ON GALOIS GROUPS OF ABELIAN EXTENSIONS OVER MAXIMAL CYCLOTOMIC FIELDS

Mamoru Asada

Introduction

Let k_0 be a finite algebraic number field in a fixed algebraic closure Ω and ζ_n denote a primitive n-th root of unity ($n \geq 1$). Let k_∞ be the maximal cyclotomic extension of k_0, i.e. the field obtained by adjoining to k_0 all ζ_n ($n = 1, 2, ...$). Let M and L be the maximal abelian extension of k_∞ and the maximal unramified abelian extension of k_∞ respectively. The Galois groups $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$ are, as profinite abelian groups, both isomorphic to the product of countable number of copies of the additive group of $\widehat{\mathbb{Z}}$. Here, $\widehat{\mathbb{Z}}$ denotes the profinite completion of the ring of rational integers $\mathbb{Z}$. In fact, more generally, if M_{sol} and L_{sol} denote the maximal solvable extension of k_∞ and the maximal unramified solvable extension of k_∞ respectively, the Galois groups $\mathrm{Gal}(M_{sol}/k_\infty)$ and $\mathrm{Gal}(L_{sol}/k_\infty)$ are both isomorphic to the free prosolvable group on countably infinite generators (Iwasawa[2], Uchida[5]).

On the other hand, as M and L are both Galois extensions of k_0, the cyclotomic Galois group $\mathrm{Gal}(k_\infty/k_0)$ acts on $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$ naturally. The structure of these Galois groups with this action, however, does not seem to be known.

Let k_1 be the field obtained by adjoining ζ_4 and ζ_p for all odd prime p to k_0 and consider the subgroup $\mathfrak{g} = \mathrm{Gal}(k_\infty/k_1)$ of $\mathrm{Gal}(k_\infty/k_0)$. It is easy to see that $\mathfrak{g}$ is isomorphic to the additive group of $\widehat{\mathbb{Z}}$. Now, as $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$ are profinite abelian groups, they are naturally $\widehat{\mathbb{Z}}$-modules and $\mathfrak{g}$ acts on them. Therefore, they can be regarded as $\mathcal{A}$-modules, where $\mathcal{A}$ denotes the completed group algebra of $\mathfrak{g}$ over $\widehat{\mathbb{Z}}$. Our main result is the following

Theorem. The Galois groups $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$ are, as $\mathcal{A}$-modules, both isomorphic to $\prod_{N=1}^{\infty} \mathcal{A}$, the direct product of countable number of copies of $\mathcal{A}$.

We shall explain the method of the proof of Theorem. Unlike the Iwasawa algebra, we have neither a good presentation of the algebra $\mathcal{A}$ nor the structure theorem of $\mathcal{A}$-modules. Our first task is to find a criterion whether a given $\mathcal{A}$-module is isomorphic to $\prod_{N=1}^{\infty} \mathcal{A}$ or not. In his paper[2], Iwasawa gives a characterization of the free pro-S group on countably infinite generators in terms of the solvability of embedding problems of finite S-groups. (S is a category of finite groups satisfying some conditions.) We shall use an $\mathcal{A}$-module version of this result ; a profinite $\mathcal{A}$-module X with at most countable open $\mathcal{A}$-submodules is isomorphic to $\prod_{N=1}^{\infty} \mathcal{A}$ if and only if every embedding problem of finite $\mathcal{A}$-modules for X has a solution (Theorem 1.2).

We apply this criterion to $\mathcal{A}$-modules $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$. There are two cases for the exact sequence of finite $\mathcal{A}$-modules of embedding problems ; split cases and non-split cases.

The non-split case seems to be more difficult. There are two points in solving embedding problems in this case. We shall briefly explain them in the case of $\mathrm{Gal}(L/k_\infty)$. A group theoretical point is that $\mathfrak{g}$ is a free profinite group (of rank 1) so that the projection $\mathrm{Gal}(L/k_1) \to \mathfrak{g}$ splits. By using this, the solvability of the embedding problem for the $\mathcal{A}$-module $\mathrm{Gal}(L/k_\infty)$ can be reduced to that of the embedding problem for the profinite group $\mathrm{Gal}(L/k_1)$. It can be further reduced to that of the embedding problem for the group $\mathrm{Gal}(\tilde{L}/k_1)$, where $\tilde{L}$ denotes the maximal unramified Galois extension of k_∞.

An arithmetical point is that the Galois group $\mathrm{Gal}(\tilde{L}/k_1)$ is projective. In Uchida[5], for an infinite algebraic number field K satisfying a certain condition such as k_1, it is shown that the Galois group $\mathrm{Gal}(K^{ur}/K)$ is projective. Here K^{ur} denotes the maximal unramified Galois extension of K. Though ramification occurs in the subextension k_∞ of $\tilde{L}/k_1$, by a slight modification of his proof, we can show that $\mathrm{Gal}(\tilde{L}/k_1)$ is projective. From this the solvability of the embedding problem follows.

The author first obtained the above mentioned $\mathcal{A}$-module version of Iwasawa's theorem. Then Professor Shoichi Nakajima pointed out that one can give its more general version, which gives a characterization of the free pro-S group on countably infinite generators with operator domain $\widehat{\Gamma}$, where $\widehat{\Gamma}$ denotes the profinite completion of an arbitrary group Γ. In the case that S is the category of finite abelian groups and Γ is an infinite cyclic group, this version gives the above mentioned $\mathcal{A}$-module version. In §1 we shall formulate this generalized version. We shall also give a necessary and sufficient condition in order that every embedding problem of finite $\mathcal{A}$-modules has a solution. In §2 we shall prove that the Galois group $\mathrm{Gal}(\tilde{L}/k_1)$ is projective. In §3 we shall give the proof of Theorem.

