Tohoku Math. J.
60 (2008), 135–147

ON GALOIS GROUPS OF ABELIAN EXTENSIONS OVER MAXIMAL CYCLOTOMIC FIELDS

MAMORU ASADA

(Received February 2, 2007, revised June 29, 2007)

Abstract. We shall consider the maximal cyclotomic extension of a finite algebraic number field and its two abelian extensions, the maximal abelian extension and the maximal abelian extension with certain restricted ramification. We shall investigate the structure of these Galois groups with the action of the cyclotomic Galois group.

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, $n = 1, 2, \ldots$. Let k_∞^{ab} and L be the maximal abelian extension of k_∞ and the maximal unramified abelian extension of k_∞, respectively. The Galois groups $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ 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 $\hat{\boldsymbol{Z}}$. Here $\hat{\boldsymbol{Z}}$ denotes the profinite completion of the ring of rational integers $\boldsymbol{Z}$. Indeed, more generally, if $\tilde{k}_\infty$ and $\tilde{L}$ denote the maximal solvable extension of k_∞ and the maximal unramified solvable extension of k_∞ respectively, the Galois groups $\mathrm{Gal}(\tilde{k}_\infty/k_\infty)$ and $\mathrm{Gal}(\tilde{L}/k_\infty)$ are both isomorphic to the free prosolvable group on countably infinite generators (Iwasawa [2], Uchida [4]).

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

In this paper, we shall consider two abelian extensions of k_∞. One is the maximal abelian extension k_∞^{ab} of k_∞ and the other is the maximal abelian extension M of k_∞ with restricted ramification. The field M is defined as follows. For a prime number p, let M_p be the maximal pro-p abelian extension of k_∞ unramified outside p. Then M is defined to be the composite of M_p, where p runs over all primes.

Let k_1 be the field obtained by adjoining ζ_4 and ζ_l for all odd prime l 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 $\hat{\boldsymbol{Z}}$. Note that, as $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ and $\mathrm{Gal}(M/k_\infty)$ are profinite abelian groups, they are naturally $\hat{\boldsymbol{Z}}$-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 $\hat{\boldsymbol{Z}}$. Our main result is the following

2000 *Mathematics Subject Classification.* Primary 11R18; Secondary 11R23.
Partly supported by the Grants-in-Aid for Scientific Research (C), Japan Society for the Promotion of Science.

THEOREM. *The Galois groups* $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ *and* $\mathrm{Gal}(M/k_\infty)$ *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 now 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 $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ and $\mathrm{Gal}(M/k_\infty)$. 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 $\mathrm{Gal}(M/k_\infty)$. A group theoretical point is that $\mathfrak{g}$ is a free profinite group (of rank 1) so that the projection $\mathrm{Gal}(M/k_1) \to \mathfrak{g}$ splits. By using this, the solvability of the embedding problem for the $\mathcal{A}$-module $\mathrm{Gal}(M/k_\infty)$ can be reduced to that of the embedding problem for the profinite group $\mathrm{Gal}(M/k_1)$. It can be further reduced to that of the embedding problem for the group $\mathrm{Gal}(\tilde{M}_p/k_1)$, where $\tilde{M}_p$ denotes, for a prime p, the maximal pro-p extension of k_∞ unramified outside p.

An arithmetical point is that the Galois group $\mathrm{Gal}(\tilde{M}_p/k_1)$ is projective. In Uchida [4], for an infinite algebraic number field K satisfying a certain condition such as k_1, it is shown that the Galois group $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ is projective. Here K^{ur} denotes the maximal unramified Galois extension of K. Though ramification occurs in the extension $\tilde{M}_p/k_1$, by a slight modification of his proof, we can show that $\mathrm{Gal}(\tilde{M}_p/k_1)$ is projective. From this the solvability of the embedding problem follows.

It seems to be an interesting problem to find canonical generators, as $\mathcal{A}$-modules, of $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ and $\mathrm{Gal}(M/k_\infty)$. It also seems to be a fundmental problem to investigate the structure of these Galois groups with the action of the whole cyclotomic Galois group $\mathrm{Gal}(k_\infty/k_0)$. At present, the author knows alomost nothing about these.

Whether the Galois group $\mathrm{Gal}(L/k_\infty)$ is also isomorphic to $\prod_{N=1}^{\infty}\mathcal{A}$ or not is an open problem. We shall give a partial result about this Galois group (Proposition 3.1).

