J. Math. Soc. Japan
Vol. 66, No. 4 (2014) pp. 1091–1103
doi: 10.2969/jmsj/06641091

On the ideal class groups of the maximal cyclotomic extensions of algebraic number fields

By Mamoru Asada

(Received Sep. 25, 2012)

Abstract. We shall consider the maximal cyclotomic extension of a totally real finite algebraic number field and its ideal class group. We shall investigate the structure of the ideal class group with the action of the cyclotomic Galois group.

Introduction.

Let k_0 be a finite algebraic number field contained in the field of complex numbers $\mathbb{C}$ and ζ_n denote a primitive n-th root of 1 ($n \geq 1$). Let k_∞ be the maximal cyclotomic extension of k_0, i.e. the field obtained by adjoining all ζ_n ($n \geq 1$) to k_0. Further, let k_1 be the subextension of k_∞/k_0 which is obtained by adjoining ζ_4 and ζ_l for all odd prime l to k_0 and consider the Galois group $\mathfrak{g} = \mathrm{Gal}(k_\infty/k_1)$. As readily seen, $\mathfrak{g}$ is isomorphic to the additive group of the profinite completion $\widehat{\mathbb{Z}}$ of the ring of rational integers $\mathbb{Z}$.

In our previous paper [**1**], we have determined the profinite $\mathfrak{g}$-module structure of the Galois group of the maximal abelian extension of k_∞ with certain restricted ramifications. In this paper, by a similar method, we shall investigate the ideal class group of k_∞, which is a discrete $\mathfrak{g}$-module.

The ideal class group C_∞ of k_∞ is, by definition,

$$C_\infty = \varinjlim C_{F_\lambda},$$

where $\{F_\lambda\}$ is the family of all finite subextensions of k_∞/k_0, C_{F_λ} denotes the ideal class group of F_λ and the inductive limit is taken with respect to natural homomorphisms $C_{F_\lambda} \to C_{F_\mu}$ for $F_\lambda \subset F_\mu$. As C_F is a finite abelian group, C_∞ is a discrete torsion abelian group. Therefore, C_∞ is a direct sum of its p-primary components $C_\infty(p)$ for all prime numbers p;

$$C_\infty = \bigoplus_p C_\infty(p).$$

It is known, by Brumer [**2**], that C_∞ is isomorphic to the direct sum of countable number of copies of $\mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}$ and $\mathbb{Z}$ denote the additive group of rational numbers and that

2010 *Mathematics Subject Classification.* Primary 11R18, 11R23.
Key Words and Phrases. ideal class groups, cyclotomic extensions.
The author is partially supported by the Grant-in-Aid for Scientific Research (C), Japan Society for the Promotion of Science.

of rational integers respectively. Therefore, $C_\infty(p)$ is isomorphic to the direct sum of countable number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$, $\mathbb{Q}_p$ and $\mathbb{Z}_p$ being the additive group of p-adic numbers and that of p-adic integers respectively;

$$C_\infty(p) \simeq \bigoplus_{N=1}^{\infty} (\mathbb{Q}_p/\mathbb{Z}_p).$$

The Galois group $\mathrm{Gal}(k_\infty/k_0)$ acts naturally on C_∞ and to describe the structure of C_∞ as $\mathrm{Gal}(k_\infty/k_0)$-module seems to be a fundamental but difficult problem. When we restrict the action of $\mathrm{Gal}(k_\infty/k_0)$ to that of the subgroup $\mathfrak{g}$ and assume that k_0 is totally real, we can determine the $\mathfrak{g}$-module structure of the minus part $C_\infty(p)^-$ of $C_\infty(p)$ for an odd prime p completely. This is the main result of this paper.

To be precise, let k_∞^+ denote the maximal totally real subfield of k_∞. The complex conjugation ρ, which is a generator of the Galois group $\mathrm{Gal}(k_\infty/k_\infty^+)$, acts on $C_\infty(p)$. Put

$$C_\infty(p)^\pm = \{c \in C_\infty(p) \mid c^\rho = \pm c\}.$$

Then, as p is odd, we have the direct sum decomposition

$$C_\infty(p) = C_\infty(p)^+ \oplus C_\infty(p)^-$$

as discrete $\mathfrak{g}$-modules. A result of Kurihara [**6**] indicates that $C_\infty(p)^+ = \{0\}$ so that we have $C_\infty(p) = C_\infty(p)^-$.

Let $W(p)$ denote the group of all p-powerth roots of unity. For a pro-p $\mathfrak{g}$-module X, let $\mathrm{Hom}(X, W(p))$ denote the set of continuous homomorphisms from X to $W(p)$. The group $\mathfrak{g}$ acts on $\mathrm{Hom}(X, W(p))$ by

$$\sigma(f)(x) = \sigma(f(\sigma^{-1}(x))) \quad (\sigma \in \mathfrak{g},\ f \in \mathrm{Hom}(X, W(p)),\ x \in X),$$

so that $\mathrm{Hom}(X, W(p))$ is a discrete $\mathfrak{g}$-module.

