TOKYO J. MATH.
VOL. 36, NO. 2, 2013

# Characterization of Arithmetical Equivalence of Number Fields by Galois Groups with Restricted Ramification

Mitsul TOHKAILIN and Manabu OZAKI

*Kinki University and Waseda University*

**Abstract.** We will give a characterization of arithmetical equivalence of number fields in terms of certain associated families of Galois groups with restricted ramification.

## 1. Introduction

The Dedekind zeta function $\zeta_K(s)$ is one of the most fundamental objects associated to a number field $K$. We believe that $\zeta_K(s)$ knows almost all the arithmetic properties of $K$. However, $\zeta_K(s)$ cannot identify completely the isomorphism class of the number field $K$ in general; For number fields $K$ and $K'$, we say that $K$ and $K'$ are *arithmetically equivalent*, denoting by $K \approx K'$, if and only if the equality $\zeta_K(s) = \zeta_{K'}(s)$ holds. Obviously, if $K \simeq K'$ then $K \approx K'$, but the converse does not hold in general. For example, $K = \mathbf{Q}(\sqrt[8]{3})$ and $K' = \mathbf{Q}(\sqrt[8]{48})$ are arithmetically equivalent, but $K \not\simeq K'$ (See [2], P. 86, (1, 9)).

Therefore it is a basic problem to determine when two number fields $K$ and $K'$ are arithmetically equivalent. The aim of the present paper is to give a characterization of arithmetical equivalence of number fields in terms of certain associated Galois groups with restricted ramification. Such an attempt was first made by N. Adachi and K. Komatsu in [1]: For any number field $F$ and prime number $p$, let $F_\infty(p)$ be the cyclotomic $\mathbf{Z}_p$-extension of $F(\zeta_p + \zeta_p^{-1})$, $\zeta_p$ being a primitive $p$-th root of unity, and denote by $X_{F_\infty(p),\{p\}}(p)$ the Galois group of the maximal abelian pro-$p$-extension over $F_\infty(p)$ unramified outside $p$. $X_{F_\infty(p),\{p\}}(p)$ has a natural $\Lambda_p := \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty(p)/\mathbf{Q})]]$-module structure as usual if $F \cap \mathbf{Q}_\infty(p) = \mathbf{Q}$, which holds for all but finitely many prime numbers $p$, via isomorphism $\mathrm{Gal}(F_\infty(p)/F) \simeq \mathrm{Gal}(\mathbf{Q}_\infty(p)/\mathbf{Q})$ induced by the restriction.

THEOREM (Adachi-Komatsu [1]). *Let $K$ and $K'$ be totally real number fields. Then the followings are equivalent*:

Received April 24, 2012; revised September 26, 2012
*Mathematics Subject Classification*: 11R42
*Key words and phrases*: arithmetical equivalence
This research was partially supported by JSPS, the Grant-in-Aid for Scientific Research (C) 21540030, and Waseda University, Grant for Special Research Projects 2012A-030.

(1) $K \approx K'$,
(2) $X_{K_\infty(p),\{p\}}(p) \simeq X_{K'_\infty(p),\{p\}}(p)$ *as* $\Lambda_p$*-modules for all but finitely many prime numbers* $p$.

It is not clear whether we can omit the assumption "totally real" in the above theorem, because the proof of "(2)$\Longrightarrow$(1)" largely relies on the Iwasawa main conjecture for totally real number fields, which was established by A. Wiles.

Our main result gives a characterization of arithmetical equivalence of any number fields in terms of a family of rather "small" Galois groups with restricted ramification, which are finite abelian groups.

## 2. Main theorem

In what follows, we will fix an algebraic closure of $\mathbf{Q}$ and regard any number fields and their algebraic extensions as subfields of it. For any set $S$ of prime numbers and number field $F$, we denote by $M_{F,S}$ the maximal abelian extension over $F$ unramified outside $S$, and let $X_{F,S} := \mathrm{Gal}(M_{F,S}/F)$.

