On Galois groups over tamely ramified cyclotomic extensions of algebraic number fields

Mamoru Asada

Abstract. Let k_0 be an algebraic number field of finite degree, S_0 be a finite set of primes and L_{S_0} be the field obtained by adjoining to k_0 all primitive q-th roots of unity, where q runs over all primes not belonging to S_0. We shall consider, for an odd prime l, the maximal unramified pro-l abelian extension of L_{S_0} and investigate the structure of this Galois group with certain cyclotomic action.

2020 *Mathematics Subject Classification.* Primary 11R32; Secondary 11R18
Keywords and Phrases. unramified extensions, cyclotomic extensions.

Introduction

Let k_0 be an algebraic number field of finite degree in a fixed algebraic closure and ζ_n denote a primitive n-th root of unity, $n \geq 1$. Let S_0 be a (possibly empty) finite set of primes and L_{S_0} be the field obtained by adjoining all ζ_q to k_0, where q runs over all primes not belonging to S_0. Let l be a prime and $L_{ur}(l)$ and $L_{ur}^{ab}(l)$ denote the maximal unramified pro-l extension and the maximal unramified pro-l abelian extension of L_{S_0}, respectively. The structures of the Galois groups $\mathrm{Gal}(L_{ur}(l)/L_{S_0})$ and $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ are known. The Galois group $\mathrm{Gal}(L_{ur}(l)/L_{S_0})$ is isomorphic to a free pro-l group on countably infinite generators, and consequently, the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is isomorphic to the direct product of countable number of copies of the additive group of l-adic integers. This follows from a more general result of Uchida[14], which implies that the Galois group over L_{S_0} of the maximal unramified solvable extension of L_{S_0} is isomorphic to the free prosolvable group on countably infinite generators.

The Galois group $\mathrm{Gal}(L_{S_0}/k_0)$ acts on $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ naturally, i.e. $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is a $\mathrm{Gal}(L_{S_0}/k_0)$-module. However, it seems difficult to describe its $\mathrm{Gal}(L_{S_0}/k_0)$-module structure. Let $\mathfrak{p}$ be a prime of k_0 and assume that it is unramified in L_{S_0}. Let D be its decomposition group for the extension L_{S_0}/k_0. We are interested in the D-module structure of $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ and our main result in this paper is to determine it under several assumptions.

Before stating our main result more precisely, we explain the reasons why we take the field L_{S_0} as a ground field and are interested in the D-module structure of $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$.

According to the analogy between algebraic number fields of finite degree and function fields of one variable over a finite constant field $\mathbb{F}$, adjoining ζ_n to k_0, where n runs over all positive integers or all powers of a fixed prime, are some of the substitutes of extending $\mathbb{F}$ to its algebraic closure $\bar{\mathbb{F}}$. In addition to these, the field L_{S_0} can also be regarded as a substitute of extending $\mathbb{F}$ to $\bar{\mathbb{F}}$. The reasons are as follows.

For one thing, (a) the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$ is obtained by adjoining primitive q-th roots of unity, where q runs over all primes except for a finite number. For another thing, (b) the decomposition group D of $\mathfrak{p}$ for the extension L_{S_0}/k_0 is isomorphic to $\widehat{\mathbb{Z}}$, the profinite completion of the additive group of rational integers. Further, the extension L_{S_0}/L_D, L_D being the decomposition field of $\mathfrak{p}$ in L_{S_0}/k_0, is everywhere unramified (Lemma 2.1). (These two facts $(a), (b)$ follow from a result of Chevalley[4].) This shows that the extension L_{S_0}/L_D is similar to the extension $\bar{\mathbb{F}}/\mathbb{F}$ in the function field case.

By the reason (a), the Galois groups $\mathrm{Gal}(L_{ur}(l)/L_{S_0})$ and $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ may be regarded as analogues of the pro-l fundamental group and the l-adic Tate module of a smooth curve over $\bar{\mathbb{F}}$. By the reason (b), the D-module structure of $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ might be interesting.

Our result on the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is the following theorem. Let $\mathcal{A}_l$ denote the completed group algebra of D over the ring of l-adic integers $\mathbb{Z}_l$. Then, as $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is a pro-l abelian group, it is naturally an $\mathcal{A}_l$-module.

Theorem (Theorem 4.3). *Let l be an odd prime and k_0 be an algebraic number field of finite degree such that l is unramified in k_0. Let p be a prime such that $p \neq l$ and S_0 be a finite set of primes containing p and l. Let L_{S_0} be the field obtained by adjoining ζ_q to k_0, where q runs over all primes not belonging to S_0. Let $\mathfrak{p}$ be a prime of k_0 lying above p and D be its decomposition group for the extension L_{S_0}/k_0.*

Then the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is, as an $\mathcal{A}_l$-module, isomorphic to the direct product of a countable number of copies of $\mathcal{A}_l$.

Somewhat more generally, for an infinite tamely ramified abelian extension L of k_0 satisfying several conditions, we shall investigate the $\mathcal{A}_l$-module structure of the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ and obtain our general result (Theorem 4.2). (Here, $L_{ur}^{ab}(l)$ denotes the maximal unramified pro-l abelian extension of L.) Since the field L_{S_0} in the above theorem satisfies these conditions, the above theorem follows.