Let $\mathcal{A}_p$ denote the completed group algebra of $\mathfrak{g}$ over $\mathbb{Z}_p$, which is a pro-p $\mathfrak{g}$-module, and let $\mathfrak{C}_p = \mathrm{Hom}(\mathcal{A}_p, W(p))$. Our main result is the following

MAIN THEOREM. *Let p be an odd prime. Then, as discrete $\mathfrak{g}$-modules, $C_\infty(p)^-$ is isomorphic to the direct sum of countable number of copies of $\mathfrak{C}_p$;*

$$C_\infty(p)^- \simeq \bigoplus_{N=1}^{\infty} \mathfrak{C}_p.$$

Let M_p^+ denote the maximal pro-p abelian extension of k_∞^+ unramified outside p and k_1^+ denote the maximal totally real subfield of k_1. As M_p^+ is a Galois extension of k_1^+, the Galois group $\mathrm{Gal}(M_p^+/k_\infty^+)$ is naturally a pro-p $\mathrm{Gal}(k_\infty^+/k_1^+)$-module, and hence a pro-p $\mathfrak{g}$-module via the isomorphism $\mathrm{Gal}(k_\infty^+/k_1^+) \simeq \mathfrak{g}$. It is known that we have, as

$\mathfrak{g}$-modules, an isomorphism

$$C_\infty(p)^- \simeq \mathrm{Hom}\big(\mathrm{Gal}(M_p^+/k_\infty^+),\ W(p)\big).$$

This will be recalled in Section 1. Therefore, the above theorem can be formulated as the following

THEOREM. *Let p be an odd prime. Then, as pro-p $\mathfrak{g}$-modules,* $\mathrm{Gal}(M_p^+/k_\infty^+)$ *is isomorphic to* $\prod_{N=1}^\infty \mathcal{A}_p$, *the direct product of countable number of copies of* $\mathcal{A}_p$.

What we shall prove is this theorem. That $C_\infty(p)$ is isomorphic to the dual of a certain Galois group holds for an arbitrary finite algebraic number field k_0 and for an arbitrary prime p. We can not, however, determine the structure of this Galois group in general cases.

For the proof of the above theorem, as an algebraic tool, we use a characterization of the pro-p $\mathfrak{g}$-module $\prod_{N=1}^\infty \mathcal{A}_p$ in terms of the solvability of embedding problems and an obvious topological condition. This will be recalled in Section 2.

To solve embedding problems for the $\mathcal{A}_p$-module $\mathrm{Gal}(M_p^+/k_\infty^+)$, we shall show, in Section 4, that the Galois group $\mathrm{Gal}(\tilde{M}_p^+/k_1^+)$ is projective (Theorem 4.1). Here $\tilde{M}_p^+$ denotes the maximal pro-p extension of k_∞^+ unramified outside p. An arithmetical point for this is that, for every prime l, the field $k_1^+\mathbb{Q}_l$ contains the maximal unramified extension of $\mathbb{Q}_l$.

Although the proof of Theorem 4.1 is a modification of that of our previous result [**1**, Theorem 2.1], which originates in that of a result of Uchida [**10**, Theorem 1], we shall give details of the proof, since there are some technical points arising from the fact that k_1^+ does not contain a primitive p-th root of unity. As preparations of Section 4, we summarize in Section 3, after Reichardt [**7**] and Shafarevich [**9**], Galois theoretical results on embedding problems for p-groups. In Section 5 we shall complete the proof of the above theorem.

The author expresses his sincere gratitudes to Professor Humio Ichimura for stimulating discussions, especially for explaining corresponding results of Iwasawa theory.

1. Ideal class groups.

1.1. The ideal class group $C_\infty(p)$ is canonically isomorphic to the character group of a certain Galois group (Iwasawa [**5**], cf. also Horie [**3**]). We shall briefly explain this.

Let k_0 be an arbitrary finite algebraic number field and k_∞ be the maximal cyclotomic extension of k_0. Let p be an arbitrary prime and M_p denote the maximal pro-p abelian extension of k_∞ unramified outside p. Further, let N_p be the field obtained by adjoining to k_∞ all p-powerth roots of all units of k_∞. Then, M_p and N_p are both Galois extensions of k_0 and N_p is a subfield of M_p.

Let $X = \mathrm{Gal}(M_p/N_p)$. For each element c of $C_\infty(p)$, a character χ_c of X is associated as follows. Take an ideal A belonging to c. Then, for some power m of p, A^m is principal; $A^m = (a)$ $(a \in k_\infty)$. Let α be an m-th root of a and define the character χ_c of X by

$$\chi_c(\sigma) = \sigma(\alpha)\alpha^{-1} \quad (\sigma \in X).$$

As can be easily verified, χ_c does not depend on the choices of A, m, a, α and is uniquely determined by c. Further, this correspondence $c \to \chi_c$ gives an isomorphism of abelian groups

$$C_\infty(p) \simeq \mathrm{Hom}(X,\ W(p)). \tag{1}$$

1.2. Now we shall restrict ourselves to the case that k_0 is a totally real finite algebraic number field and p is an odd prime.

As before, let k_1 denote the field obtained by adjoining ζ_4 and ζ_l for all odd prime l to k_0. Let k_1^+ denote the maximal totally real subfield of k_1. Since k_∞, N_p, and M_p are all Galois extensions of k_1^+, the Galois group $\mathrm{Gal}(k_\infty/k_1^+)$ acts on $\mathrm{Hom}(X, W(p))$ by

$$\sigma(\chi)(x) = \sigma(\chi(\sigma^{-1}(x))) \quad \big(\sigma \in \mathrm{Gal}(k_\infty/k_1^+),\ \chi \in \mathrm{Hom}(X, W(p)),\ x \in X\big).$$

The Galois group $\mathrm{Gal}(k_\infty/k_1^+)$ also acts on $C_\infty(p)$ naturally and (1) is an isomorphism as $\mathrm{Gal}(k_\infty/k_1^+)$-modules.

Put

$$X^\pm = \{x \in X \mid x^\rho = \pm x\},$$

where $\rho \in \mathrm{Gal}(k_\infty/k_1^+)$ denotes, as before, the complex conjugation. Then, (1) induces an isomorphism

$$C_\infty(p)^- \simeq \mathrm{Hom}(X/X^-,\ W(p)).$$

Let M_p^+ denote the maximal pro-p abelian extension of k_∞^+ unramified outside p. As M_p^+ is a Galois extension of k_1^+, the Galois group $\mathrm{Gal}(M_p^+/k_\infty^+)$ is naturally a pro-p $\mathfrak{g}$-module via the isomorphism $\mathrm{Gal}(k_\infty^+/k_1^+) \simeq \mathfrak{g}$, on which ρ acts trivially.