Our main result is the following:

THEOREM 1. *For number fields $K$ and $K'$ of finite degree, the following three statements are equivalent*:

(1) $K \approx K'$,
(2) *There exists a prime number $l_0$ such that*
(i) $l_0 \nmid [N : \mathbf{Q}]$ *for the minimal Galois extension $N/\mathbf{Q}$ containing $K$ and $K'$*,
(ii) *$l_0$ does not divide the class numbers of $K$ and $K'$*,
(iii) *$l_0$ is unramified in $K/\mathbf{Q}$ and $K'/\mathbf{Q}$*,
(iv) $X_{K,\{p\}}/l_0 \simeq X_{K',\{p\}}/l_0$ *for all but finitely many prime numbers $p$.*
(3) *Let $N/\mathbf{Q}$ be the minimal Galois extension containing both of $K$ and $K'$. Then for any set $S$ of prime numbers and prime number $l$ satisfying $l \nmid [N : \mathbf{Q}]$, we have $X_{K,S}(l) \simeq X_{K',S}(l)$, where $X_{K,S}(l)$ and $X_{K',S}(l)$ denote the $l$-parts of $X_{K,S}$ and $X_{K',S}$, respectively.*

## 3. Preliminary lemmas

In this section, we will give a collection of preliminary lemmas to prove Theorem 1.

The following lemma is well known:

LEMMA 1. *Let $L/K$ be a finite extension of number fields and $N/K$ a Galois extension containing $L$. Put $G = \mathrm{Gal}(N/K)$, $H = \mathrm{Gal}(N/L)$. For any prime ideal $\mathfrak{p}$ of $K$, we denote by $P_\mathfrak{p}$ the set of the prime ideals of $L$ lying above $\mathfrak{p}$. Also, let $\mathfrak{P}$ be a prime ideal of $N$ lying above $\mathfrak{p}$ and $G_\mathfrak{P}$ the decomposition subgroup group of $G$ for $\mathfrak{P}$. Then the map*

$$\begin{array}{ccc} H \backslash G/G_\mathfrak{P} & \longrightarrow & P_\mathfrak{p} \\ H\sigma G_\mathfrak{P} & \longmapsto & \sigma\mathfrak{P} \cap L \end{array}$$

*is a bijection. In the case where* $\mathfrak{p}$ *is unramified in* $N/K$, *we find especially the number of the prime ideals of* $L$ *lying over* $\mathfrak{p}$ *depends only on the Frobenius class of* $\mathfrak{p}$ *in* $G$, *namely*, *the conjugacy class of the Frobenius automorphism* $\left[\frac{N/K}{\mathfrak{P}}\right]$ *for* $\mathfrak{P}$. □

LEMMA 2. *For a prime power* $r$, *we denote by* $\mathbf{F}_r$ *the finite field of order* $r$. *If a prime number* $l$ *and a positive integer* $d$ *satisfy* $l \nmid d$ *and* $l \mid r-1$ , *then we have*

$$(\mathbf{F}_{r^d}^{\times})^l \cap \mathbf{F}_r^{\times} = (\mathbf{F}_r^{\times})^l .$$

PROOF. Because the inclusion $(\mathbf{F}_{r^d}^{\times})^l \cap \mathbf{F}_r^{\times} \supseteq (\mathbf{F}_r^{\times})^l$ clearly holds, it is enough to show that the converse inclusion $(\mathbf{F}_{r^d}^{\times})^l \cap \mathbf{F}_r^{\times} \subseteq (\mathbf{F}_r^{\times})^l$ holds. Assume that $x \in \mathbf{F}_{r^d}^{\times}$ and $x^l \in \mathbf{F}_r^{\times}$. Then we have $(x^{r-1})^l = x^{l(r-1)} = 1$. Suppose that the order $\mathrm{ord}(x^{r-1})$ of $x^{r-1} \in \mathbf{F}_{r^d}^{\times}$ is equal to $l$. Then it follows from $x^{(r-1)\cdot\frac{r^d-1}{r-1}} = x^{r^d-1} = 1$ that $l \mid \frac{r^d-1}{r-1}$. However, this is impossible by $\frac{r^d-1}{r-1} = r^{d-1} + r^{d-2} + \cdots + r + 1 \equiv d \not\equiv 0 \pmod{l}$. Therefore we conclude that $x^{r-1} = 1$, which implies $x \in \mathbf{F}_r$. □