The author first obtained the above mentioned $\mathcal{A}$-module version of Iwasawa's theorem. Then Professor Shoichi Nakajima pointed out that one can prove a more general version of it, which gives a characterization of the free pro-S group on countably infinite generators with operator domain $\hat{\Gamma}$, where $\hat{\Gamma}$ 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 $\mathcal{A}$-module version mentioned above. In Section 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 Section 2 we shall prove that the Galois group $\mathrm{Gal}(\tilde{M}_p/k_1)$ is projective. In Section 3 the proof of Theorem is given.

As noticed above, for our proof, we owe much to Iwasawa [2] and Uchida [4]. We shall give in this paper the details of proofs of the modified versions of their theorems, since an application of embedding problems to the study of the cyclotomic Galois action on Galois groups of abelian extensions over k_∞ 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 $x_1, x_2, \ldots$ 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 S be a category of finite groups whose objects 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 normal Γ-subgroups of finite index 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 also at most countable.

The profinite completion $\hat{\Gamma}$ 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

$$\hat{\Gamma} \to \varprojlim A_N \subset \mathrm{Aut}F_S\,,$$

which shows that $\hat{\Gamma}$ operates on F_S.

We call the group F_S the free pro-S $\hat{\Gamma}$-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 $\psi : X \to B$ such that $\alpha\psi = \varphi$. If, moreover, ψ is surjective, then ψ is called a proper solution, or simply a

solution. When A, B, C and X are profinite groups with operator domain $\hat{\Gamma}$ and homomorphisms of the diagram are $\hat{\Gamma}$-homomorphisms, then a (weak) solution is also assumed to be a $\hat{\Gamma}$-homomorphism.

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

THEOREM 1.1. *Let X be a pro-S $\hat{\Gamma}$-group with at most countable open $\hat{\Gamma}$-subgroups. Then X is isomorphic to F_S as $\hat{\Gamma}$-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 $\hat{\Gamma}$.*

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

(1-3) Now we shall restrict ourselves to the case that Γ is an infinite cyclic group, so that $\hat{\Gamma} \simeq \mathfrak{g}$, $\mathfrak{g}$ being the Galois group $\mathrm{Gal}(k_\infty/k_1)$, and S is the category of finite abelian groups. Let $\mathcal{A}$ denote the completed group algebra of $\mathfrak{g}$ over the profinite completion $\hat{\boldsymbol{Z}}$ of the ring of integers $\boldsymbol{Z}$, i.e.,

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

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

$$(P_{\mathcal{A}}) \qquad \begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0\,. \end{array}$$

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 follows.

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 $\boldsymbol{F}_p[C_n]$ denote the group algebra of C_n over the prime field $\boldsymbol{F}_p$ of characteristic p. Via the projection $\mathfrak{g} \to C_n$, $\boldsymbol{F}_p[C_n]$ is naturally regarded as a $\mathfrak{g}$-module, and hence as 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, Theorem 1]. (See also Serre [3, I, 3.4, Exercices 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) To prove 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, and hence are $\mathcal{A}$-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

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle \bar{\varphi}} & & \\ 0 & \longrightarrow & A_p & \longrightarrow & B_p & \longrightarrow & C_p & \longrightarrow & 0\,, \end{array}$$

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 $\gamma : X \to B = \bigoplus B_p$ 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

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & A/A_1 & \longrightarrow & B/A_1 & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

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

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & & & \downarrow{\scriptstyle \psi_1} & & \\ 0 & \longrightarrow & A_1/A_2 & \longrightarrow & B/A_2 & \longrightarrow & B/A_1 & \longrightarrow & 0 \end{array}$$

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.

(a) *Any $\mathcal{A}$-submodule B' of B such that $\alpha(B') = C$ coincides with B.*

(b) *The sequence splits, and 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. The necessity of (i) 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 $\mathrm{pr}_1 : A \oplus C \to A$ be the projection and Y be the kernel of $\mathrm{pr}_1\psi$. 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 by the property (a).

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 $\psi : X \to A \oplus C$ of the embedding problem (P_p). □

(1-6) 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 $\boldsymbol{F}_p[C_n]$-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 $\mathcal{S}$ consisting of proper open $\mathcal{A}$-submodules of X containing X' and let s be its cardinality. By the condition (II_p) for $m = s + 1$, there exist open $\mathcal{A}$-submodules $X_1, \ldots, X_{s+1}$ such that $X/X_i \simeq E_n(p)$ and $X_i + X_j = X$ for $i \neq j$. We have $X' + X_i \in \mathcal{S}$ or $X' + X_i = X$. Further, if $X' + X_i$ and $X' + X_j$ belong to $\mathcal{S}$ for $i \neq j$, we have $X' + X_i \neq X' + X_j$. Therfore, 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_l for all odd prime l 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, $n \geq 1$. For a prime number p, let $\tilde{M}_p$ denote the maximal pro-p extension of k_∞ unramified outside p.