As noticed above, for our methods of the proofs of several results, we owe much to Iwasawa[2] and Uchida[5]. We have given the details of the proofs of theorems, since an application of embedding problems to the study of the cyclotomic Galois action on $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$ has not been appeared.

The author expresses his sincere gratitudes to Professor Shoichi Nakajima for valuable comments, especially for suggesting a generalization of a theorem of Iwasawa.

§1. Embedding problems of $\mathcal{A}$-modules

(1-1) Let Γ be a group and $x_1, x_2, ...$ be a countable number of letters. Let F be the free group generated by the symbols (γ_λ, x_i) $(\gamma_\lambda \in \Gamma, i \geq 1)$. The group Γ operates on F via $\gamma(\gamma_\lambda, x_i) = (\gamma\gamma_\lambda, x_i)$ $(\gamma \in \Gamma)$. Let S be a category of finite groups whose object satisfy the following conditions ;

(i) any subgroup of an object of S is an object of S,

(ii) any quotient group of an object of S is an object of S,
(iii) the direct product of two objects of S is an object of S.

The projective limit of finite groups which are objects of S is called a pro-S group. 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 the cardinality of such subgroups is at most countable, the cardinality of open subgroups of F_S is at most countable.

The profinite completion $\widehat{\Gamma}$ of Γ operates naturally on the group F_S. In fact, let A_N denote the image of the homomorphism $\Gamma \to \mathrm{Aut}(F/N)$ induced by the operation of Γ on the quotient F/N. (Aut $*$: the automorphism group of the group $*$.) As $\{\Gamma \to A_N\}_N$ is a projective system, we have a homomorphism $\varprojlim \Gamma \to \varprojlim A_N$, i.e. $\Gamma \to \varprojlim A_N$. Since A_N is a finite group and $\varprojlim A_N$ can be regarded as a subgroup of $\mathrm{Aut} F_S$, this induces a homomorphism

$$\widehat{\Gamma} \to \varprojlim A_N \subset \mathrm{Aut} F_S.$$

This shows that $\widehat{\Gamma}$ operates on F_S.

We call the group F_S the free pro-S $\widehat{\Gamma}$-group generated by $x_1, x_2, \ldots$.

(1-2) Recall that an embedding problem for a profinite group X is a diagram

$$(P) \qquad \begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{\alpha} & C & \longrightarrow & 1, \end{array}$$

where the horizontal sequence is an exact sequence of profinite groups and φ is a surjective homomorphism. A weak solution of this problem is a homomorphism $\tilde{\varphi} : X \to B$ such that $\alpha\tilde{\varphi} = \varphi$. If, moreover, $\tilde{\varphi}$ is surjective, then $\tilde{\varphi}$ is called a proper solution, or simply a solution. When A, B, C and X are profinite groups with operator domain $\widehat{\Gamma}$ and homomorphisms of the diagram are $\widehat{\Gamma}$-homomorphisms, then a (weak) solution is also assumed to be a $\widehat{\Gamma}$-homomorphism.

Now we have the following theorem, which is a version of Iwasawa's theorem in the case of the free pro-S $\widehat{\Gamma}$-group.

Theorem 1.1. *Let X be a pro-S $\widehat{\Gamma}$-group with at most countable open $\widehat{\Gamma}$-subgroups. Then X is isomorphic to F_S as $\widehat{\Gamma}$-groups if and only if every embedding problem (P) has a solution, where the horizontal sequence is an exact sequence of finite S-groups with operator domain $\widehat{\Gamma}$.*

When Γ is the trivial group, this is a theorem of Iwasawa[2, Th.4]. The proof of this theorem is done step by step in the same way as that of [2, Th.4], hence is omitted.

(1-3) Now we shall restrict ourselves to the case that Γ is an infinite cyclic group, hence $\widehat{\Gamma} \simeq \mathfrak{g}$, and S is the category of finite abelian groups. Let $\mathcal{A}$ denote the completed group algebra of $\mathfrak{g}$ over the profinite completion $\widehat{\mathbb{Z}}$ of the ring of integers $\mathbb{Z}$, i.e.

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

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 profinite abelian $\mathfrak{g}$-group, it is naturally an $\mathcal{A}$-module. As can be easily verified, F_S is, as $\mathcal{A}$-modules, isomorphic to the direct product of countable number of copies of $\mathcal{A}$; $F_S \simeq \prod_{N=1}^{\infty} \mathcal{A}$.

Let X be a profinite $\mathcal{A}$-module and consider the following embedding problem :

$(P_{\mathcal{A}})$

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \big\downarrow{\scriptstyle\varphi} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

Here, the horizontal sequence is an exact sequence of finite $\mathcal{A}$-modules and φ is a surjective $\mathcal{A}$-homomorphism. In this case, Theorem 1.1 is formulated as the following

Theorem 1.2. *Let X be a profinite $\mathcal{A}$-module with at most countable open $\mathcal{A}$-submodules. Then X is isomorphic to $\prod_{N=1}^{\infty} \mathcal{A}$ if and only if every embedding problem $(P_{\mathcal{A}})$ has a solution.*

(1-4) We shall give conditions on the solvability of the embedding problem $(P_{\mathcal{A}})$ in (1-3). To state these, we introduce certain finite $\mathcal{A}$-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 p be a prime and $\mathbb{F}_p[C_n]$ 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, hence an $\mathcal{A}$-module. We denote this module by $E_n(p)$.