LEMMA 3. *Let* $G$ *be a finite group and* $p$ *a prime number with* $p \nmid \#G$. *Assume that two subgroups* $H_1, H_2 \subseteq G$ *satisfy*

$$\mathbf{Q}_p[G] \underset{\mathbf{Q}_p[H_1]}{\otimes} \mathbf{Q}_p \simeq \mathbf{Q}_p[G] \underset{\mathbf{Q}_p[H_2]}{\otimes} \mathbf{Q}_p \ (\textit{as } \mathbf{Q}_p[G]\textit{-modules}) .$$

*Here we regard* $\mathbf{Q}_p[G]$ *as a two-sided* $\mathbf{Q}_p[G]$*-module via the ring structure of it*, *and the action of* $G$ *on* $\mathbf{Q}_p[G] \underset{\mathbf{Q}_p[H_i]}{\otimes} \mathbf{Q}_p$ *is defined by* $\sigma(a \otimes b) = \sigma a \otimes b$ $(a \in \mathbf{Q}_p[G],\ b \in \mathbf{Q}_p,\ \sigma \in G)$. *Then for any* $\mathbf{Z}_p[G]$*-module* $M$, *we have*

$$M_{H_1} \simeq M_{H_2} \ (\textit{as } \mathbf{Z}_p\textit{-modules}) ,$$

*where* $M_{H_i} = M/\sum_{\sigma \in H_i}(\sigma - 1)M$ *is the* $H_i$*-coinvariant of* $M$.

PROOF. We recall the following lemma from the theory of integral representations of finite groups to prove Lemma 3:

LEMMA 4 ([2, p.626, (30, 16)]). *Let* $G$ *be a finite group and* $p$ *a prime number with* $p \nmid \#G$. *For any finitely generated* $\mathbf{Z}_p[G]$*-modules* $A$ *and* $B$ *without non-trivial* $\mathbf{Z}_p$*-torsions*, $A \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p \simeq B \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p$ *as* $\mathbf{Q}_p[G]$*-modules implies* $A \simeq B$ *as* $\mathbf{Z}_p[G]$*-modules.* □

It follows from

$$(\mathbf{Z}_p[G] \underset{\mathbf{Z}_p[H_i]}{\otimes} \mathbf{Z}_p) \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p \simeq \mathbf{Q}_p[G] \underset{\mathbf{Q}_p[H_i]}{\otimes} \mathbf{Q}_p \ (\text{as } \mathbf{Q}_p[G]\text{-modules}) \ (i = 1, 2) ,$$

and our assumption

$$\mathbf{Q}_p[G] \underset{\mathbf{Q}_p[H_1]}{\otimes} \mathbf{Q}_p \simeq \mathbf{Q}_p[G] \underset{\mathbf{Q}_p[H_2]}{\otimes} \mathbf{Q}_p \ (\text{as } \mathbf{Q}_p[G]\text{-modules}) ,$$

that

$$\mathbf{Z}_p[G] \underset{\mathbf{Z}_p[H_1]}{\otimes} \mathbf{Z}_p \simeq \mathbf{Z}_p[G] \underset{\mathbf{Z}_p[H_2]}{\otimes} \mathbf{Z}_p \text{ (as } \mathbf{Z}_p[G]\text{-modules)}$$

