infty) \text{ is isomorphic to } \text{Gal}(k_1/\mathbb{Q}_\infty) \times \cdots \times \text{Gal}(k_n/\mathbb{Q}_\infty)
\]

for all \( n \geq 1 \).

This will be proved by induction on \( n \). For \( n = 1 \), this holds trivially. Assume that this holds for \( n = m \), so that \( \text{Gal}(k_1 \cdots k_m/\mathbb{Q}_\infty) \) is isomorphic to \( \text{PSL}_2(\mathbb{F}_p)^m \). As \( \text{Gal}(k_{m+1}/\mathbb{Q}_\infty) \) 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 \( \text{PSL}_2(\mathbb{F}_p) \) 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 \( H = \text{Gal}(K_1 \cdots K_n/\mathbb{Q}_\infty) \) and consider the commutative diagram

\[
\begin{array}{ccc}
H & \xrightarrow{r_1} & \text{Gal}(K_1/\mathbb{Q}_\infty) \times \cdots \times \text{Gal}(K_n/\mathbb{Q}_\infty) = \text{SL}_2(\mathbb{Z}_p)^n \\
\downarrow & & \downarrow \\
\text{Gal}(k_1 \cdots k_n/\mathbb{Q}_\infty) & \xrightarrow{r_2} & \text{Gal}(k_1/\mathbb{Q}_\infty) \times \cdots \times \text{Gal}(k_n/\mathbb{Q}_\infty) = \text{PSL}_2(\mathbb{F}_p)^n
\end{array}
\]

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 \( \text{PSL}_2(\mathbb{F}_p)^n \) coincides with \( \text{PSL}_2(\mathbb{F}_p)^n \). 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 \( \tilde{L}_Q/\mathbb{Q}_\infty \) and have shown that the unramified Galois extension \( k_n M_0/M_0 \) \((n \geq 1)\) has also \( \text{PSL}_2(\mathbb{F}_p) \) 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 \( M' \) of \( \tilde{L}_Q/\mathbb{Q} \). The above arguments for determining the Galois group \( H \) can be also applied to the Galois
group \( \text{Gal}(K_1 \cdots K_n M_0/M_0) \). Hence we have that the extension \( FM_0/M_0 \) is unramified and that it has \( \prod_{n=1}^\infty \text{SL}_2(\mathbb{Z}_p) \) as the Galois group.

Further, let \( \gamma \) be an element of \( \text{Gal}(M_0/M') \) and \( \tilde{\gamma} \in \text{Gal}(\tilde{L}_Q/M') \) be any extension of \( \gamma \). Then, for \( n \geq 1 \), \( \tilde{\gamma} \) transforms the field \( K_n M_0 \) to the subextension \( \tilde{\gamma}(K_n M_0) \) of \( \tilde{L}_Q/M' \), which also has \( \text{SL}_2(\mathbb{Z}_p) \) as the Galois group. This may be different from \( K_n M_0 \) because \( K_n M_0 \) is not necessarily Galois over \( M' \). 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 \( M' \) (in fact Galois over \( Q \)) 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 \( \text{Gal}(\tilde{L}_k/k) \) has the property (P).

References