Now we have the following theorem, which is the $\mathcal{A}$-module counterpart of [2, Th. 1]. (Cf. also Serre[3, I, 3.4, Ex.1].)

Theorem 1.3. *Let X be a profinite $\mathcal{A}$-module. In order that every embedding problem $(P_{\mathcal{A}})$ has a solution, it is necessary and sufficient that for every prime number p, the following conditions (I_p) and (II_p) are satisfied ;*

(I_p) *: Every embedding problem $(P_{\mathcal{A}})$ has a weak solution whenever A, B and C are finite $\mathcal{A}$-modules with p-power orders.*

(II_p) *: For any $m, n \geq 1$, there exists an open $\mathcal{A}$-submodule Y of X such that X/Y is isomorphic to $E_n(p)^{\oplus m}$.*

(1-5) For the proof of Theorem 1.3, we need several lemmas.

Lemma 1.1. *Let X be a profinite $\mathcal{A}$-module. In order that every embedding problem $(P_{\mathcal{A}})$ has a solution, it is necessary and sufficient that for every prime number p, it has a solution whenever A, B and C are finite $\mathcal{A}$-modules with p-power orders.*

Proof. It is enough to show that the condition is sufficient. Let $(P_{\mathcal{A}})$ be a given embedding problem and let A_p, B_p and C_p be the p-Sylow subgroups, hence $\mathcal{A}$-submodules, of A, B and C respectively. Let $\bar{\varphi}$ be the composite of φ and the projection $C \to C_p$ and consider the embedding problem

$$\begin{tikzcd} & & & X \arrow[d, "\bar{\varphi}"] & \\ 0 \arrow[r] & A_p \arrow[r] & B_p \arrow[r] & C_p \arrow[r] & 0, \end{tikzcd}$$

where the horizontal sequence is induced from that of $(P_{\mathcal{A}})$. Let $\gamma_p : X \to B_p$ be a solution of this problem. Define an $\mathcal{A}$-homomorphism $\gamma : X \to B = \oplus B_p$ by $\gamma(x) = (\gamma_p(x))_p$. Then it is immeadiately verified that γ is a solution of the problem $(P_{\mathcal{A}})$.

Lemma 1.2. *Let X be a profinite $\mathcal{A}$-module. In order that every embedding problem $(P_{\mathcal{A}})$ has a solution, it is necessary and sufficient that it has a solution whenever A is an irreducible $\mathcal{A}$-module.*

Proof. It is enough to show that the condition is sufficient. Let $(P_{\mathcal{A}})$ be a given embedding problem and let A_1 be a maximal $\mathcal{A}$-submodule of A. Then, as A/A_1 is irreducible, the embedding problem

$$\begin{tikzcd} & & & X \arrow[d, "\varphi"] & \\ 0 \arrow[r] & A/A_1 \arrow[r] & B/A_1 \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

has a solution ψ_1. Let A_2 be a maximal $\mathcal{A}$-submodule of A_1. Again, the embedding problem

$$\begin{tikzcd} & & & X \arrow[d, "\psi_1"] & \\ 0 \arrow[r] & A_1/A_2 \arrow[r] & B/A_2 \arrow[r] & B/A_1 \arrow[r] & 0 \end{tikzcd}$$

has a solution ψ_2. After iterating this process finitely many times, we obtain a solution ψ of the embedding problem $(P_{\mathcal{A}})$.

The following lemma is easily proved.

Lemma 1.3. *Let*

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\alpha} C \longrightarrow 0$$

be an exact sequence of finite $\mathcal{A}$-modules. Assume that A is irreducible. Then we have the following two cases.

(i) *Any $\mathcal{A}$-submodule B' of B such that $\alpha(B') = C$ coincides with B.*
(ii) *The sequence splits, hence $B \simeq A \oplus C$ as $\mathcal{A}$-modules.*

We shall now consider the embedding problem $(P_{\mathcal{A}})$ in the case that A, B, and C are finite $\mathcal{A}$-modules with p-power orders, p being a prime. In this case we denote the embedding problem by (P_p).

Lemma 1.4. *Let X be a profinite $\mathcal{A}$-module. In order that every embedding problem (P_p) has a solution, it is necessary and sufficient that the following conditions are satisfied ;*
(i) *Every embedding problem (P_p) has a weak solution.*
(ii) *For any open $\mathcal{A}$-submodule X' of X with a p-power index and any finite irreducible $\mathcal{A}$-module A with a p-power order, there exists an open $\mathcal{A}$-submodule Y of X such that $X/Y \simeq A$ and $X = X' + Y$.*

Proof. We shall first show that the conditions (i) and (ii) are necessary. That (i) is necessary is obvious. To show that (ii) is necessary, let $C = X/X'$ and consider the embedding problem

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 0 & \longrightarrow & A & \longrightarrow & A \oplus C & \longrightarrow & C & \longrightarrow & 0, \end{array}$$

where φ is the projection. Let $\psi : X \to A \oplus C$ be a solution of this embedding problem. Let $pr_1 : A \oplus C \to A$ be the projection and Y be the kernel of $pr_1\psi$. Then Y satisfies the condition in (ii).