by using Lemma 4. Hence we obtain

$$M \underset{\mathbf{Z}_p[G]}{\otimes} (\mathbf{Z}_p[G] \underset{\mathbf{Z}_p[H_1]}{\otimes} \mathbf{Z}_p) \simeq M \underset{\mathbf{Z}_p[G]}{\otimes} (\mathbf{Z}_p[G] \underset{\mathbf{Z}_p[H_2]}{\otimes} \mathbf{Z}_p) \tag{1}$$

as $\mathbf{Z}_p$-modules, where we define the right action of $\sigma \in G$ on $m \in M$ by $m\sigma := \sigma^{-1}m$ to give a right $\mathbf{Z}_p[G]$-module structure to $M$.

On the other hand, by the associative law of tensor product, we have

$$M \underset{\mathbf{Z}_p[G]}{\otimes} (\mathbf{Z}_p[G] \underset{\mathbf{Z}_p[H_i]}{\otimes} \mathbf{Z}_p) \simeq (M \underset{\mathbf{Z}_p[G]}{\otimes} \mathbf{Z}_p[G]) \underset{\mathbf{Z}_p[H_i]}{\otimes} \mathbf{Z}_p \simeq M \underset{\mathbf{Z}_p[H_i]}{\otimes} \mathbf{Z}_p \simeq M_{H_i}$$

as $\mathbf{Z}_p$-modules for $i = 1, 2$, where we regard $M \underset{\mathbf{Z}_p[G]}{\otimes} \mathbf{Z}_p[G]$ as a right $H_i$-module via $(m \otimes \alpha)h := m \otimes \alpha h$ for $m \in M, \alpha \in \mathbf{Z}_p[G], h \in H_i$. Therefore it follows from (1) that $M_{H_1} \simeq M_{H_2}$ as $\mathbf{Z}_p$-modules. □

The following is the key to derive the equivalence of the three statements in Theorem 1:

LEMMA 5 [3, P. 77, (1.3)]. *Let $K$ and $K'$ be any number fields. Then the following three statements are equivalent*:

(1) $K \approx K'$

(2) *For a prime number $p$, let $g_p$ and $g'_p$ be the numbers of the prime divisors of $K$ and $K'$ lying over $p$, respectively. Then $g_p = g'_p$ for all but finitely many prime numbers $p$.*

(3) *For any Galois extension $N/\mathbf{Q}$ containing $K$ and $K'$, put $G = \mathrm{Gal}(N/\mathbf{Q})$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/K')$. Then $\mathbf{Q}[G] \underset{\mathbf{Q}[H]}{\otimes} \mathbf{Q} \simeq \mathbf{Q}[G] \underset{\mathbf{Q}[H']}{\otimes} \mathbf{Q}$ as $\mathbf{Q}[G]$-modules.*

LEMMA 6 ([4, p.41, Thm. 2.3.15]). *Let $G$ be a pro-finite group and $N \subseteq G$ a pro-$p$ normal subgroup. Assume that the quotient group $Q = G/N$ has no non-trivial pro-$p$-subgroups. Then the natural exact sequence*

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

*splits.* □

## 4. Proof of Theorem 1

PROOF. First, we will derive statement (1) from statement (2).

Assume that the prime number $l_0$ satisfies the condition given in statement (2) of the theorem. For a prime number $q$ and $n \geq 0$, we write $K_{q^n}$ for the ray class field of modulo

$q^n\mathcal{O}_K$ over $K$, $\mathcal{O}_K$ being the integer ring of $K$. Then $M_{K,\{q\}} = \bigcup_{n=1}^{\infty} K_{q^n}$, and $X_{K,\{q\}} = \varprojlim_n \mathrm{Gal}(K_{q^n}/K)$. We denote by $I_{K,q}$ the group of the fractional ideals of $K$ which are prime to $q$, and we write $P_{K,q}$ for the group of the principal ideals contained in $I_{K,q}$. Also, we put $S_{K,q^n} = \{\alpha\mathcal{O}_K | \alpha \in K^\times, \alpha \equiv 1 \pmod{q^n}\}$.