The $\mathcal{A}_l$-module $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ we have considered is huge and its structure is independent of the ground field k_0. One of the reasons why $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ is huge is that $L_{ur}^{ab}(l)$ contains those unramified extensions of L that originate in (tamely) *ramified* extensions F of various subextensions k of L/k_0. Namely, the ramifications of F/k are absorbed in L/k so that FL/L is unramified. (Much smaller fields than L_{S_0} are treated as ground fields in [14], but similar phenomena also occur in those cases.) In the case of function fields, such phenomena do not occur. Hence it is desirable to remove those extensions FL from $L_{ur}^{ab}(l)$ and clarify "genuine" unramified extensions buried in $L_{ur}^{ab}(l)$. But the author does not know how to do this. Further, the above theorem does not include the case that $L_{ur}^{ab}(l)$ contains the maximal unramified pro-l abelian extension of $\mathbb{Q}(\zeta_l)$, which seems to be interesting. Nevertheless, our result might be of some interest, for in the process of obtaining the above theorem, we have investigated structures of

related Galois groups and clarified, to some extent, which properties affect the structure of which Galois groups.

We shall briefly explain the method of the proof. There are two arithmetical points to determine the $\mathcal{A}_l$-module structure of the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$.

One is to show that the larger Galois group $\mathrm{Gal}(L_{S_L}(l)/L_D)$ is a projective profinite group, where $L_{S_L}(l)$ denotes the maximal pro-l extension of L unramified outside l. This reduces at once to showing that the pro-l group $\mathrm{Gal}(L_{S_L}(l)/K)$ is free, where K is the unique subextension of L/L_D such that $\mathrm{Gal}(L/K)$ is isomorphic to $\mathbb{Z}_l$. Then, $L_{S_L}(l)$ coincides with $K_{S_K}(l)$, the maximal pro-l extension of K unramified outside l. In our previous papers [1],[2], similar situations have arised. But there, the cohomological dimension (or cohomological l-dimension) of the ground field is 1, whereas that of K is not. Thus, our task is to show the vanishing of the second Galois cohomology group $\mathrm{H}^2(\mathrm{Gal}(K_{S_K}(l)/K); \mathbb{Z}/l\mathbb{Z})$. This will be carried out by showing that both the kernel and the image of the localization map of the Galois cohomology group vanish under suitable assumptions on the extension L/k_0. The crucial point here is a result of Neukirch[7] which shows that the kernel is trivial if and only if certain embedding problem is solvable, and we shall apply its "if part". Another arithmetical point is, after verifying that $\mathrm{Gal}(L_{S_L}(l)/K)$ is a free pro-l group, to show that its quotient $\mathrm{Gal}(L_{ur}(l)/K)$ is also a free pro-l group. As for its proof, we owe the method to [14]. Here, another condition on the extension L/k_0 is needed.

An outline of the paper is as follows. In §1, we shall give a criterion of the vanishing of the kernel of the localization map. This is a result of [7] combined with a result of O. Neumann[9]. We shall formulate it over an algebraic number field which is not necessarily of finite degree. As explained above, we have assumed, at each stage of the arguments, conditions on the extension L/k_0. In §2, we consider an infinite abelian extension L of an algebraic number field of finite degree k_0 satisfying certain conditions (I_1) and (I_2) and show that, for such an extension, the kernel of the localization map vanishes. In §3, we add another conditions (II_l) and (III_l) to the extension L/k_0 and show that the pro-l groups $\mathrm{Gal}(L_{S_L}(l)/K)$ and $\mathrm{Gal}(L_{ur}(l)/K)$ are free, under the conditions (I_1), (I_2) and (II_l) and under the conditions (I_1), (I_2), (II_l) and (III_l), respectively. In §4 we shall prove that, for an extension L of k_0 satisfying (I_1), (I_2), (II_l), (III_l) and $[L(\zeta_l) : L] = l - 1$, the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ is, as an $\mathcal{A}_l$-module, isomorphic to $\prod_{N=1}^{\infty} \mathcal{A}_l$, the direct product of a countable number of copies of $\mathcal{A}_l$ (Theorem 4.2). Here we use a characterization of the pro-l $\mathcal{A}_l$-module $\prod_{N=1}^{\infty} \mathcal{A}_l$ in terms of embedding problems of $\mathcal{A}_l$-modules and a topological condition ([1]). Further, it is verified that the field L_{S_0} in the main result satisfies all these conditions. This is a consequence of a result of Chevalley[4]. Applying Theorem 4.2, we thus obtain the main result. As a consequence of Theorem 4.2, in §5, we show some properties of decomposition groups for the unramified non-abelian extension $L_{ur}^{ab}(l)/L_D$.