On the other hand, ρ acts on $\mathrm{Gal}(N_p/k_\infty)$ as the (-1)-multiplication. This follows from the fact that the unit group of k_∞ is generated by that of k_∞^+ and all roots of unity. Therefore we have $X/X^- = \mathrm{Gal}(M_p^+ N_p/N_p)$ and, as $\mathfrak{g}$-modules, an isomorphism

$$C_\infty(p)^- \simeq \mathrm{Hom}\big(\mathrm{Gal}(M_p^+/k_\infty^+),\ W(p)\big).$$

2. Embedding problems of $\mathcal{A}_p$-modules.

2.1. In our previous paper [**1**], we have given a characterization of pro-p $\mathcal{A}_p$-module $\prod_{N=1}^\infty \mathcal{A}_p$ in terms of embedding problems of $\mathcal{A}_p$-modules. We shall briefly recall this.

Let Γ be an infinite cyclic group and $x_1, x_2, \ldots$ be a countable number of letters. Let F be the free group generated by the symbols (γ_λ, x_i), where $\gamma_\lambda \in \Gamma$, $i \geq 1$. The group Γ operates on F via $\gamma(\gamma_\lambda, x_i) = (\gamma\gamma_\lambda, x_i)$, $\gamma \in \Gamma$. Let p be a fixed prime and S be the category of finite abelian p-groups. We define the pro-S group F_S by

$$F_S = \varprojlim F/N,$$

where N runs over all index finite normal Γ-subgroups containing all (γ_λ, x_i) except for a finite number such that F/N is an object of S. As readily seen, the cardinality of open subgroups of F_S is countable and the profinite completion $\mathfrak{g}$ of Γ operates naturally on F_S.

Let $\mathcal{A}_p$ denote the completed group algebra of $\mathfrak{g}$ over $\mathbb{Z}_p$, i.e.

$$\mathcal{A}_p = \varprojlim \mathbb{Z}_p/(p^m)[\mathfrak{g}/\mathfrak{h}],$$

where the projective limit is taken with respect to all integers m and all index finite subgroups $\mathfrak{h}$ of $\mathfrak{g}$. Then, as F_S is a pro-p abelian $\mathfrak{g}$-group, it is naturally an $\mathcal{A}_p$-module. As can be easily verified, F_S is, as an $\mathcal{A}_p$-module, isomorphic to the direct product of countable number of copies of $\mathcal{A}_p$; $F_S \simeq \prod_{N=1}^{\infty} \mathcal{A}_p$.

2.2. An embedding problem for a pro-p $\mathcal{A}_p$-module X is the following diagram:

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{\alpha} & C & \longrightarrow & 0 \end{array} \qquad (\mathrm{P}_{\mathcal{A}_p})$$

Here, the horizontal sequence is an exact sequence of finite $\mathcal{A}_p$-modules with p-power orders and φ is a surjective $\mathcal{A}_p$-homomorphism. A weak solution of this problem is an $\mathcal{A}_p$-homomorphism $\psi : X \to B$ such that $\alpha\psi = \varphi$. If, moreover, ψ is surjective, then ψ is called a proper solution, or simply a solution.

Let X be a pro-p $\mathcal{A}_p$-module with at most countable open $\mathcal{A}_p$-submodules. A variant of classical Iwasawa's theorem [**4**, Theorem 4] is that X is isomorphic to F_S, and hence to $\prod_{N=1}^{\infty} \mathcal{A}_p$, as $\mathcal{A}_p$-modules if and only if every embedding problem $(\mathrm{P}_{\mathcal{A}_p})$ has a solution ([**1**, Theorem 1.1]).

2.3. The solvability of every embedding problem $(\mathrm{P}_{\mathcal{A}_p})$ is reduced to two conditions. To state these, let us introduce certain finite $\mathcal{A}_p$-modules. For each $n \geq 1$, let C_n denote the unique quotient of $\mathfrak{g}$ such that C_n is cyclic of order n. Let $\mathbb{F}_p[C_n]$ denote the group algebra of C_n over the prime field $\mathbb{F}_p$ of characteristic p. Via the projection $\mathfrak{g} \to C_n$, $\mathbb{F}_p[C_n]$ is naturally regarded as a $\mathfrak{g}$-module, and hence an $\mathcal{A}_p$-module. We denote this module by $E_n(p)$.

Now we have the following theorem ([**1**, Theorem 1.3]).

THEOREM 2.1. *Let X be a pro-p $\mathcal{A}_p$-module with at most countable open $\mathcal{A}_p$-submodules. Then X is isomorphic to $\prod_{N=1}^{\infty} \mathcal{A}_p$ if and only if the following conditions* (I_p) *and* (II_p) *are satisfied*;

- (I_p): *Every embedding problem $(\mathrm{P}_{\mathcal{A}_p})$ has a weak solution whenever A, B and C are finite $\mathcal{A}_p$-modules with p-power orders.*
- (II_p): *For any $m, n \geq 1$, there exists an open $\mathcal{A}_p$-submodule Y of X such that X/Y is isomorphic to $E_n(p)^{\oplus m}$.*

REMARK. Let Γ be the identity group, instead of an infinite cyclic group, and F be a free group generated by a countable number of letters. Then the pro-S group F_S is defined similarly and is isomorphic to $\prod_{N=1}^{\infty}\mathbb{Z}_p$, the direct product of countable number of copies of $\mathbb{Z}_p$. A variant of Theorem 2.1 holds, $\mathcal{A}_p$ being replaced by $\mathbb{Z}_p$ and $E_n(p)$ being replaced by $\mathbb{Z}/p\mathbb{Z}$, which gives a characterization of the profinite abelian group $\prod_{N=1}^{\infty}\mathbb{Z}_p$. This immediately gives a characterization of $\bigoplus_{N=1}^{\infty}(\mathbb{Q}_p/\mathbb{Z}_p)$, the character group of $\prod_{N=1}^{\infty}\mathbb{Z}_p$. As readily seen, this is equivalent to the result of infinite abelian group theory which Brumer used in [**2**].