We shall next show that the conditions (i) and (ii) are sufficient. We may assume, by Lemma 1.2, that A is an irreducible $\mathcal{A}$-module. By Lemma 1.3, we have two cases.

Case (a) : By the condition (i), the embedding problem (P_p) has a weak solution, which is automatically a solution.

Case (b) : Let X' be the kernel of φ. Let Y be an open A-submodule of X satisfying the condition in (ii). Then we have isomorphisms $X/X' \cap Y \simeq X/Y \oplus X/X' \simeq A \oplus C$. Composing this with the projection $X \to X/X' \cap Y$, we obtain a solution $\psi : X \to A \oplus C$.

(1-5) *Proof of Theorem 1.3.* We shall first show that the conditions are necessary. It is obvious that, for every prime number p, (I_p) is necessary. To see that (II_p) is necessary, consider the embedding problem (P_p) in the case that $A = B = E_n(p)^{\oplus m}, C = 0$ and φ is the trivial homomorphism. Since this embedding problem has a solution, for every prime number p, the condition (II_p) is necessary.

We shall show that the conditions are sufficient. It suffices to show that, for every prime number p, the conditions (i) and (ii) in Lemma 1.4 are satisfied. Obviously, (i) is satisfied. To see that (ii) is satisfied, assume that an open $\mathcal{A}$-submodule X' of X with a p-power index and a finite irreducible $\mathcal{A}$-module A with a p-power order are given. As A is finite, the action of $\mathfrak{g}$ on A factors through some C_n. As A is irreducible, $pA = \{0\}$, hence A is regarded as an $\mathbb{F}_p[C_n]$-module. Moreover, by the irreducibility, it is isomorphic to a quotient of $E_n(p)$. Therefore, it suffices to show that there exists an open $\mathcal{A}$-submodule Y_1 of X such that $X/Y_1 \simeq E_n(p)$ and $X = X' + Y_1$. To show this, consider the set

$$\{X'' : open\ \mathcal{A} - submodule \mid X' \subset X'' \subset X\}$$

and let s be its cardinality. By the condition (II_p), there exist open $\mathcal{A}$-submodules $X_1, ..., X_{s+1}$ such that $X/X_i \simeq E_n(p)$ and $X_i + X_j = X$ $(i \neq j)$. Then one verifies at once that at least for one $i = i_1$, we have $X' + X_{i_1} = X$. Putting $Y_1 = X_{i_1}$, we obtain the desired $\mathcal{A}$-submodule.

§2. Projectivity of Galois groups

(2-1) Let k_0 be a finite algebraic number field. As in the introduction, let k_1 be the field obtained by adjoining ζ_4 and ζ_p for all odd prime p to k_0. Let k_∞ be the maximal cyclotomic extension of k_0, i.e. the field obtained by adjoining to k_0 all ζ_n $(n \geq 1)$. Let $\tilde{L}$ denote the maximal unramified Galois extension of k_∞.

What we shall need for the proof of Theorem is the fact that the Galois groups $\mathrm{Gal}(\tilde{L}/k_1)$ and $\mathrm{Gal}(\bar{k}_1/k_1)$ are both projective. (For projective profinite groups, cf. e.g. [3, I, 5.9].) It is not so difficult to verify that $\mathrm{Gal}(\bar{k}_1/k_1)$ is projective. (See Corollary in (2-4) below.) A little harder is to show the following

Theorem 2.1. *The Galois group* $\mathrm{Gal}(\tilde{L}/k_1)$ *is a projective profinite group.*

In [5], Uchida has proved that, for an infinite algebraic number field K satisfying a certain condition, the Galois group $\mathrm{Gal}(K^{ur}/K)$ is projective, where K^{ur} denotes the maximal unramified Galois extension of K. His result can be applied to, e.g. $K = k_\infty$ or $K = k_1$. Since ramification occurs in the subextension k_∞ of $\tilde{L}/k_1$, his theorem cannot by applied directly to $\mathrm{Gal}(\tilde{L}/k_1)$. But its proof can be applied with a slight modification. The proof of his theorem is terse and a little complicated in order to be applied to a wider class of ground fields. We shall give, in our simpler case that the ground field is k_1, a detailed proof for the sake of completeness.

(2-2) We shall first reduce the proof of Theorem 2.1, as in the arguement of [5, Th.1], to showing the projectivity of the maximal pro-p *quotient* of $\mathrm{Gal}(\tilde{L}/k_1)$.

Let G be an arbitrary profinite group and p be a prime number. We denote by cdG and cd_pG the cohomological dimension and the p-cohomological dimension of G respectively. We also denote by $G(p)$ the maximal pro-p quotient of G.

Lemma 2.1. *Let G be a profinite group with at most countable open subgroups. Assume that G satisfies the following condition for every prime number p.*

($*_p$) *For any open subgroup U of G, $cd_pU(p) \leq 1$.*

Then we have $cdG \leq 1$, i.e. G is projective.