The author expresses his gratitudes to Professor Akio Tamagawa for valuable information and stimulating discussions. When the author first obtained Theorem 4.2 (i) (the unramified outside l case), he informed him a result of [4] with the indication of Propositions 4.1 and 4.2. This enables the author, after several years, to consider the condition (III_l) and obtain Theorem 4.2(ii)(the unramified case). The author also

expresses his gratitudes to the late Professor Akito Nomura for stimulating discussions about embedding problems of Galois groups.

1. A criterion of the vanishing of the kernel of the localization map

In his investigations on embedding problems on Galois groups over algebraic number fields, Neukirch[7] has given, among other interesting results, a necessary and sufficient condition for the kernel of the localization map to be trivial in terms of embedding problems.

In this section, we shall give a version of this Neukirch's result. This is obtained by combining it with a result of Neumann[9] and is formulated for Galois groups over algebraic number fields which are not necessarily of finite degree.

For an algebraic number field K, not necessarily of finite degree, we denote by G_K the absolute Galois group of K. We fix a prime l and denote by S_K the set of archimedean primes of K and the primes of K lying above l. We also denote by G_{S_K} the Galois group over K of the maximal Galois extension of K unramified outside S_K. When K is totally imaginary, we sometimes say that an extension of K is unramified outside l instead of unramified outside S_K.

Let $G_K(l)$ and $G_{S_K}(l)$ denote the maximal pro-l quotient of G_K and G_{S_K} respectively, i.e. $G_K(l)$ and $G_{S_K}(l)$ are the Galois groups over K of the maximal pro-l extension of K and the maximal pro-l extension of K unramified outside of S_K respectively.

We shall consider the following embedding problem

$$(\mathcal{E}) \qquad \begin{array}{ccccccccc} & & & & & & G_K(l) & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & \mathbb{Z}/l\mathbb{Z} & \longrightarrow & E & \xrightarrow{\alpha} & H & \longrightarrow & 1. \end{array}$$

Here, the horizontal sequence is an exact sequence of finite l-groups and φ is a surjective homomorphism. A weak solution of this problem is a homomorphism $\psi : G_K(l) \to E$ such that $\alpha\psi = \varphi$. If the problem has a weak solution, it is called solvable. Note that $\mathbb{Z}/l\mathbb{Z}$ is contained in the center of E and hence $\mathbb{Z}/l\mathbb{Z}$ is naturally a trivial H-module. In the following, we always assume that *in* $(\mathcal{E})$ φ *factors through* $G_{S_K}(l)$.

Let k be an algebraic number field of finite degree contained in K. For each prime v of k, let k_v be the v-completion of k and G_{k_v} denote the absolute Galois group of k_v.

Let f_{S_k} denote the localization map of the Galois cohomology group $\mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z})$ of the trivial G_{S_k}-module $\mathbb{Z}/l\mathbb{Z}$:

$$(*S_k) \qquad f_{S_k} : \mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z}) \to \bigoplus_{v \in S_k} \mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z})$$

(Cf. Neukirch, Schimidt, Wingberg [8, (8.6.2)].) When k runs over all algebraic number fields of finite degree contained in K, $(*S_k)$ are naturally inductive systems. We have the following criterion of the vanishing of the inductive limit $\varinjlim \mathrm{Ker} f_{S_k}$ of the kernels of f_{S_k}.

Theorem 1.1. *The following three conditions are equivalent.*

(i) *Every solvable problem* $(\mathcal{E})$ *has a weak solution which factors through* $G_{S_K}(l)$.

(ii) *The inflation homomorphism* $\mathrm{Inf}_1 : \mathrm{H}^2(G_{S_K}(l); \mathbb{Z}/l\mathbb{Z}) \to \mathrm{H}^2(G_K(l); \mathbb{Z}/l\mathbb{Z})$ *is injective.*

(iii) *We have* $\varinjlim \mathrm{Ker} f_{S_k} = \{0\}$.

Proof. The proof of the equivalence of (i) and (ii) is purely group-theoretical and will be done in the same way as that given in [7, (8.1)], and hence is omitted.

We shall show the equivalence of (ii) and (iii). By a result of [9](cf. also [8, (10.4.8)]), for an algebraic number field k of finite degree, the inflation maps

$$\mathrm{H}^2(G_{S_k}(l); \mathbb{Z}/l\mathbb{Z}) \to \mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z})$$

$$\mathrm{H}^2(G_k(l); \mathbb{Z}/l\mathbb{Z}) \to \mathrm{H}^2(G_k; \mathbb{Z}/l\mathbb{Z})$$

are isomorphisms.

Since we have $G_{S_K} = \varprojlim G_{S_k}$, by taking inductive limits, we have the following commutative diagram :

$$\begin{array}{ccc} \mathrm{H}^2(G_{S_K}(l); \mathbb{Z}/l\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(G_{S_K}; \mathbb{Z}/l\mathbb{Z}) \\ {\scriptstyle \mathrm{Inf}_1}\downarrow & & \downarrow{\scriptstyle \mathrm{Inf}_2} \\ \mathrm{H}^2(G_K(l); \mathbb{Z}/l\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(G_K; \mathbb{Z}/l\mathbb{Z}) \end{array}$$

Here, vertical homomorphisms are the inflation homomorphisms. Therefore, we first observe that (ii) is equivalent to that the homomorphism Inf_2 is injective.