3. Embedding problems for p-groups.

3.1. Let k be an algebraic number field, not necessarily finite over the rationals $\mathbb{Q}$, and p be a prime number. Let us consider the following embedding problem for the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$ of k;

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(\bar{k}/k) & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & C_p & \longrightarrow & E & \xrightarrow{\alpha} & H & \longrightarrow & 1. \end{array}$$

Here, the horizontal sequence is an exact sequence of finite p-groups, C_p being a cyclic group of order p, and φ is a surjective homomorphism. Note that the group E is a central extension of H.

Assume that this embedding problem has a proper solution $\psi : \mathrm{Gal}(\bar{k}/k) \to E$, i.e., ψ is a surjective homomorphism such that $\alpha\psi = \varphi$.

In this section, after Reichardt [**7**] and Shafarevich [**9**], we shall summarize how other proper solutions will be obtained, especially in the case that the ground field k does not contain a primitive p-th root of unity.

Let F and $\tilde{F}$ be the fields corresponding to the kernel of φ and that of ψ respectively. Let F_1 and $\tilde{F}_1$ be the fields obtained by adjoining ζ_p to F and $\tilde{F}$ respectively, where ζ_p is a primitive p-th root of unity. Then there exists an element $\mu \in F_1^* \setminus (F_1^*)^p$ such that $\tilde{F}_1 = F_1(\sqrt[p]{\mu})$.

Let G be the Galois group of $\tilde{F}_1/F_1$, V be the subgroup of $F_1^*/(F_1^*)^p$ generated by the class of μ, and W_p denote the group of p-th roots of unity. By Kummer theory, G is isomorphic to $\mathrm{Hom}(V, W_p)$, the group of homomorphisms from V to W_p;

$$G \simeq \mathrm{Hom}(V,\ W_p).$$

Since F_1 and $\tilde{F}_1$ are both Galois extensions of k, the Galois group $\mathrm{Gal}(F_1/k)$ acts naturally on G and $\mathrm{Hom}(V, W_p)$, and this is an isomorphism as $\mathrm{Gal}(F_1/k)$-modules. (The action on $\mathrm{Hom}(V, W_p)$ is defined similarly as the action of $\mathfrak{g}$ on $\mathrm{Hom}(X, W(p))$.)

Let Δ denote the subgroup $\mathrm{Gal}(F_1/F)$ of $\mathrm{Gal}(F_1/k)$, ρ a generator of the cyclic group Δ, and n be the order of Δ. The group Δ acts on W_p, so that we have a character

$$\omega : \Delta \to (\mathbb{Z}/(p))^*$$

such that $\zeta_p^{\rho} = \zeta_p^r, r \in \mathbb{Z}$ and $\omega(\rho)$ is the residue class of r.

LEMMA 3.1. *The element μ satisfies the following conditions*:

(i) $\mu^{\sigma} \equiv \mu \bmod (F_1^*)^p$ *for any* $\sigma \in \mathrm{Gal}(F_1/k(\zeta_p))$.
(ii) $\mu^{\rho} \equiv \mu^r \bmod (F_1^*)^p$.

PROOF. Since $\tilde{F}_1/k(\zeta_p)$ is a central extension of the extension $F_1/k(\zeta_p)$, the Galois group $\mathrm{Gal}(F_1/k(\zeta_p))$ acts trivially on G. As it also acts trivially on W_p, it acts trivially on V. This shows (i).

If Δ acts on V via a character $\varepsilon : \Delta \to (\mathbb{Z}/(p))^*$, then Δ acts on G via the character $\varepsilon^{-1}\omega$. Since the extension $\tilde{F}_1/F_1$ is abelian, we have $\varepsilon^{-1}\omega = 1$, i.e., Δ acts on V via the character ω. This shows (ii). □

REMARK. Conversely, assume that an element μ of $F_1^* \setminus (F_1^*)^p$ is given and that it satisfies the condition (ii) in Lemma 3.1. Then, $F_1(\sqrt[p]{\mu})/F$ is a Galois extension. Furthermore, it is an abelian extension. This follows from the above proof and the fact that the Galois group $\mathrm{Gal}(F_1(\sqrt[p]{\mu})/F)$ is a split extension of $\mathrm{Gal}(F_1/F)$.

Let $\mathbb{F}_p[\Delta]$ be the group algebra of Δ over $\mathbb{F}_p$ and regard the abelian group $F_1^*/(F_1^*)^p$ as $\mathbb{F}_p[\Delta]$-module. Let $e_\omega \in \mathbb{F}_p[\Delta]$ denote the projector from $F_1^*/(F_1^*)^p$ to its ω-eigenspace. Then we have

$$e_\omega = \frac{1}{n} \sum_{\sigma \in \Delta} \omega(\sigma)\sigma^{-1}.$$

As in Reichardt [**7**], let

$$T = \rho^{n-1} + r\rho^{n-2} + \cdots + r^{n-2}\rho + r^{n-1},$$

which is an element of the group algebra $\mathbb{Z}[\Delta]$ of Δ over $\mathbb{Z}$. Then, $n\rho^{-1}e_\omega$ coincides with the image of T under the reduction modulo $p : \mathbb{Z}[\Delta] \to \mathbb{F}_p[\Delta]$. From this we have the following

LEMMA 3.2. *The condition* (ii) *in Lemma* 3.1 *is equivalent to the following condition* (ii)′:

(ii)′ *There exists an element ν of F_1^* such that $\mu \equiv \nu^T \bmod (F_1^*)^p$.*

3.2. Let a be an arbitrary element of $k(\zeta_p)^*$ such that $\mu a^T \notin (F_1^*)^p$ and consider the extension $F_1(\sqrt[p]{\mu a^T})/k$.