Proof. For a prime number p, let G_p be a p-Sylow subgroup of G. Then, there exists a family of open subgroups $\{U_n\}_{n=1}^{\infty}$ of G such that

$$G = U_1 \supset U_2 \supset \ldots \supset U_n \supset U_{n+1} \supset \ldots, \quad \bigcap_{n=1}^{\infty} U_n = G_p.$$

It is easy to see that the composite φ_n of the inclusion homomorphism $G_p \to U_n$ and the projection $U_n \to U_n(p)$ is surjective. These φ_n $(n = 1, 2, \ldots)$ induce an isomorphism $G_p \simeq \varprojlim U_n(p)$.

By the condition $(*_p)$, we have

$$H^2(G_p : \mathbb{F}_p) = \varinjlim H^2(U_n(p) : \mathbb{F}_p) = \{0\}.$$

Thus it follows that $cd_p G_p \leq 1$ ([3, I, Prop.2]). Since $cd_p G = cd_p G_p$ ([3, I, Prop.14]) and p is arbitrary, it follows that $cdG \leq 1$.

We shall apply the above lemma to the Galois group $G = \mathrm{Gal}(\tilde{L}/k_1)$. Let $U = \mathrm{Gal}(\tilde{L}/F_1)$ be an open subgroup of G, where F_1 is a finite extension of k_1. It is easy to see that there exists a finite algebraic number field F_0 such that $F_1 = F_0(\zeta_4, \zeta_p; p \geq 3)$ and that $\tilde{L}$ is the maximal unramified Galois extension of $F_\infty = F_0(\zeta_n; n \geq 1)$. Therefore, the proof of Theorem 2.1 is reduced to showing that for every prime number p, $cd_p G(p) \leq 1$, or equivalently, $G(p)$ is a free pro-p group ([3, I, 4.2]).

Let $L^{(p)}$ denote the maximal pro-p extension of k_1 contained in $\tilde{L}$. Then we have $G(p) = \mathrm{Gal}(L^{(p)}/k_1)$ and $L^{(p)}$ contains $k_1(\zeta_{p^m}; m \geq 1)$. Then we have

Lemma 2.2. *The field $L^{(p)}$ is the maximal unramified pro-p extension of $k_1(\zeta_{p^m}; m \geq 1)$.*

Proof. Let v_p be a p-place of $k_1(\zeta_{p^m}; m \geq 1)$, i.e. a finite place of $k_1(\zeta_{p^m}; m \geq 1)$ which is an extension of the p-adic place of $\mathbb{Q}$. Then it is unramified in $\tilde{L}$, hence in $L^{(p)}$. Let v_l be an l-place of $k_1(\zeta_{p^m}; m \geq 1)$, where l is a prime different from p. The inertia group of v_l in $k_\infty/k_1(\zeta_{p^m}; m \geq 1)$ is a pro-l group and $\tilde{L}$ is unramifed over k_∞. Therefore, as $L^{(p)} \subset \tilde{L}$, the inertia group of any extension of v_l to $L^{(p)}$ is a pro-l group. Thus it is the trivial group as $G(p)$ is a pro-p group. This shows that v_l is unramified in $L^{(p)}$. Therefore $L^{(p)}$ is unramified over $k_1(\zeta_{p^m}; m \geq 1)$. The maximality of $L^{(p)}$ is immeadiately verified.

By Lemmas 2.1 and 2.2, the proof of Theorem 2.1 is reduced to verifying the following

Theorem 2.2. *For a prime number p, let $L^{(p)}$ be the maximal unramified pro-p extension of $k_1(\zeta_{p^m}; m \geq 1)$. Then the Galois group $\mathrm{Gal}(L^{(p)}/k_1)$ is a free pro-p group.*

(2-3) In the rest of this section, we shall give the proof of Theorem 2.2. Let us consider an embedding problem

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

where $G(p) = \mathrm{Gal}(L^{(p)}/k_1)$, E is a finite p-group and C_p is a cyclic group of order p. Then, in order that $cd_pG(p) \leq 1$, it is necessary and sufficient that every embedding problem (P) has a weak solution ([3, I, Prop.16, 20]). In the case that the exact sequence is split, the embedding problem has obviously a weak solution. On the other hand, in the case that the sequence is non-split, its weak solution, if it exists, is automatically a solution. Thus, to prove Theorem 2.2, it suffices to show that every embedding problem (P) has a solution in the case that the exact sequence is non-split.

Let F be the subextension of $L^{(p)}/k_1$ corresponding to the kernel of φ. To find a solution of the embedding problem (P) is equivalent to find a Galois extension $\tilde{F}$ of k_1 containing F such that the following conditions hold ;

(1) The diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\tilde{F}/F) & \longrightarrow & \mathrm{Gal}(\tilde{F}/k_1) & \longrightarrow & \mathrm{Gal}(F/k_1) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & C_p & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

is commutative.

(2) $\tilde{F}$ is contained in $L^{(p)}$.

(2-4) First we find an extension $\tilde{F}$ satisfying the condition (1). It is based on the following

Proposition 2.1. *For each prime l, $k_1\mathbb{Q}_l$ contains the maximal unramified extension of $\mathbb{Q}_l$.*

For the proof, cf. e.g. [5, Lemma 1]. (The field k_1 contains the field $\mathbb{Q}^{(1)}$ in [5].)

By Proposition 2.1, as k_1 is totally imaginary, we obtain the following

Corollary. *The Galois group* $\mathrm{Gal}(\bar{k}_1/k_1)$ *is projective.*

Cf. e.g. [3, II, Prop.9].