What we shall need for the proof of Theorem is the fact that the absolute Galois group $\mathrm{Gal}(\bar{k}_1/k_1)$ of k_1 and the Galois group $\mathrm{Gal}(\tilde{M}_p/k_1)$ 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. *Let p be a prime. Then the Galois group* $\mathrm{Gal}(\tilde{M}_p/k_1)$ *is a projective profinite group.*

In [4], Uchida has proved that, for an infinite algebraic number field K satisfying a certain condition, the Galois group $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ 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 $K = k_1$. Though his theorem cannot be applied to $\mathrm{Gal}(\tilde{M}_p/k_1)$, 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. In our simpler case that the ground field is k_1, a detailed proof is given for the sake of completeness.

The main part of the proof is to show that a certain Galois group over k_1 is a free pro-p group (Theorem 2.2). Its proof is a little long and it is desirable that we find a more simplified proof.

(2-2) We shall first reduce the proof of Theorem 2.1, as in the arguement of [4, Theorem 1], to showing the projectivity of the maximal pro-p *quotient* of $\mathrm{Gal}(\tilde{M}_p/k_1)$.

Let G be an arbitrary profinite group and l be a prime number. We denote by $\mathrm{cd}G$ and $\mathrm{cd}_l G$ the cohomological dimension and the l-cohomological dimension of G, respectively. We also denote by $G(l)$ the maximal pro-l 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 l.*

$(*_l)$ *For any open subgroup U of G, $\mathrm{cd}_l U(l) \leq 1$.*

Then we have $\mathrm{cd}G \leq 1$, i.e., G is projective.

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

$$G = U_1 \supset U_2 \supset \cdots \supset U_n \supset U_{n+1} \supset \cdots, \bigcap_{n=1}^{\infty} U_n = G_l\,.$$

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

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

$$H^2(G_l : \boldsymbol{F}_l) = \varinjlim H^2(U_n(l) : \boldsymbol{F}_l) = \{0\}\,.$$

Thus it follows that $\mathrm{cd}_l G_l \leq 1$ ([3, I, Proposition 2]). Since $\mathrm{cd}_l G = \mathrm{cd}_l G_l$ ([3, I, Proposition 14]) and l is arbitrary, we have $\mathrm{cd}G \leq 1$. □

We shall apply the above lemma to the Galois group $G = \mathrm{Gal}(\tilde{M}_p/k_1)$. Let $U = \mathrm{Gal}(\tilde{M}_p/F_1)$ 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 $F_1 = F_0(\zeta_4, \zeta_l; l \geq 3)$ and that $\tilde{M}_p$ is the maximal pro-p extension of $F_\infty = F_0(\zeta_n; n \geq 1)$ unramified outside p. Therefore, the proof of Theorem 2.1 is reduced to showing that for every prime number l, $\mathrm{cd}_l G(l) \leq 1$, or equivalently, $G(l)$ is a free pro-l group ([3, I, 4.2]).

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 $\boldsymbol{Z}_l$, the additive group of l-adic integers. Hence we have $cd_l G(l) = 1$.

Assume next 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 $\tilde{M}_p$.

LEMMA 2.2. *The field $M^{(p)}$ is the maximal pro-p extension of k_1 unramified outside p.*

PROOF. Let q be a prime different from p and v_q be a q-place of k_1, i.e., a finite place of k_1 which is an extension of the q-adic place of $\boldsymbol{Q}$. The inertia group of v_q in the extension k_∞/k_1 is a pro-q group and $\tilde{M}_p/k_\infty$ is unramifed outside p. Therefore, as $M^{(p)} \subset \tilde{M}_p$, the inertia group of any extension of v_q to $M^{(p)}$ is a pro-q group. Thus it is the trivial group as $G(p)$ is a pro-p group. This shows that v_q is unramified in $M^{(p)}$. Therefore $M^{(p)}/k_1$ is unramified outside p. The maximality of $M^{(p)}$ follows from the maximality of $\tilde{M}_p$. □

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 $M^{(p)}$ 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.*

(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 $G(p) = \mathrm{Gal}(M^{(p)}/k_1)$, E is a finite p-group and C_p is a cyclic group of order p. Then, in order that $\mathrm{cd}_p G(p) \leq 1$, it is necessary and sufficient that every embedding problem (P) has a weak solution. This follows from e.g., [3, I, Proposition 16] and the fact that every finite p-group is obtained from a series of central extensions by cyclic groups of order p. 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 $M^{(p)}/k_1$ 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 $M^{(p)}$.