PROPOSITION 3.1. (i) *The field $F_1(\sqrt[p]{\mu a^T})$ is a Galois extension of k and is an abelian extension of F.*
(ii) *The Galois group* $\mathrm{Gal}(F_1(\sqrt[p]{\mu a^T})/k(\zeta_p))$ *is isomorphic to E.*

PROOF. One verifies at once, by using Lemma 3.1, that

$$(\mu a^T)^\sigma \equiv \mu a^T \bmod\ (F_1^*)^p$$

for any $\sigma \in \mathrm{Gal}(F_1/k(\zeta_p))$ and that

$$(\mu a^T)^\rho \equiv (\mu a^T)^r \bmod\ (F_1^*)^p.$$

From this and the remark after Lemma 3.1, (i) follows.

Let $c \in H^2(H; C_p)$ be the cohomology class associated with the extension E of H. Then, it is easily verified that c is determined by the elements $\mu^{\sigma-1}, \sigma \in H$. If we replace μ with μa^T, these elements are invariant. From this (ii) follows. □

PROPOSITION 3.2. *There exists a Galois extension $\tilde{F}'$ of k such that $k \subset F \subset \tilde{F}'$, $\tilde{F}' \cap k(\zeta_p) = k$, and $\tilde{F}'k(\zeta_p) = F_1(\sqrt[p]{\mu a^T})$.*

PROOF. Let $G = \mathrm{Gal}(F_1(\sqrt[p]{\mu a^T})/k)$ and $E = \mathrm{Gal}(F_1(\sqrt[p]{\mu a^T})/k(\zeta_p))$. It suffices to show that E is a direct summand of G.

First, one sees immediately that there exists a subgroup D of G such that $\mathrm{Gal}(F_1(\sqrt[p]{\mu a^T})/F) = C_p \times D$, where $C_p = \mathrm{Gal}(F_1(\sqrt[p]{\mu a^T})/F_1)$. Then, as the order n of D is prime to p and E is a finite p-group, G is the semi-direct product of E with D; $G = E.D$.

The group D acts on E by conjugation. As D is isomorphic to $\mathrm{Gal}(F_1/F)$, D acts on the quotient E/C_p trivially. As D also acts on C_p trivially and n is prime to p, it follows easily that D acts on E trivially. Hence we have $G = E \times D$. □

4. Projectivity of Galois groups.

4.1. Let k_0 be a totally real finite algebraic number field. Let k_1 and k_∞ be the fields as defined in Introduction and k_1^+ and k_∞^+ be the maximal totally real subfield of k_1 and k_∞ respectively. Let p be an odd prime and $\tilde{M}_p^+$ denote the maximal pro-p extension of k_∞^+ unramified outside p. By the maximality of $\tilde{M}_p^+$, $\tilde{M}_p^+$ is a Galois extension of k_1^+.

The aim of this section is to show the following

THEOREM 4.1. *Let p be an odd prime. Then the Galois group $\mathrm{Gal}(\tilde{M}_p^+/k_1^+)$ is a projective profinite group.*

We shall first reduce the proof of Theorem 4.1 to showing that a certain Galois group over k_1^+ is a free pro-p group.

Let $G = \mathrm{Gal}(\tilde{M}_p^+/k_1^+)$ and, for each prime l, denote by $G(l)$ the maximal pro-l quotient of G. By the same arguement as in [**1**, 2.2], to prove Theorem 4.1, it suffices to show that $cd_l G(l) \leq 1$ for all prime l. Here cd_l denotes the l-cohomological dimension.

Assume that $l \neq p$. As G is an extension of $\mathrm{Gal}(k_\infty^+/k_1^+)$ by a pro-p group, $G(l)$ is isomorphic to $\mathbb{Z}_l$, the additive group of l-adic integers. Hence we have $cd_l G(l) = 1$.

Assume that $l = p$. Then we have $G(p) = \mathrm{Gal}(M^{(p)}/k_1^+)$, where $M^{(p)}$ denotes the maximal pro-p extension of k_1^+ contained in $\tilde{M}_p^+$.

The following lemma is proved in the same way as [**1**, Lemma 2.2].

LEMMA 4.1. *The field $M^{(p)}$ is the maximal pro-p extension of k_1^+ unramified outside p.*

By Lemma 4.1, the proof of Theorem 4.1 is reduced to showing the following

THEOREM 4.2. *For an odd prime number p, let $M^{(p)}$ be the maximal pro-p extension of k_1^+ unramified outside p. Then the Galois group* $\mathrm{Gal}(M^{(p)}/k_1^+)$ *is a free pro-p group.*

4.2. For the proof of Theorem 4.2, let $G(p) = \mathrm{Gal}(M^{(p)}/k_1^+)$ and consider an embedding problem for the Galois group $G(p)$;

$$\begin{array}{ccccccccc} & & & & & & G(p) & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & C_p & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1. \end{array} \tag{P}$$

Here, the horizontal sequence is an exact sequence of finite p-groups, C_p being a cyclic group of order p, and φ is a surjective homomorphism. Then, as explained in [**1**, 2.3], to prove Theorem 4.2, it suffices to show that every embedding problem (P) has a solution in the case that the exact sequence is non-split.

First we need the following

PROPOSITION 4.1. *For each prime l, $k_1^+\mathbb{Q}_l$ contains the maximal unramified extension of $\mathbb{Q}_l$.*

For the proof, cf. Uchida [**10**, Lemma 1]. (The field k_1^+ contains the field $\mathbb{Q}^{(2)}$ in [**10**].)

By Proposition 4.1, we obtain the following corollary (cf., e.g., Serre [**8**, II, Proposition 9]).