Let $\tilde{\varphi} : \mathrm{Gal}(\bar{k}_1/k_1) \to H$ be the composite of φ and the projection $\mathrm{Gal}(\bar{k}_1/k_1) \to G(p)$. Consider the embedding problem $(\tilde{P})$ 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 $(\tilde{P})$ has a solution. The field $\tilde{F}$ corresponding to it satisfies the condition (1).

(2-5) As k_1 contains ζ_p, $\tilde{F}$ is of the form $F(\sqrt[p]{\mu})$, where μ is an element of F. Since E is a central extension of H, it follows immeadiately that $\mu^\sigma \equiv \mu \mod (F^*)^p$ for every $\sigma \in \mathrm{Gal}(F/k_1)$ and that any field of the form $F(\sqrt[p]{\mu\beta})$ $(\beta \in k_1)$ gives a solution of the same embedding problem. We shall find an element $\beta \in k_1$ such that $F(\sqrt[p]{\mu\beta})$ is contained in $L^{(p)}$.

As $F(\sqrt[p]{\mu})/k_1$ is a finite extension, there exist finite algebraic number fields k_0 and F_0 such that $F_0(\sqrt[p]{\mu}) \cap k_1 = k_0$ and $F_0(\sqrt[p]{\mu})k_1 = F(\sqrt[p]{\mu})$.

The following lemma is easily proved by using Proposition 2.1.

Lemma 2.3. *There exists a finite subextension k' of k_1/k_0 such that any p-place of F_0k' is of degree one over k'.*

By Lemma 2.3, we may and shall assume that any p-place of F_0 is of degree one over k_0.

Lemma 2.4. *There exists an element a of k_0^* such that μa is prime to p and every p-place of F_0 splits completely in $F_0(\sqrt[p]{\mu a})$.*

Proof. Let $\mathfrak{p}_1, ..., \mathfrak{p}_r$ be all prime ideals of F_0 lying above p. Let $N_1, ..., N_r$ be positive integers such that any element x of F_0^* satisfying $x \equiv 1 \mod \mathfrak{p}_i^{N_i}$ is a p-th power in the $\mathfrak{p}_i$-adic completion $F_{0,\mathfrak{p}_i}$ of F_0. As every $\mathfrak{p}_i$ is of degree one over k_0, there exists an element a of k_0^* such that

$$a^{-1} \equiv \mu \mod \mathfrak{p}_i^{N_i} \quad (1 \leq i \leq r).$$

Then μa is a p-th power in $F_{0,\mathfrak{p}_i}$ so that $\mathfrak{p}_1, ..., \mathfrak{p}_r$ split completely in $F_0(\sqrt[p]{\mu a})$.

(2-6) By Lemma 2.4, we can take, as the field corresponding to a solution of the embedding problem $(\tilde{P})$, the field of the form $F_0(\sqrt[p]{\mu})$, where $\mu \in F_0^*$ is prime to p and every p-place of F_0 splits completely in $F_0(\sqrt[p]{\mu})$. In the following, we assume that $F_0(\sqrt[p]{\mu})$ has been taken as such. Furthermore, as F/k_1 is unramified outside p by Lemma 2.2, we may assume, by taking k_0 sufficiently large, that F_0/k_0 is unramified outside p.

Lemma 2.5. *There exist an ideal $\mathfrak{m}$ of k_0 and an ideal $\mathfrak{a}$ of F_0 such that $(\mu) = \mathfrak{m}\mathfrak{a}^p$.*

Proof. As noted above, we have, for every $\sigma \in H = \mathrm{Gal}(F_0/k_0)$, $\mu^\sigma \equiv \mu \mod (F_0^*)^p$. Thus the ideal (μ) is H-invariant modulo I^p, where I denotes the ideal group of F_0. Since F_0/k_0 is unramified outside p and μ is prime to p, the lemma follows.

Let N be an arbitrary positive integer and consider the ideal class group of k_0 defined modulo p^N. By the density theorem, there exists a prime ideal $\mathfrak{q}$ of k_0 whose absolute degree is one and belongs to the class of $\mathfrak{m}$. This means that there exists an element β of k_0 such that $\mathfrak{q} = \mathfrak{m}(\beta)$ and $\beta \equiv 1 \mod p^N$. We take N sufficiently large so that every p-place of F_0 splits completely in $F_0(\sqrt[p]{\mu\beta})$. This field also gives a solution of the embedding problem and, as $(\mu\beta) = (\mu)(\beta) = \mathfrak{q}\mathfrak{a}^p$, the extension $F_0(\sqrt[p]{\mu\beta})/F_0$ is unramified outside $\mathfrak{q}$.

Lemma 2.6. *Let $q = \mathfrak{q} \cap \mathbb{Z}$. Then the extension $F_0(\zeta_q, \sqrt[p]{\mu\beta})/F_0(\zeta_q)$ is unramified.*

Proof. First we note that, as $\mathbb{Q}(\zeta_p) \subset k_0$ and the absolute degree of $\mathfrak{q}$ is one, the prime q splits completely in $\mathbb{Q}(\zeta_p)$, i.e. $q \equiv 1 \mod p$. Since $k_0 \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$, we have $[k_0(\zeta_q) : k_0] = q - 1$. As $k_1 \cap F_0(\sqrt[p]{\mu\beta}) = k_0$, we have $F_0(\zeta_q) \cap F_0(\sqrt[p]{\mu\beta}) = F_0$.