Let f_k denote the localization map of the Galois cohomology group $\mathrm{H}^2(G_k; \mathbb{Z}/l\mathbb{Z})$ of the trivial G_k-module $\mathbb{Z}/l\mathbb{Z}$:

$$(*_k) \qquad f_k : \mathrm{H}^2(G_k; \mathbb{Z}/l\mathbb{Z}) \to \bigoplus_v \mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z})$$

Here, v runs over all primes of k. As is verified in the proof of [7, (8.1)], two localization maps f_{S_k} and f_k are connected as the following diagram :

$$(**) \qquad \begin{array}{ccc} \mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(G_k; \mathbb{Z}/l\mathbb{Z}) \\ {\scriptstyle f_{S_k}}\downarrow & & \downarrow{\scriptstyle f_k} \\ \bigoplus_{v \in S_k} \mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z}) & \longrightarrow & \bigoplus_v \mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z}) \end{array}$$

Here, the upper horizontal homomorphism is the inflation homomorphism and the lower one is the inclusion. It is known that f_k is injective ([7, (4.7)]).

When k runs over all algebraic number fields of finite degree contained in K, $(*_k)$ are also inductive systems. Then one first proves that

$$\varinjlim \bigoplus_{v\in S_k} \mathrm{H}^2(G_{k_v};\mathbb{Z}/l\mathbb{Z}) = \prod_{w\in S_K} \mathrm{H}^2(G_{K_w};\mathbb{Z}/l\mathbb{Z}),$$

$$\varinjlim \bigoplus_{v} \mathrm{H}^2(G_{k_v};\mathbb{Z}/l\mathbb{Z}) = \prod_{w} \mathrm{H}^2(G_{K_w};\mathbb{Z}/l\mathbb{Z}).$$

Here, w runs over all primes of S_K and all primes of K respectively. For a prime w of K, K_w denotes the union $\cup_k k_w$, where k runs over all algebraic number fields of finite degree contained in K and k_w denotes the completion of k with respect to the restriction of w to k.

Therefore, by taking inductive limits of $(**)$, we have the commutative diagram :

$$\begin{array}{ccc} \mathrm{H}^2(G_{S_K};\mathbb{Z}/l\mathbb{Z}) & \xrightarrow{\mathrm{Inf}_2} & \mathrm{H}^2(G_K;\mathbb{Z}/l\mathbb{Z}) \\ {\scriptstyle f_{S_K}}\downarrow & & \downarrow{\scriptstyle f_K} \\ \prod_{w\in S_K} \mathrm{H}^2(G_{K_w};\mathbb{Z}/l\mathbb{Z}) & \longrightarrow & \prod_{w} \mathrm{H}^2(G_{K_w};\mathbb{Z}/l\mathbb{Z}) \end{array}$$

Here $f_{S_K} = \varinjlim f_{S_k}$ and $f_K = \varinjlim f_k$.

Since inductive limit preserves the injectivity, f_K is injective. Thus, Inf_2 is injective if and only if f_{S_K} is injective. Therefore, (ii) is equivalent to (iii) and this completes the proof of Theorem 1.

2. Infinite abelian extensions

(2-1) Let k_0 be an algebraic number field of finite degree. We shall consider an infinite abelian extension L of k_0 satisfying the following conditions (I_1) and (I_2):

(I_1) For any finite prime $\mathfrak{q}$ of k_0, its inertia group for the extension L/k_0 is a finite group. Further, for all finite prime $\mathfrak{q}$ of k_0 except for a finite number, the order of its inertia group is $q-1$, where q is a prime such that $\mathfrak{q}\cap\mathbb{Z} = (q)$.

(I_2) There exists a finite prime $\mathfrak{p}$ of k_0 such that $\mathfrak{p}$ is unramified in L and that the decomposition group of $\mathfrak{p}$ for the extension L/k_0 is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of the additive group of rational integers.

As before, let l be a fixed prime and $L_{S_L}(l)$ be the maximal pro-l extension of L unramified outside S_L.

Let L_D be the decomposition field of $\mathfrak{p}$ in L/k_0. By the condition (I_2), there exists a unique subextension K of L/L_D such that the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to $\mathbb{Z}_l$, the additive group of l-adic integers.

Lemma 2.1. (i) *The extension L/L_D is everywhere unramified.*
(ii) *The field $L_{S_L}(l)$ is the maximal pro-l extension of K unramified outside S_K.*

Proof. (i) Since $\mathrm{Gal}(L/L_D)$ is torsion-free, every inertia group of a prime of k_0, which is finite by the condition (I_1), can not be contained in $\mathrm{Gal}(L/L_D)$. Thus, (i) follows.
(ii) This follows immediately from (i), that $\mathrm{Gal}(L/K)$ is isomorphic to $\mathbb{Z}_l$, and the maximality of $L_{S_L}(l)$.