If we assume $q \neq l_0$, then, by using class field theory, we have

$$X_{K,\{q\}}/l_0 \simeq \mathrm{Gal}(K_q/K)/l_0 \simeq (I_{K,q}/S_{K,q})/l_0 \simeq (P_{K,q}/S_{K,q})/l_0 \tag{2}$$

because $\mathrm{Gal}(K_{q^n}/K_q)$ is a $q$-group ($q \neq l_0$) and the $l_0$-part of the class group of $K$, which is isomorphic to that of $I_{K,q}/P_{K,q}$, is trivial from our assumption. Thus we derive from the exact sequence

$$\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/q)^\times \longrightarrow P_{K,q}/S_{K,q} \longrightarrow 0$$

and (2) the exact sequence

$$\mathcal{O}_K^\times \xrightarrow{\pi_{K,q}} (\mathcal{O}_K/q)^\times/l_0 \longrightarrow X_{K,\{q\}}/l_0 \longrightarrow 0\,. \tag{3}$$

Assume that the prime $q$ is unramified in $K/\mathbf{Q}$ and let $q\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_{g_q}$ be the prime decomposition in $K$. Then it follows from the Chinese Remainder Theorem that

$$(\mathcal{O}_K/q)^\times/l_0 \simeq \bigoplus_{i=1}^{g_q} (\mathcal{O}_K/\mathfrak{q}_i)^\times/l_0\,.$$

If we further assume that $q \equiv 1 \pmod{l_0}$, then

$$(\mathcal{O}_K/q)^\times/l_0 \simeq \bigoplus_{i=1}^{g_q} (\mathcal{O}_K/\mathfrak{q}_i)^\times/l_0 \simeq (\mathbf{Z}/l_0)^{\oplus g_q}\,. \tag{4}$$

Recall that $N/\mathbf{Q}$ denotes the minimal Galois extension containing $K$ and $K'$. Put $L = N(\mu_{l_0}, \{\sqrt[l_0]{\varepsilon} \,|\, \varepsilon \in \mathcal{O}_N^\times\})$, $G_N = \mathrm{Gal}(N/\mathbf{Q})$, $G_{N(\mu_{l_0})} = \mathrm{Gal}(N(\mu_{l_0})/\mathbf{Q})$, and $G_L = \mathrm{Gal}(L/\mathbf{Q})$, where $\mu_{l_0}$ stands for the group of the $l_0$-th roots of unity. We note that $[L : N(\mu_{l_0})] = l_0^e$ for some $e \geq 0$, and that $[N(\mu_{l_0}) : \mathbf{Q}]$ is prime to $l_0$ from our assumption. For any Galois extension $F/\mathbf{Q}$ and prime number $q$ which is unramified in $F$, we set $C_{F/\mathbf{Q}}(q) = \left\{\left[\frac{F/\mathbf{Q}}{\mathfrak{q}}\right] \,\middle|\, \mathfrak{q} \mid q \text{ is a prime of } F\right\}$, and for any group $G$ and $\sigma \in G$, put $C(G,\sigma) = \{g\sigma g^{-1} | g \in G\}$.

In what follows, we will show that for any $\sigma \in G_N$ there exist infinitely many prime numbers $q$ satisfying the following three conditions:

(a) $q \equiv 1 \pmod{l_0}$,

(b) the prime $q$ is unramified in $L$ and $C_{N/\mathbf{Q}}(q) = C(G_N, \sigma)$,

(c) $\langle x \rangle \cap \mathrm{Gal}(L/N) = \{1\}$ for all $x \in C_{L/\mathbf{Q}}(q)$.