Let $\tilde{\mathfrak{q}}$ be any prime ideal of F_0 lying above $\mathfrak{q}$. Since $\mathfrak{q}$ is totally and tamely ramified in $k_0(\zeta_q)$ and unramified in F_0, $\tilde{\mathfrak{q}}$ is totally and tamely ramified in $F_0(\zeta_q)$. As the extension degree p of $F_0(\sqrt[p]{\mu\beta})/F_0$ divides the ramification index $q-1$ of $\tilde{\mathfrak{q}}$ in $F_0(\zeta_q)$, by Abhyanker's lemma (cf. e.g. Cornell[1]), the prime ideal of $F_0(\zeta_q)$ lying above $\tilde{\mathfrak{q}}$ is unramified in $F_0(\zeta_q, \sqrt[p]{\mu\beta})$.

By Lemma 2.6, it follows that the extension $F(\sqrt[p]{\mu\beta})/F$ is unramified, hence $F(\sqrt[p]{\mu\beta})$ is contained in $L^{(p)}$. Thus the proof of Theorem 2.2 is completed.

§3. Proof of Theorem.

(3-1) The Galois groups $\mathrm{Gal}(M/k_\infty)$ and $\mathrm{Gal}(L/k_\infty)$ are both profinite $\mathcal{A}$-modules with countable open $\mathcal{A}$-submodules. Therefore, by Theorem 1.2, it is enough to verify that, for every prime p, these Galois groups satisfy the conditions (I_p) and (II_p) in Theorem 1.3.

We first show that the condition (I_p) is satisfied. Let us first consider $X = \mathrm{Gal}(L/k_\infty)$. Let

$$(P_p)\qquad \begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{\alpha} & C & \longrightarrow & 0 \end{array}$$

be an embedding problem of $\mathcal{A}$-modules, where A, B and C are finite $\mathcal{A}$-modules with p-power orders. Taking the semi-direct product with $\mathfrak{g} = \mathrm{Gal}(k_\infty/k_1)$, we have the following embedding problem of profinite groups ;

$$(\tilde{P}_p)\qquad \begin{array}{ccccccccc} & & & & & & \mathfrak{g}\cdot X & & \\ & & & & & & \downarrow{\scriptstyle\tilde\varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & \mathfrak{g}\cdot B & \xrightarrow{\tilde\alpha} & \mathfrak{g}\cdot C & \longrightarrow & 1. \end{array}$$

Here, $\tilde\alpha$ and $\tilde\varphi$ are defined as $\tilde\alpha(\sigma b) = \sigma\alpha(b)$ and $\tilde\varphi(\sigma x) = \sigma\varphi(x)$ $(\sigma \in \mathfrak{g}, b \in B, x \in X)$ respectively.

Since $\mathfrak{g}$ is a free profinite group, the exact sequence

$$1 \longrightarrow X \longrightarrow \mathrm{Gal}(L/k_1) \longrightarrow \mathfrak{g} \longrightarrow 1$$

splits so that $\mathfrak{g}\cdot X$ is identified with the Galois group $\mathrm{Gal}(L/k_1)$.

As before, let $\tilde L$ denote the maximal unramified Galois extension of k_∞. Let $\Phi : \mathrm{Gal}(\tilde L/k_1) \to \mathfrak{g}\cdot C$ be the composite of $\tilde\varphi$ and the projection $\mathrm{Gal}(\tilde L/k_1) \to \mathrm{Gal}(L/k_1)$. Since $\mathrm{Gal}(\tilde L/k_1)$ is projective by Theorem 2.1, there exists a homomorphism $\Psi : \mathrm{Gal}(\tilde L/k_1) \to \mathfrak{g}\cdot B$ such that $\tilde\alpha\Psi = \Phi$.

We claim that Ψ factors through $\mathrm{Gal}(L/k_1)$. Indeed, as $\Phi^{-1}(C) = \mathrm{Gal}(\tilde L/k_\infty)$, we have

$$\Psi^{-1}(B) = \Psi^{-1}(\tilde\alpha^{-1}(C)) = \mathrm{Gal}(\tilde L/k_\infty).$$

Since B is abelian, we have $\Psi(\mathrm{Gal}(\tilde L/L)) = \{1\}$, i.e. Ψ factors through $\mathrm{Gal}(L/k_1)$.

Therefore, Ψ induces a weak solution $\tilde\psi$ of the embedding problem $(\tilde P_p)$. As can be easily verified, the restriction of $\tilde\psi$ to X gives a weak solution of the embedding problem (P_p) so that the condition (I_p) is satisfied for X.

That (I_p) is satisfied for $\mathrm{Gal}(M/k_\infty)$ can be proved in the same way by using, instead of Theorem 2.1, Corollary of Proposition 2.1.

(3-2) It remains to show that the condition (II_p) of Theorem 1.3 is also satisfied. As the $\mathcal{A}$-module $\mathrm{Gal}(L/k_\infty)$ is a quotient of $\mathrm{Gal}(M/k_\infty)$, it suffices to prove the following

Proposition 3.1. *Let m and n be any positive integers. Then 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 $\mathcal{A}$-modules.*

Proof. For each $n \geq 1$, let k_n be the unique subextension of k_∞/k_1 such that $[k_n : k_1] = n$. The Galois group $C_n = \mathrm{Gal}(k_n/k_1)$ is a cyclic group of order n. Let k_0 be a finite algebraic number field containing ζ_p and K_0 be a cyclic extension of k_0 of degree n such that k_1 is cyclotomic over k_0 and that $k_1 \cap K_0 = k_0$ and $k_1 K_0 = k_n$.