Remark. Let $\mathbb{F}_{p^f}$ be the residue field of $\mathfrak{p}$, p being a prime and $f \geq 1$. Let $\mathfrak{p}'$ be a prime of L lying above $\mathfrak{p}$. Then the residue field of $\mathfrak{p}'$ is the algebraic closure $\bar{\mathbb{F}}_{p^f}$ of $\mathbb{F}_{p^f}$. In fact, let $\tilde{F}$ be the residue field of $\mathfrak{p}'$, so that we have $\mathbb{F}_{p^f} \subset \tilde{F} \subset \bar{\mathbb{F}}_{p^f}$. By the condition (I_2), $\mathrm{Gal}(\tilde{F}/\mathbb{F}_{p^f})$ is isomorphic to $\hat{\mathbb{Z}}$. As $\mathrm{Gal}(\bar{\mathbb{F}}_{p^f}/\mathbb{F}_{p^f})$ is isomorphic to $\hat{\mathbb{Z}}$ and any quotient of $\hat{\mathbb{Z}}$ which is isomorphic to $\hat{\mathbb{Z}}$ is the trivial one, we have $\tilde{F} = \bar{\mathbb{F}}_{p^f}$.

(2-2) Let K be the field defined in (2-1). As in §1, for each algebraic number field k of finite degree contained in K, let f_{S_k} denote the localization map of the Galois cohomology group $\mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z})$. The aim of this section is to prove the following

Theorem 2.1. *Let k_0 be an algebraic number field of finite degree and L be an abelian extension of k_0 satisfying the conditions (I_1) and (I_2). Then we have $\varinjlim \mathrm{Ker} f_{S_k} = \{0\}$, where k runs over all algebraic number fields of finite degree such that $k_0 \subset k \subset K$.*

Let $(\mathcal{E})$ be the embedding problem defined in §1. By Theorem 1.1, in order to prove Theorem 2.1, it suffices to verify the statement (i) in Theorem 1.1. The verification will be done almost in the same way as that of Theorem 4.2 in [2]. We first reduce it to showing Proposition 2.1 below as follows.

First, consider the case that the exact sequence in $(\mathcal{E})$ splits. Then, composing φ with the splitting homomorphism, we obtain a weak solution of $(\mathcal{E})$. By the assumption on $(\mathcal{E})$, it factors through $G_{S_K}(l)$. Thus, in this case, the statement (i) in Theorem 1.1 holds.

In the following, we consider the case that the exact sequence in $(\mathcal{E})$ does not split. Assume that $(\mathcal{E})$ has a weak solution $\psi : G_K(l) \to E$. Then, as readily seen, ψ is a proper solution, i.e. ψ is surjective.

Let F and $\tilde{F}$ be the fields corresponding to the kernel of φ and that of ψ respectively. Thus $\mathrm{Gal}(F/K)$ and $\mathrm{Gal}(\tilde{F}/K)$ are isomorphic to H and E respectively. Let ζ_l be a primitive l-th root of unity. Then, as the extension $\tilde{F}(\zeta_l)/F(\zeta_l)$ is cyclic of degree l, there exists an element μ of $F(\zeta_l)^* \setminus (F(\zeta_l)^*)^l$ such that $\tilde{F}(\zeta_l) = F(\zeta_l, \sqrt[l]{\mu})$.

Let Δ denote the Galois group $\mathrm{Gal}(K(\zeta_l)/K)$, n be the order of Δ, and ρ be the generator of the cyclic group Δ such that $\zeta_l^\rho = \zeta_l^r$. Here r is an integer such that $1 - r^n = ls$ with $(l, s) = 1$. As in Reichardt[10] (see also Shafarevich[13]), we define an element T of the group algebra $\mathbb{Z}[\Delta]$ of Δ by

$$T = \rho^{n-1} + r\rho^{n-2} + \ldots + r^{n-2}\rho + r^{n-1}.$$

(If $\zeta_l \in K$, then we have $n = 1$ and ρ and T are the identity element.) Then, for an arbitrary element a of $K(\zeta_l)^*$ such that $\mu a^T \notin (K(\zeta_l)^*)^l$, $F(\zeta_l, \sqrt[l]{\mu a^T})$ is a Galois

extension of K and contains a Galois subextension $\tilde{F}'$ of K which corresponds to another solution of the embedding problem $(\mathcal{E})$. (Cf. e.g. [2, Prop.3.1].) Further, in order for the extension $\tilde{F}'/K$ to be unramified outside S_K, it is sufficient that the extension $F(\zeta_l, \sqrt[l]{\mu a^T})/F(\zeta_l)$ is unramified outside $S_{F(\zeta_l)}$, as F/K is unramified outside S_K.

Therefore, the verification of (i) in Theorem 1.1, and hence the proof of Theorem 2.1, is reduced to showing the following

Proposition 2.1. *There exists an element $a \in K(\zeta_l)^*$ such that $\mu a^T \notin (F(\zeta_l)^*)^l$ and that the extension $F(\zeta_l, \sqrt[l]{\mu a^T})/F(\zeta_l)$ is unramified outside l.*

(2-3) The proof of Proposition 2.1 is done in the same way as that of Proposition 4.2 in [2]. However, in this subsection, we shall indicate the proof in several steps, for we need the unramified version of Proposition 2.1 in (3-3).