COROLLARY. *Let p be an odd prime. Then we have* $cd_p\,\mathrm{Gal}(\bar{k_1}/k_1^+) \leq 1$.

Let $\tilde{\varphi} : \mathrm{Gal}(\bar{k_1}/k_1^+) \to H$ be the composite of φ and the projection $\mathrm{Gal}(\bar{k_1}/k_1^+) \to G(p)$ and consider the embedding problem ($\tilde{\mathrm{P}}$) obtained from (P) by replacing $G(p)$ and φ with $\mathrm{Gal}(\bar{k_1}/k_1^+)$ and $\tilde{\varphi}$, respectively. By the above corollary, the embedding problem ($\tilde{\mathrm{P}}$) has a solution $\tilde{\psi}$.

4.3. Now we are in the situation in Section 3. Let F and $\tilde{F}$ be the fields corresponding to the kernel of $\tilde{\varphi}$ and that of $\tilde{\psi}$ respectively. Let F_1 and $\tilde{F}_1$ denote the fields obtained by adjoining ζ_p to F and to $\tilde{F}$ respectively so that there exists an element μ of $F_1^* \setminus (F_1^*)^p$ such that $\tilde{F}_1 = F_1(\sqrt[p]{\mu})$.

Let Δ denote the Galois group $\mathrm{Gal}(k_1/k_1^+)$ and define an element T of the group algebra $\mathbb{Z}[\Delta]$ by

$$T = \rho + r,$$

where $\rho \in \Delta$ is the complex conjugation and $r = p - 1$. Note that $\zeta_p^\rho = \zeta_p^r$.

Let a be an arbitrary element of k_1 such that $\mu a^T \notin (k_1^*)^p$ and consider the extension $F_1(\sqrt[p]{\mu a^T})$ of k_1^+. This is a Galois extension (Proposition 3.1). Moreover, $F_1(\sqrt[p]{\mu a^T})$ contains a Galois extension $\tilde{F}'$ of k_1^+ such that

$$F \subset \tilde{F}', \quad \tilde{F}' \cap k_1 = k_1^+, \quad \tilde{F}'k_1 = F_1\big(\sqrt[p]{\mu a^T}\big)$$

(Proposition 3.2). Namely, $\tilde{F}'$ corresponds to another solution of the embedding problem $(\tilde{\mathrm{P}})$. If the extension $\tilde{F}'/k_1^+$ is unramified outside p, then this gives a solution of the embedding problem (P). In order that $\tilde{F}'/k_1^+$ is unramified outside p, it is sufficient that the extension $F_1(\sqrt[p]{\mu a^T})/F_1$ is unramified outside p, because F/k_1^+ is unramified outside p and p is odd. Therefore, the proof of Theorem 4.2 is reduced to showing the following

PROPOSITION 4.2. *There exists an element $a \in k_1^*$ such that $\mu a^T \notin (k_1^*)^p$ and the extension $F_1(\sqrt[p]{\mu a^T})/F_1$ is unramified outside p.*

4.4. In the rest of this section, we shall give the proof of Proposition 4.2.

As F/k_1^+ is a finite extension, there exist finite algebraic number fields k_0 and F_0 such that $F_0 \cap k_1^+ = k_0$ and $F_0k_1^+ = F$. By taking k_0 sufficiently large, we may assume that the extension F_0/k_0 is unramified outside p and that $\mu \in F_0(\zeta_p)$.

First we have the following

LEMMA 4.2. *There exist an ideal $\mathfrak{m}$ of $k_0(\zeta_p)$ prime to p, an ideal $\mathfrak{a}$ of $F_0(\zeta_p)$, and an ideal $\mathfrak{b}$ of $F_0(\zeta_p)$ which is a product of primes lying above p such that $(\mu) = \mathfrak{m}\mathfrak{b}\mathfrak{a}^p$.*

PROOF. This is proved in the same way as [**1**, Lemma 2.3] by noting that $F_0(\zeta_p, \sqrt[p]{\mu})/k_0(\zeta_p)$ is a central extension of $F_0(\zeta_p)/k_0(\zeta_p)$ and that the extension $F_0(\zeta_p)/k_0(\zeta_p)$ is unramified outside p. □

LEMMA 4.3. *There exist an ideal $\mathfrak{n}$ of $k_0(\zeta_p)$, an ideal $\mathfrak{a}_1$ of $F_0(\zeta_p)$ and an ideal $\mathfrak{b}$ of $F_0(\zeta_p)$ which is a product of primes lying above p such that $(\mu) = \mathfrak{n}^T\mathfrak{b}\mathfrak{a}_1^p$.*

PROOF. Let $\mathfrak{m}$, $\mathfrak{b}$ and $\mathfrak{a}$ be ideals as in Lemma 4.2. Then we have

$$(\mu)^{\rho-r} = \mathfrak{m}^{\rho-r}\mathfrak{b}^{\rho-r}(\mathfrak{a}^{\rho-r})^p.$$

By Lemma 3.1 (ii), $(\mu)^{\rho-r}$ is a p-th power of an ideal of $F_0(\zeta_p)$, and hence so is $\mathfrak{m}^{\rho-r}$, because $\mathfrak{m}^{\rho-r}$ and $\mathfrak{b}^{\rho-r}$ are relatively prime. As $\mathfrak{m}^{\rho-r}$ is prime to p and the extension $F_0(\zeta_p)/k_0(\zeta_p)$ is unramified outside p, $\mathfrak{m}^{\rho-r}$ is a p-th power of an ideal of $k_0(\zeta_p)$, i.e., we have

$$\mathfrak{m}^{\rho} \equiv \mathfrak{m}^{r} \bmod I^p,$$

where I denotes the ideal group of $k_0(\zeta_p)$. From this, it follows that there exists an ideal $\mathfrak{n}$ of $k_0(\zeta_p)$ such that

$$\mathfrak{m} \equiv \mathfrak{n}^T \bmod I^p.$$

This is proved completely in the same way as that of Lemma 3.2. Now the lemma follows from this. □

4.5. Let $\mathfrak{n}$ be the ideal of $k_0(\zeta_p)$ as given in Lemma 4.3. By the density theorem, there exists a prime ideal $\mathfrak{q}$ of $k_0(\zeta_p)$ whose absolute degree is one such that $\mathfrak{q}$ and $\mathfrak{n}$ belong to the same ideal class of $k_0(\zeta_p)$. We may also assume that $\mathfrak{q}$ is unramified over $\mathbb{Q}$ and is prime to 2. Thus we have $\mathfrak{q} = \mathfrak{n}(a)$ with some element a of $k_0(\zeta_p)^*$.