Since $l_0$ is unramified in $N/\mathbf{Q}$ from our assumption on $l_0$, we have $N \cap \mathbf{Q}(\mu_{l_0}) = \mathbf{Q}$ and the isomorphism

$$\begin{array}{ccc} G_{N(\mu_{l_0})} & \simeq & G_N \times \mathrm{Gal}(\mathbf{Q}(\mu_{l_0})/\mathbf{Q}) \, . \\ x & \mapsto & \big(x \mid_N, x \mid_{\mathbf{Q}(\mu_{l_0})}\big) \end{array}$$

We will identify $G_{N(\mu_{l_0})}$ with $G_N \times \mathrm{Gal}(\mathbf{Q}(\mu_{l_0})/\mathbf{Q})$ via the above isomorphism. Let $\bar{\sigma} \in G_L$ be an automorphism such that $\bar{\sigma} \mid_{N(\mu_{l_0})} = (\sigma, 1)$. Because $l_0 \nmid \#G_N$ by our assumption on $l_0$, there exists a positive integer $d$ such that $d \equiv 1 \pmod{\#G_N}$ and $d \equiv 0 \pmod{l_0^e}$. Put $y = \bar{\sigma}^d \in G_L$. Then we see that $y|_{N(\mu_{l_0})} = (\sigma^d, 1^d) = (\sigma, 1) = \bar{\sigma}|_{N(\mu_{l_0})}$ and $(\mathrm{ord}\, y, l_0) = 1$ since $l_0^e \,\|\, \#G_L$. By the Chebotarev density theorem, there exist infinitely many prime numbers $q$ such that $q$ is unramified in $L$ and $C_{L/\mathbf{Q}}(q) = C(G_L, y)$. We will show that this prime number $q$ satisfies conditions (a), (b), and (c).

For any subset $C$ of $G_L$, we put $C|_N = \{g|_N \in G_N | \, g \in C\}$. Then we have $C_{N/\mathbf{Q}}(q) = C(G_L, y)|_N = C(G_N, y|_N) = C(G_N, \sigma)$, which implies that $q$ satisfies (b). Since $C_{\mathbf{Q}(\mu_{l_0})/\mathbf{Q}}(q) = C_{L/\mathbf{Q}}(q)|_{\mathbf{Q}(\mu_{l_0})} = C(G_L, y) \mid_{\mathbf{Q}(\mu_{l_0})} = 1$, we see that $\left(\frac{\mathbf{Q}(\mu_{l_0})/\mathbf{Q}}{q}\right) = 1$, which implies that $q$ satisfies (a). Finally, let $x \in C_{L/\mathbf{Q}}(q)$ and $g \in \langle x \rangle \cap \mathrm{Gal}(L/N)$ be any element. Since $x \in C_{L/\mathbf{Q}}(q) = C(G_L, y)$, we find that $x = zyz^{-1}$ for some $z \in G_L$. Then we obtain $g = (zyz^{-1})^m$ for some $m \in \mathbf{Z}$. Because $y|_{\mathbf{Q}(\mu_{l_0})} = 1$, we have $g \mid_{\mathbf{Q}(\mu_{l_0})} = (zy^m z^{-1}) \mid_{\mathbf{Q}(\mu_{l_0})} = z \mid_{\mathbf{Q}(\mu_{l_0})} z^{-1} \mid_{\mathbf{Q}(\mu_{l_0})} = 1$. Hence we obtain $g \in \mathrm{Gal}(L/N) \cap \mathrm{Gal}(L/\mathbf{Q}(\mu_{l_0})) = \mathrm{Gal}(L/N(\mu_{l_0}))$. It follows from the facts $\mathrm{ord}\, g = \mathrm{ord}\,(zyz^{-1})^m = \mathrm{ord}\, y^m$ and $(\mathrm{ord}\, y, l_0) = 1$ that $(\mathrm{ord}\, g, l_0) = 1$, which implies $g = 1$ since $\mathrm{Gal}(L/N(\mu_{l_0}))$ is an $l_0$-group. Hence we find that $q$ satisfies (c). Thus we conclude that $q$ satisfies conditions (a), (b) and (c).