First, consider the extension $\tilde{F}(\zeta_l) = \tilde{F}K(\zeta_l)$ of K. As it is a finite Galois extension, there exist algebraic number fields K_0 and $\tilde{F}_0$ of finite degree contained in K and $\tilde{F}$ respectively such that the Galis groups $\mathrm{Gal}(\tilde{F}_0(\zeta_l)/K_0)$ and $\mathrm{Gal}(\tilde{F}(\zeta_l)/K)$ are canonically isomorphic. We denote by F_0 the subextension $F \cap K_0$ of $\tilde{F}_0/K_0$. By taking K_0 sufficiently large, we may assume that the extension F_0/K_0 is unramified outside S_{K_0} and that $\mu \in F_0(\zeta_l)$. We identify the Galois groups $\mathrm{Gal}(F_0(\zeta_l, \sqrt[l]{\mu})/K_0(\zeta_l))$ and $\mathrm{Gal}(F_0(\zeta_l)/K_0(\zeta_l))$ with E and H respectively.

Step 1. As $F_0(\zeta_l, \sqrt[l]{\mu})/K_0(\zeta_l)$ is a central extension of $F_0(\zeta_l)/K_0(\zeta_l)$, we have $\mu^\sigma \equiv \mu \bmod (F_0(\zeta_l)^*)^l$ for any $\sigma \in H$. (Cf. e.g. [2, Lemma 3.1].) For the principal ideal (μ) of $F_0(\zeta_l)$, it follows from this that there exist an ideal $\mathfrak{m}$ of $F_0(\zeta_l)$ prime to l which is H-invariant, an ideal $\mathfrak{b}$ of $F_0(\zeta_l)$ which is a product of primes lying above l, and an ideal $\mathfrak{a}$ of $F_0(\zeta_l)$ such that $(\mu) = \mathfrak{m}\mathfrak{b}\mathfrak{a}^l$. As the extension $F_0(\zeta_l)/K_0(\zeta_l)$ is unramified outside l, $\mathfrak{m}$ is an ideal of $K_0(\zeta_l)$.

Step 2. Further, there exist an ideal $\mathfrak{n}$ of $K_0(\zeta_l)$, an ideal $\mathfrak{a}_1$ of $F_0(\zeta_l)$, and an ideal $\mathfrak{b}$ of $F_0(\zeta_l)$ which is a product of primes lying above l such that $(\mu) = \mathfrak{n}^T\mathfrak{b}\mathfrak{a}_1^l$.

This is verified completely in the same way of the proof of Lemma 4.3 in [2].

Step 3. Let us consider the ideal class group of $K_0(\zeta_l)$ and let c_0 be the ideal class to which $\mathfrak{n}$ belongs. By the density theorem and the condition (I_1) of L/k_0, there exists a prime ideal $\mathfrak{q}$ in c_0 satisfying the following conditions :

(a) $\mathfrak{q}$ is of absolute degree one, is unramified over $\mathbb{Q}$, and is prime to 2.
(b) The order of the inertia group of the prime $\mathfrak{q} \cap K_0$ for the extension L/K_0 is $q-1$, where $(q) = \mathfrak{q} \cap \mathbb{Z}$.

Then we have $\mathfrak{q} = \mathfrak{n}(a)$ with some element a of $K_0(\zeta_l)^*$. Using this a, we consider the element $\mu a^T \in F_0(\zeta_l)^*$ and the extension $F_0(\zeta_l, \sqrt[l]{\mu a^T})$ of $F_0(\zeta_l)$.

Lemma 2.2. *The extension $F_0(\zeta_l, \sqrt[l]{\mu a^T})/F_0(\zeta_l)$ has the following properties :*

(i) *it is of degree l.*

(ii) *it is unramified outside those primes of $F_0(\zeta_l)$ lying above $l, \mathfrak{q}, \mathfrak{q}^\rho, ..., \mathfrak{q}^{\rho^{n-1}}$, where ρ is a generator of* $\mathrm{Gal}(K_0(\zeta_l)/K_0)$.

(iii) $F_0(\zeta_l, \sqrt[l]{\mu a^T}) \cap F(\zeta_l) = F_0(\zeta_l)$.

Proof. First, the principal ideal (μa^T) of $F_0(\zeta_l)$ is decomposed as $(\mu a^T) = \mathfrak{q}^T \mathfrak{b}\mathfrak{a}_1^l$, where

$$\mathfrak{q}^T = \mathfrak{q}^{\rho^{n-1}} (\mathfrak{q}^{\rho^{n-2}})^r ... (\mathfrak{q}^{\rho})^{r^{n-2}} \mathfrak{q}^{r^{n-1}}.$$

From this (ii) follows. By the condition (a) of $\mathfrak{q}$, $\mathfrak{q}$ is prime to l and $\mathfrak{q}^{\rho^{n-1}}, \mathfrak{q}^{\rho^{n-2}}, ..., \mathfrak{q}$ are distinct prime ideals of $K_0(\zeta_l)$. As $F_0(\zeta_l)/K_0(\zeta_l)$ is unramified outside l, it follows from these that $\mu a^T \notin (F_0(\zeta_l)^*)^l$, i.e. (i) follows.