(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, $k_1 \boldsymbol{Q}_l$ contains the maximal unramified extension of $\boldsymbol{Q}_l$.*

For the proof, cf. e.g., [4, Lemma 1]. (The field k_1 contains the field $\boldsymbol{Q}^{(1)}$ in [4].)

By Proposition 2.1, as k_1 is totally imaginary, we obtain the following corollary (cf., e.g., [3, II, Proposition 9]).

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

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 corollary above, 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 that $\mu^\sigma \equiv \mu \mod (F^*)^p$ for every $\sigma \in \mathrm{Gal}(F/k_1)$. Further, by simple calculations of 2-cocycle associated to the group extension, we see that any field of the form $F(\sqrt[p]{\mu a})$ $(a \in k_1^*)$ gives a solution of the same embedding problem. We shall find an element $a \in k_1^*$ such that $F(\sqrt[p]{\mu a})$ is contained in $M^{(p)}$.

As $F(\sqrt[p]{\mu})/k_1$ is a finite extension, there exist a finite algebraic number field k_0 and its finite Galois extension F_0 such that $\zeta_p \in k_0$, $\mu \in F_0$, $F_0(\sqrt[p]{\mu}) \cap k_1 = k_0$ and $F_0(\sqrt[p]{\mu})k_1 = F(\sqrt[p]{\mu})$. We may assume, by taking k_0 sufficiently large, that F_0/k_0 is unramified outside p.

LEMMA 2.3. *There exist an ideal* $\mathfrak{m}$ *of* k_0, *an ideal* $\mathfrak{a}$ *of* F_0, *and an ideal* $\mathfrak{b}$ *of* F_0 *which is a product of primes lying above* p *such that* $(\mu) = \mathfrak{m}\mathfrak{b}\mathfrak{a}^p$.

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

Let us consider the ideal class group of k_0. By the density theorem, there exists a prime ideal $\mathfrak{q}$ of k_0 whose absolute degree is one, which is unramified over $\boldsymbol{Q}$, and which belongs to the class of $\mathfrak{m}$. Thus we have $\mathfrak{q} = \mathfrak{m}(a)$ with some element a of k_0^*. The field $F_0(\sqrt[p]{\mu a})$ also gives a solution of the embedding problem and, as $(\mu a) = (\mu)(a) = \mathfrak{q}\mathfrak{b}\mathfrak{a}^p$, the extension $F_0(\sqrt[p]{\mu a})/F_0$ is unramified outside $\mathfrak{q}$ and p.

LEMMA 2.4. *Let* $q = \mathfrak{q} \cap \boldsymbol{Z}$. *Then the extension* $F_0(\zeta_q, \sqrt[p]{\mu a})/F_0(\zeta_q)$ *is unramified outside* p.

PROOF. We shall show that any prime ideal of $F_0(\zeta_q)$ lying above $\mathfrak{q}$ is unramified in $F_0(\zeta_q, \sqrt[p]{\mu a})$. First we note that, as $\boldsymbol{Q}(\zeta_p) \subset k_0$ and the absolute degree of $\mathfrak{q}$ is one, the prime q splits completely in $\boldsymbol{Q}(\zeta_p)$, i.e., $q \equiv 1 \mod p$. Since $k_0 \cap \boldsymbol{Q}(\zeta_q) = \boldsymbol{Q}$, we have $[k_0(\zeta_q) : k_0] = q - 1$. As $k_1 \cap F_0(\sqrt[p]{\mu a}) = k_0$, we have $F_0(\zeta_q) \cap F_0(\sqrt[p]{\mu a}) = F_0$.