Let $p$ be any prime number which is unramified in $N/\mathbf{Q}$. By the above discussion, there exist infinitely many prime numbers $q$ such that (a) $q \equiv 1 \pmod{l_0}$, (b′) $q$ is unramified in $L$ and $C_{N/\mathbf{Q}}(q) = C_{N/\mathbf{Q}}(p)$, and (c) $\langle x \rangle \cap \mathrm{Gal}(L/N) = \{1\}$ for all $x \in C_{L/\mathbf{Q}}(q)$. Furthermore, by our assumption, we may assume that the prime number $q$ satisfies condition (iv) of statement (2), that is, $X_{K,\{q\}}/l_0 \simeq X_{K',\{q\}}/l_0$. Condition (c) implies that all the prime ideals of $N$ lying over $q$ are completely decomposed in $L/N$. Hence, for any prime $\mathfrak{q}_K$ of $K$ lying over $q$ and a prime $\mathfrak{q}_N$ of $N$ lying over $\mathfrak{q}_K$, we obtain the inclusion and the isomorphism

$$(\mathcal{O}_K/\mathfrak{q}_K)^\times \hookrightarrow (\mathcal{O}_N/\mathfrak{q}_N)^\times \simeq (\mathcal{O}_L/\mathfrak{Q})^\times$$

for a prime $\mathfrak{Q}$ of $L$ lying over $\mathfrak{q}_N$. We see that $l_0 \nmid [\mathcal{O}_N/\mathfrak{q}_N : \mathcal{O}_K/\mathfrak{q}_K]$ from our assumption on $l_0$. Since $(\varepsilon \bmod \mathfrak{q}_K) \in (\mathcal{O}_K/\mathfrak{q}_K)^\times$ maps to $((\sqrt[l_0]{\varepsilon})^{l_0} \bmod \mathfrak{Q}) \in ((\mathcal{O}_L/\mathfrak{Q})^\times)^{l_0}$ for any $\varepsilon \in \mathcal{O}_K^\times$, it follows from Lemma 2 that $(\varepsilon \bmod \mathfrak{q}_K) \in ((\mathcal{O}_K/\mathfrak{q}_K)^\times)^{l_0}$ for any $\varepsilon \in \mathcal{O}_K^\times$, which implies $\pi_{K,q}(\mathcal{O}_K^\times) = 0$, where $\pi_{K,q}$ is the map defined in (3). Therefore we derive from condition (a), (3) and (4) that

$$X_{K,\{q\}}/l_0 \simeq (\mathbf{Z}/l\mathbf{Z})^{\oplus g_q} ,$$

where $g_q$ is the number of primes of $K$ lying over $q$. Similarly, we also have

$$X_{K',\{q\}}/l_0 \simeq (\mathbf{Z}/l\mathbf{Z})^{\oplus g'_q} ,$$

where $g'_q$ is a number of primes of $K'$ lying over $q$. Therefore we see by using our assumption $X_{K,\{q\}}/l_0 \simeq X_{K',\{q\}}/l_0$ that $g_q = g'_q$. On the other hand, it follows from property (b$'$) of the prime $q$ and Lemma 1 that $g_p = g_q$ and $g'_p = g'_q$. Thus we have shown that $g_p = g'_p$ for any prime number $p$ which is unramified in $N/\mathbf{Q}$. Therefore, by using Lemma 5 ((2)$\Longrightarrow$(1)), we conclude $K \approx K'$.

Next, we will derive statement (3) of the theorem assuming statement (1) holds.