We shall verify (iii). Assume that (iii) does not hold. Then $F_0(\zeta_l, \sqrt[l]{\mu a^T})$ is contained in $F(\zeta_l)$. As $\mathrm{Gal}(F(\zeta_l)/K_0(\zeta_l))$ is the direct product of $\mathrm{Gal}(F(\zeta_l)/K(\zeta_l))$ and $\mathrm{Gal}(F(\zeta_l)/F_0(\zeta_l))$, it follows that $\mathrm{Gal}(F_0(\zeta_l, \sqrt[l]{\mu a^T})/K_0(\zeta_l))$ is isomorphic to $H \times \mathbb{Z}/l\mathbb{Z}$, which contradicts with the assumption that the exact sequence in $(\mathcal{E})$ does not split. Thus (iii) follows.

Step 4. Let $\mathfrak{q}_0 = \mathfrak{q} \cap K_0$. By the condition (a) of $\mathfrak{q}$, the primes of $K_0(\zeta_l)$ lying above $\mathfrak{q}_0$ are $\mathfrak{q}, \mathfrak{q}^{\rho}, ..., \mathfrak{q}^{\rho^{n-1}}$. Further, by the condition (b) of $\mathfrak{q}$ and as L/K is unramified, the ramification index of $\mathfrak{q}_0$ in K is $q-1$.

Lemma 2.3. *There exists a finite subextension K_0' of K/K_0 such that the ramification index of $\mathfrak{q}_0$ in K_0' is $q-1$ and that every prime ideal of K_0' lying above $\mathfrak{q}_0$ is unramified in K.*

Proof. Let K_I be the inertia field of $\mathfrak{q}_0$ in the abelian extension K/K_0. By the remark before the lemma, K/K_I is a finite extension of degree $q-1$. Hence there exists a finite subextension K_0' of K/K_0 such that $K = K_0' K_I$. Then every prime ideal of K_0' lying above $\mathfrak{q}_0$ is unramified in K, and hence the ramification index of $\mathfrak{q}_0$ in K_0' is $q-1$.

Let $F_0' = F_0 K_0'$, K_0' being a finite subextension of K/K_0 satisfying the condition in Lemma 2.3. Consider the extension $F_0'(\zeta_l, \sqrt[l]{\mu a^T})/F_0'(\zeta_l)$, which is, by Lemma 2.2, of degree l. Finally, we have the following lemma, and this completes the proof of Proposition 2.1.

Lemma 2.4. *The extension $F_0'(\zeta_l, \sqrt[l]{\mu a^T})/F_0'(\zeta_l)$ is unramified outside l.*

Proof. Let $\tilde{\mathfrak{q}}$ be any prime ideal of $F_0(\zeta_l)$ lying above $\mathfrak{q}$. Then $\tilde{\mathfrak{q}}$ is totally and tamely ramified in $F_0(\zeta_l, \sqrt[l]{\mu a^T})$ with ramification index $e_1 = l$. On the other hand, by Lemma 2.3, $\tilde{\mathfrak{q}}$ is ramified in $F_0'(\zeta_l)$ with ramification index $e_2 = q-1$. By the condition (a) of $\mathfrak{q}$, q splits completely in the subfield $\mathbb{Q}(\zeta_l)$ of $K_0(\zeta_l)$. Hence $q \equiv 1 \bmod l$, i.e. e_1 divides e_2. Therefore, by Abhyanker's lemma (cf. e.g. Cornell[5]), any prime ideal of $F_0'(\zeta_l)$ lying above $\tilde{\mathfrak{q}}$ is unramified in $F_0'(\zeta_l, \sqrt[l]{\mu a^T})$. Same arguments can also be applied to any prime ideal of $F_0(\zeta_l)$ lying above $\mathfrak{q}^{\rho}, ..., \mathfrak{q}^{\rho^{n-1}}$. Hence the proof of Lemma 2.4 is completed.

3. Some free pro-l Galois groups

(3-1) Let k_0 be an algebraic number field of finite degree and l be a fixed prime. Let L and K be the abelian extensions of k_0 defined in (2-1) and $L_{S_L}(l)$ be the maximal pro-l extension of L unramified outside S_L. By Lemma 2.1 (ii), the extension $L_{S_L}(l)/K$ coincides with $K_{S_K}(l)/K$, the maximal pro-l extension of K unramified outside S_K, and we denote its Galois group by $G_{S_K}(l)$.

For the extension L/k_0, we shall add the following condition :

(II_l) For any finite subextension k of L/k_0 and for any finite l-place v of k, the v-completion k_v does not contain a primitive l-th root of unity.