Fix an integer $q > 1$. By the theorem of primes in arithmetic progressions, there exists a prime l such that $l \equiv 1 \bmod q$ and that l is unramified in k_0. Since $\mathrm{Gal}(k_0(\zeta_l)/k_0)$ is a cyclic group of order $l-1$, there exists a subextension $\mathfrak{K}$ of $k_0(\zeta_l)/k_0$ such that $k_0(\zeta_l)$ is a cyclic extension of $\mathfrak{K}$ of degree q. Here we change the notations and denote the fields $k_0(\zeta_l)$ and $K_0(\zeta_l)$ by k_0 and K_0 respectively. Thus we have

$$\mathfrak{K} \subset k_0 \subset K_0 \subset k_\infty.$$

Let $\mathfrak{p}_1, ..., \mathfrak{p}_g$ be all prime ideals of K_0 lying above p. Let N_i $(1 \leq i \leq g)$ be a positive integer such that every element α of K_0 satisfying $\alpha \equiv 1 \bmod \mathfrak{p}_i^{N_i}$ is a p-th power in the $\mathfrak{p}_i$-adic completion of K_0. Let $\mathfrak{m}$ be an integral ideal such that $\mathfrak{p}_i^{N_i}$ divides $\mathfrak{m}$ 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 $\mathfrak{L}_i = (\alpha_i)$ $(1 \leq i \leq m)$ of K_0 satisfying

(i) $\alpha_i \equiv 1 \bmod \mathfrak{m}$.
(ii) the absolute degree of $\mathfrak{L}_i$ is one and $\mathfrak{L}_i$ is unramified in K_0.
(iii) the prime ideal $\mathfrak{L}_i \cap \mathbb{Q} = (l_i)$ $(1 \leq i \leq m)$ are distinct.

Let F_i be the field obtained by adjoining to K_0 p-th roots of α_i^σ $(1 \leq i \leq m)$, where σ runs over every element of C_n. Then F_i is a Kummer extension of K_0 with exponent p and is a Galois extension of k_0. By the conditions (i), (ii) and (iii), the primes $\mathfrak{p}_1, ..., \mathfrak{p}_g$ split completely in F_i and the extension F_i/K_0 is unramified outside $\mathfrak{L}_i^\sigma$ $(\sigma \in C_n)$. It is easy to see that $\mathrm{Gal}(F_i/K_0)$ is, as $\mathcal{A}$-modules, isomorphic to $E_n(p)$. Since α_i^σ $(1 \leq i \leq m,\ \sigma \in C_n)$ are multiplicatively independent in $K_0^*/(K_0^*)^p$, $F_1, ..., F_m$ are linearly disjoint over K_0. Therefore, the Galois group $\mathrm{Gal}(F/K_0)$ is isomorphic to $E_n(p)^{\oplus m}$, where F is the composite of $F_1, ..., F_m$.

We shall show that $F \cap k_\infty = K_0$. Let $K' = F \cap k_\infty$ and assume, on the contrary, that $K' \neq K_0$. Then there exists at least one prime $\mathfrak{L}_i^\sigma$ of K_0 which is ramified in K'. Let $\mathfrak{l} = \mathfrak{L}_i^\sigma \cap \mathfrak{K}$ and $\mathfrak{l}_0 = \mathfrak{L}_i^\sigma \cap k_0$.

As $\mathfrak{l}$ splits completely in K_0, there exists a prime $\mathfrak{l}_0'$ of k_0 such that $\mathfrak{l}_0 \neq \mathfrak{l}_0'$. By the condition (iii), every prime ideal of K_0 lying above $\mathfrak{l}_0'$ is, over k_0, neither conjugate to $\mathfrak{L}_i$ nor to $\mathfrak{L}_j$ $(j \neq i)$. Therefore $\mathfrak{l}_0'$ is unramified in K'. As $\mathfrak{l}_0$ is ramified in K' and K' is a cyclotomic, hence a Galois extension of $\mathfrak{K}$, this is a contradiction. Thus we have $F \cap k_\infty = K_0$.

Now we see that $F_i(\zeta_{l_i})$ is unramified over $K_0(\zeta_{l_i})$. This can be verified completely in the same way as the proof of Lemma 2.6 by noting that $l_i \equiv 1 \bmod p$, i.e. l_i splits completely in the subfield $\mathbb{Q}(\zeta_p)$ of K_0.

Therefore, it follows that the extension Fk_∞/k_∞ is unramified and the Galois group $\mathrm{Gal}(Fk_\infty/k_\infty)$ is isomorphic to $E_n(p)^{\oplus m}$.

References

[1] G.Cornell, *Abhyanker's lemma and the class group. In : Lecture Notes in Mathematics,* **751** (1979), Springer, 82-88.

[2] K. Iwasawa, *On solvable extensions of algebraic number fields*, Ann. Math. **5** (1953), 548-572.

[3] J.P.Serre, *Cohomologie Galoisienne, Lecture Notes in Mathematics*, vol. 5, Springer, 1964 (5. edition 1994).

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

Faculty of Engineering and Design, Kyoto Institute of Technology, Matsugasaki, Kyoto