Let us consider the element μa^T of $F_0(\zeta_p)^*$. By Lemma 4.3, we have $(\mu a^T) = \mathfrak{q}^\rho \mathfrak{q}'^r \mathfrak{b}\mathfrak{a}_1^p$. As $\mathfrak{q}$ is prime to p, $\mathfrak{q}^\rho \neq \mathfrak{q}$, and the extension $F_0(\zeta_p)/k_0(\zeta_p)$ is unramified outside p, it follows that $\mu a^T \notin (F_0(\zeta_p)^*)^p$. It also follows that the extension $F_0(\zeta_p, \sqrt[p]{\mu a^T})/F_0(\zeta_p)$ is unramified outside those primes of $F_0(\zeta_p)$ lying above $p, \mathfrak{q}^\rho$ and $\mathfrak{q}$.

Let $q = \mathfrak{q} \cap \mathbb{Z}$. Let $\eta_q = \zeta_q + \zeta_q^{-1}$ and put $F_0' = F_0(\eta_q)$, which is contained in k_1^+. By extending F_0 to F_0', we have the following

LEMMA 4.4. *The extension $F_0'(\zeta_p, \sqrt[p]{\mu a^T})/F_0'(\zeta_p)$ is of degree p and is unramified outside p.*

PROOF. This is proved in the same way as [**1**, Lemma 2.4] by using Abhyanker's lemma. Since the verification of the extension degree is lacking in [**1**, Lemma 2.4], we shall supplement it.

Assume, on the contrary, that this extension is trivial. Then, $F_0(\zeta_p, \sqrt[p]{\mu a^T})$ is contained in $F_0'(\zeta_p)$. As $k_0(\eta_q, \zeta_p)/k_0(\zeta_p)$ is abelian, it follows that $\mathrm{Gal}(F_0(\zeta_p, \sqrt[p]{\mu a^T})/k_0(\zeta_p)$ is isomorphic to $H \times C_p$, which contradicts with the assumption that E is a non-split extension of H. □

By Lemma 4.4, it follows that the extension $F_1(\sqrt[p]{\mu a^T})/F_1$ is unramified outside p. That this extension is of degree p is verified in the same way as the proof of Lemma 4.4. Thus the proof of Proposition 4.2 is completed.

5. Proof of Theorem.

In this section we shall give the proof of Theorem.

The Galois group $\mathrm{Gal}(M_p^+/k_\infty^+)$ is a pro-p $\mathcal{A}_p$-module with countable open $\mathcal{A}_p$-submodules. Therefore, by Theorem 2.1, it is enough to verify that this Galois group satisfies the conditions (I_p) and (II_p) in Theorem 2.1. The proof that (I_p) is satisfied can be done, by using Theorem 4.1, completely in the same way as given in [**1**, 3.1], and hence is omitted.

To show that the condition (II_p) in Theorem 2.1 is satisfied, it suffices to prove the following

PROPOSITION 5.1. *Let p be an odd prime. Then, for each positive integers m and n, there exists a finite unramified abelian extension F^+ of k_∞^+ which is a Galois extension of k_1^+ such that the Galois group* $\mathrm{Gal}(F^+/k_\infty^+)$ *is isomorphic to $E_n(p)^{\oplus m}$ as $\mathcal{A}_p$-modules.*

PROOF. The proof can be done along the same line of the proof of Proposition 3.1 in [**1**]. As $\mathfrak{g}$ is isomorphic to $\widehat{\mathbb{Z}}$, there exists a unique subextension k_n^+ of k_∞^+/k_1^+ such that $[k_n^+ : k_1^+] = n$. Let K_0'/k_0' be a finite Galois extension of finite algebraic number fields such that $k_1^+ \cap K_0' = k_0'$, $k_1^+ K_0' = k_n^+$ and that k_1^+ is cyclotomic over k_0'. Replacing k_0' by a finite extension if necessary, we may assume that $[k_0'(\zeta_p) : k_0'] = 2$. The extension K_0'/k_0' is cyclic of degree n.

Fix an even integer $2N$ with $N > 1$. By the theorem of primes in an arithmetic progression, there exists a prime l such that $l \equiv 1 \bmod 2N$ and that l is unramified in k_0'. Then, as $k_0'(\zeta_l)/k_0'$ is a cyclic extension of degree $l-1$, there exists a unique subextension $\mathfrak{K}$ of $k_0'(\zeta_l)/k_0'$ such that $[k_0'(\zeta_l) : \mathfrak{K}] = 2N$. As $2N$ is even, $\mathfrak{K}$ is contained in $k_0'(\zeta_l + \zeta_l^{-1})$. Let $k_0^+ = k_0'(\zeta_l + \zeta_l^{-1})$, which is a subfield of k_1^+, and $K_0^+ = K_0'(\zeta_l + \zeta_l^{-1})$. Thus we have totally real cyclotomic extensions of $\mathfrak{K}$:

$$\mathfrak{K} \subset k_0^+ \subset K_0^+ \subset k_\infty^+, \tag{2}$$

where $k_0^+/\mathfrak{K}$ is cyclic of degree $N > 1$ and K_0^+/k_0^+ is cyclic of degree n.