Let $l$ be any prime number which satisfies $l \nmid [N : \mathbf{Q}]$. Since $l \nmid [N : K]$ and $M_{K,S}(l)/K$ is a pro-$l$-extension, we see $N \cap M_{K,S}(l) = K$. Put $F = NM_{K,S}(l)$ and $H = \mathrm{Gal}(N/K)$. We will show that $\mathrm{Gal}(F/N) \simeq (X_{N,S}(l))_H$, where we regard $X_{N,S}(l)$ as a $\mathrm{Gal}(N/\mathbf{Q})$-module via inner automorphism of $\mathrm{Gal}(M_{N,S}(l)/\mathbf{Q})$ induced by an extension of each element of $\mathrm{Gal}(N/\mathbf{Q})$ to $\mathrm{Gal}(M_{N,S}(l)/\mathbf{Q})$.

Let $F'$ be the intermediate field of $M_{N,S}(l)/N$ which satisfies $\mathrm{Gal}(F'/N) \simeq (X_{N,S}(l))_H$. It follows from Lemma 6 together with the fact that $H$ acts trivially on $\mathrm{Gal}(F'/N)$ that $\mathrm{Gal}(F'/K)$ admits a direct product decomposition

$$\mathrm{Gal}(F'/K) = \mathrm{Gal}(F'/N) \times \mathrm{Gal}(F'/E)$$

for some sub-Galois-extension $E/K$ of $F'/K$ with $\mathrm{Gal}(F'/E) \simeq H$ and $\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(F'/N)$. Since $\mathrm{Gal}(E/K)$ is a pro-$l$ abelian group and the order of $\mathrm{Gal}(F'/E)$ is prime to $l$, we see that $E \subseteq M_{K,S}(l)$. Hence $F' = NE \subseteq NM_{K,S}(l) = F$. Conversely, because $F \subseteq M_{N,S}(l)$ and the action of $H$ on $\mathrm{Gal}(F/N)$ is trivial, we find that $F \subseteq F'$. Thus we have shown $F = F'$. Therefore we have

$$(X_{N,S}(l))_H \simeq \mathrm{Gal}(F/N) \simeq X_{K,S}(l) ,$$

since $N \cap M_{K,S}(l) = K$. Similarly, we obtain

$$(X_{N,S}(l))_{H'} \simeq X_{K',S}(l)$$

for $H' = \mathrm{Gal}(N/K')$. Then it follows from Lemma 5 ((1)$\Longrightarrow$(3)) and Lemma 3 that

$$X_{K,S}(l) \simeq (X_{N,S}(l))_H \simeq (X_{N,S}(l))_{H'} \simeq X_{K',S}(l) .$$

Thus we have shown that statement (3) holds.

Finally, it is obvious that statement (3) implies statement (2). This completes the proof of Theorem 1. □

## References

[ 1 ] N. ADACHI and K. KOMATSU, The maximal $p$-extensions and zeta-functions of algebraic number fields, Mem. School Sci. Engrg. Waseda Univ. No. **51** (1987), 25–31.

[ 2 ] C. W. CURTIS and I. REINER, *Methods of representation theory Vol. I*, John Wiley & Sons, Inc., New York (1990).

[ 3 ] N. KLINGEN, *Arithmetical Similarities*, Clarendon Press, Oxford (1998).

[ 4 ] L. RIBES and P. ZALESSKII, *Profinite Groups,* A series of Modern surveys in Mathematics, vol. 40, Springer (1991).

*Present Addresses*:
MITSUL TOHKAILIN
DEPARTMENT OF MATHEMATICS,
FACULTY OF SCIENCE AND TECHNOLOGY,
KINKI UNIVERSITY,
3–4–1, KOWAKAE, HIGASHI-OSAKA, 577–8502 JAPAN.
*e-mail*: tohkailin@math.kindai.ac.jp

MANABU OZAKI
DEPARTMENT OF MATHEMATICS,
SCHOOL OF FUNDAMENTAL SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
3–4–1, OHKUBO, SHINJUKU-KU, TOKYO, 169–8555 JAPAN.
*e-mail*: ozaki@waseda.jp