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 is unramified in F_0, $\tilde{\mathfrak{q}}$ is totally and tamely ramified in $F_0(\zeta_q)$. As the extension degree p of $F_0(\sqrt[p]{\mu a})/F_0$ 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 $F_0(\zeta_q, \sqrt[p]{\mu a})$. □

By Lemma 2.4, it follows that the extension $F(\sqrt[p]{\mu a})/F$ is unramified outside p, and hence $F(\sqrt[p]{\mu a})$ is contained in $M^{(p)}$. Thus the proof of Theorem 2.2 is completed. □

3. Proof of Theorem. (3-1) The Galois groups $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ and $\mathrm{Gal}(M/k_\infty)$ 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 number 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 $X = \mathrm{Gal}(M/k_\infty)$. 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. Then φ factors through $X(p) = \mathrm{Gal}(M_p/k_\infty)$ and induces an $\mathcal{A}$-homomorphism $\varphi_p : X(p) \to C$. Taking the semi-direct product with $\mathfrak{g} = \mathrm{Gal}(k_\infty/k_1)$, we have the following embedding problem of profinite groups:

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

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

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

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

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

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

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

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

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

Thus, Ψ induces a weak solution $\tilde{\psi}_p$ of the embedding problem $(\tilde{P}_p)$. Let ψ be the composite of the restriction of $\tilde{\psi}_p$ to $X(p)$ and the projection $X \to X(p)$. Then, as can be easily verified, ψ gives a weak solution of the embedding problem (P_p), i.e., an $\mathcal{A}$-homomorphism from X to B such that $\alpha\psi = \varphi$. Therefore, the condition (I_p) is satisfied for X.

That (I_p) is satisfied for $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ 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 for the $\mathcal{A}$-modules $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$ and $\mathrm{Gal}(M/k_\infty)$. We shall show somewhat more than this. As in the introduction, let L be the maximal unramified abelian extension of k_∞. We shall show that the condition (II_p) of Theorem 1.3 is satisfied for the $\mathcal{A}$-module $\mathrm{Gal}(L/k_\infty)$, which is a quotient of $\mathrm{Gal}(M/k_\infty)$, and hence that of $\mathrm{Gal}(k_\infty^{\mathrm{ab}}/k_\infty)$. Namely we shall prove the following

PROPOSITION 3.1. *Let m and n be any positive integers and p be a prime. 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 notation 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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ 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 of K_0 such that $\mathfrak{p}_i^{N_i}$ divides $\mathfrak{m}$ for $1 \leq i \leq g$ 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 $\mathfrak{L}_i = (\alpha_i)$, $1 \leq i \leq m$, 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 $\mathfrak{L}_i \cap \boldsymbol{Q} = (l_i)$ $(1 \leq i \leq m)$ are distinct.

For each element σ of C_n, let $F_{i,\sigma}$ be the field obtained by adjoining to K_0 p-th roots of α_i^σ, $1 \leq i \leq m$. Further, let F_i be the composite of $F_{i,\sigma}$, 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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ 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 $E_n(p)$. By the conditions (ii) and (iii), α_i^σ, where $1 \leq i \leq m$, $\sigma \in C_n$, are multiplicatively independent in $K_0^*/(K_0^*)^p$. Therefore, $F_1, \ldots, F_m$ are linearly disjoint over K_0 so that the Galois group $\mathrm{Gal}(F/K_0)$ is isomorphic to $E_n(p)^{\oplus m}$, where F is the composite of $F_1, \ldots, F_m$.

We shall show that $F \cap k_\infty = K_0$. Let $K' = F \cap k_\infty$ and assume, on the contrary, that $K' \neq K_0$. Note that $F_{i,\sigma}$ is a cyclic extension of degree p over K_0 which is totally ramified at $\mathfrak{L}_i^\sigma$ and F is the composite of all $F_{i,\sigma}$, where $1 \leq i \leq m$, $\sigma \in C_n$. Therefore, as can be easily seen, 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 lying above $\mathfrak{l}$ 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 $\mathfrak{L}_j$ for $j \neq i$. Therefore $\mathfrak{l}_0'$ is unramified in K'. As $\mathfrak{l}_0$ is ramified in K' and K'

is a cyclotomic, and hence is 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 2.4 by noting that $l_i \equiv 1 \bmod p$, i.e., l_i splits completely in the subfield $\boldsymbol{Q}(\zeta_p)$ 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, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), 82–88, Lecture Notes in Math. 751, Springer, Berlin, 1979.

[2] K. IWASAWA, On solvable extensions of algebraic number fields, Ann. of Math. (2) 5 (1953), 548–572, also see Collected papers Vol. I [27], Springer, 2001.

[3] J.-P. SERRE, Cohomologie galoisienne, Fifth edition, Lecture Notes in Math. 5, Springer, Berlin, 1994.

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

GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY
KYOTO INSTITUTE OF TECHNOLOGY
MATSUGASAKI, KYOTO 606–8585
JAPAN