Let $k_0 = k_0^+(\zeta_p)$, $K_0 = K_0^+(\zeta_p)$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be all prime ideals of K_0 lying above p. For each i $(1 \leq i \leq g)$, fix a positive integer s_i such that every element α of K_0 satisfying $\alpha \equiv 1 \bmod \mathfrak{p}_i^{s_i}$ is locally a p-th power, i.e. α is a p-th power in the $\mathfrak{p}_i$-adic completion of K_0. Let $\mathfrak{m}$ be an integral ideal of K_0 such that $\mathfrak{p}_i^{s_i} | \mathfrak{m}$ $(1 \leq i \leq g)$ and that $\mathfrak{m}$ is invariant by the action of $\mathrm{Gal}(K_0/k_0^+)$.

By the density theorem, there exist principal prime ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_m$, $\mathfrak{L}_i = (\alpha_i)$ $(1 \leq i \leq m)$, of K_0 satisfying the following conditions;

(i) $\alpha_i \equiv 1 \bmod \mathfrak{m}$.
(ii) Let $\mathfrak{L}_i \cap \mathbb{Q} = (l_i)$. Then $l_1, \ldots, l_m$ are distinct primes.
(iii) Every $\mathfrak{L}_i$ is of absolute degree one and is unramified in $K_0/\mathbb{Q}$.

Let ρ be the generator of the Galois group $\mathrm{Gal}(K_0/K_0^+)$ and let $C_n = \mathrm{Gal}(K_0/k_0)$, which is a cyclic group of order n. For each i $(1 \leq i \leq m)$, let F_i be the field obtained by adjoining to K_0 p-th roots of $(\alpha_i^{\rho-1})^\sigma$, where σ runs over all elements of C_n.

By the conditions (i), (ii) and (iii), the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ split completely in F_i and the extension F_i/K_0 is unramified outside $\mathfrak{L}_i^\sigma$, $\mathfrak{L}_i^{\sigma\rho}$, $\sigma \in C_n$. By the conditions (ii) and (iii), $(\alpha_i^{\rho-1})^\sigma$ $(1 \leq i \leq m,\ \sigma \in C_n)$ are multiplicatively independent in $K_0^*/(K_0^*)^p$, so that $F_1, \ldots, F_m$ are linearly disjoint over K_0.

One proves, by Galois theory, the following:

(a) F_i is a Kummer extension of K_0 with exponent p.
(b) F_i is a Galois extension of k_0 and the Galois group $\mathrm{Gal}(F_i/K_0)$ is, as $\mathrm{Gal}(K_0/k_0)$-modules and hence as $\mathcal{A}_p$-modules, isomorphic to $E_n(p)$.
(c) F_i is a Galois extension of k_0^+ and is an abelian extension of K_0^+.
(d) There exists a subextension F_i^+ of F_i/K_0^+ such that $F_i^+ \cap K_0 = K_0^+$, $F_i^+ K_0 = F_i$ and that F_i^+/k_0^+ is a Galois extension.

Let F be the composite of $F_1, \ldots, F_m$. Then we have that $F \cap k_\infty = K_0$ and that $F_i(\zeta_{l_i})$ is unramified over $K_0(\zeta_{l_i})$. These can be proved in the same way of the proof of Proposition 3.1 in [**1**]. (As for the former, this is where the tower of fields (2) is used.)

Now, let F^+ be the composite of $F_1^+, \dots, F_m^+$. As $F_1, \dots, F_m$ are linearly disjoint over K_0, $F_1^+, \dots, F_m^+$ are linearly disjoint over K_0^+. Thus, by (b) and (d), the Galois group $\mathrm{Gal}(F^+/K_0^+)$ is isomorphic to $E_n(p)^{\oplus m}$ as $\mathcal{A}_p$-modules and hence, as $F \cap k_\infty = K_0$, so is $\mathrm{Gal}(F^+k_\infty^+/k_\infty^+)$.

It remains to show that $F^+k_\infty^+$ is unramified over k_∞^+. As $F_i(\zeta_{l_i})$ is unramified over $K_0(\zeta_{l_i})$, F^+k_∞ is unramified over k_∞. Since the extension degree $[F^+k_\infty : k_\infty] = [F^+k_\infty^+ : k_\infty^+]$ is a power of p and $[k_\infty : k_\infty^+] = 2$, it follows that $F^+k_\infty^+$ is unramified over k_∞^+. □

References

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

[2] A. Brumer, The class group of all cyclotomic integers, J. Pure Appl. Algebra, **20** (1981), 107–111.

[3] K. Horie, CM-fields with all roots of unity, Compositio Math., **74** (1990), 1–14.

[4] K. Iwasawa, On solvable extensions of algebraic number fields, Ann. of Math. (2), **58** (1953), 548–572.

[5] K. Iwasawa, Sheaves for algebraic number fields, Ann. of Math. (2), **69** (1959), 408–413.

[6] M. Kurihara, On the ideal class groups of the maximal real subfields of number fields with all roots of unity, J. Eur. Math. Soc. (JEMS), **1** (1999), 35–49.

[7] H. Reichardt, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, J. Reine Angew. Math., **177** (1937), 1–5.

[8] J.-P. Serre, Cohomologie Galoisienne. 5th ed., Lecture Notes in Math., **5**, Springer-Verlag, Berlin, 1994.

[9] I. R. Shafarevich, On the construction of fields with a given Galois group of order l^α, Izv. Akad. Nauk SSSR Ser. Mat., **18** (1954), 261–296.

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

Mamoru Asada

Graduate school of Science and Technology
Kyoto Institute of Technology
Matsugasaki
Kyoto 606-8585, Japan