Then we can determine the structure of the Galois group $G_{S_K}(l)$. Namely we have the following

Theorem 3.1. *Let l be an odd prime. Let L be an abelian extension of k_0 satisfying the conditions* (I_1), (I_2) *in (2-1) and the condition* (II_l). *Then the Galois group $G_{S_K}(l)$ is a free pro-l group.*

Proof. Let k be a finite subextension of L/k_0. We have an exact sequence

$$0 \to \mathrm{Ker} f_{S_k} \to \mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z}) \xrightarrow{f_{S_k}} \bigoplus_{v \in S_k} \mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z}),$$

where f_{S_k} denotes, as before, the localization map. By the local Tate duality ([8, (7.2.6)], Serre[12, Ch II 5.2]), $\mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z})$ is the dual of $\mathrm{H}^0(G_{k_v}; \mu_l)$, μ_l being the group of l-th roots of unity. By the condition (II_l), we have $\mathrm{H}^0(G_{k_v}; \mu_l) = \{0\}$ and hence $\mathrm{H}^2(G_{k_v}; \mathbb{Z}/l\mathbb{Z}) = \{0\}$ for all $v \in S_k$. By Theorem 2.1 we have $\varinjlim \mathrm{Ker} f_{S_k} = \{0\}$. Hence $\varinjlim \mathrm{H}^2(G_{S_k}; \mathbb{Z}/l\mathbb{Z}) = \{0\}$, i.e. $\mathrm{H}^2(G_{S_K}; \mathbb{Z}/l\mathbb{Z}) = \{0\}$. As $\mathrm{H}^2(G_{S_K}(l); \mathbb{Z}/l\mathbb{Z})$ is isomorphic to $\mathrm{H}^2(G_{S_K}; \mathbb{Z}/l\mathbb{Z})$ ([9]), we have $\mathrm{H}^2(G_{S_K}(l); \mathbb{Z}/l\mathbb{Z}) = \{0\}$. Hence $G_{S_K}(l)$ is a free pro-l group ([8, (3.5.17)], [12, Ch I 4.2]).

Let L_D be the field defined in (2-1). By the maximality of $L_{S_L}(l)$, it is a Galois extension of L_D.

Corollary. *Let the assumptions be the same as in Theorem 3.1. Then the Galois group* $\mathrm{Gal}(L_{S_L}(l)/L_D)$ *is a projective profinite group.*

Proof. It suffices to show that for every prime q, the q-Sylow subgroups of $\mathrm{Gal}(L_{S_L}(l)/L_D)$ are free pro-q groups ([12, Ch I 5.9]). As $\mathrm{Gal}(L/L_D)$ is isomorphic to $\hat{\mathbb{Z}} = \prod_q \mathbb{Z}_q$, this follows immediately from Theorem 3.1.

(3-2) Let $L_{ur}(l)$ be the maximal unramified pro-l extension of L. It follows from Lemma 2.1 (i) that $L_{ur}(l)$ is also the maximal unramified pro-l extension of K. For the extension K/k_0, let us further add the following condition :

(III_l) For any l-place of K, its residue field is the algebraic closure of the prime field $\mathbb{F}_l$.

Then we can determine the structure of the Galois group $\mathrm{Gal}(L_{ur}(l)/K)$. Namely we have the following

Theorem 3.2. *Let l be an odd prime. Let L be an abelian extension of k_0 satisfying the conditions* (I_1), (I_2) *in (2-1), the condition* (II_l) *in (3-1) and the condition* (III_l). *Then the Galois group* $\mathrm{Gal}(L_{ur}(l)/K)$ *is a free pro-l group.*

Similarly to the case of $L_{S_L}(l)$, $L_{ur}(l)$ is also a Galois extension of L_D and we have the following

Corollary. *Let the assumptions be the same as in Theorem 3.2. Then the Galois group* $\mathrm{Gal}(L_{ur}(l)/L_D)$ *is a projective profinite group.*

(3-3) In the rest of this section, we shall give the proof of Theorem 3.2.

Let us consider the following embedding problem for the Galois group $\mathrm{Gal}(L_{ur}(l)/K)$:

$$(P) \qquad \begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(L_{ur}(l)/K) & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \longrightarrow & \mathbb{Z}/l\mathbb{Z} & \longrightarrow & E & \xrightarrow{\alpha} & H & \longrightarrow & 1 \end{array}$$

Here, the horizontal sequence is an exact sequence of finite l-groups and φ is a surjective homomorphism. As explained in [1, (2-3)], to prove Theorem 3.2, it suffices to show that the embedding problem (P) has always a solution in the case that the exact sequence in (P) is non-split.

Assume that the exact sequence in (P) is non-split. Let $K_{S_K}(l)$ be the maximal pro-l extension of K unramified outside S_K and $\tilde{\varphi} : \mathrm{Gal}(K_{S_K}(l)/K) \to H$ be the composite of φ and the projection $\mathrm{Gal}(K_{S_K}(l)/K) \to \mathrm{Gal}(L_{ur}(l)/K)$. Consider the embedding problem $(\tilde{P})$ obtained from (P) by replacing $\mathrm{Gal}(L_{ur}(l)/K)$ and φ with $\mathrm{Gal}(K_{S_K}(l)/K)$ and $\tilde{\varphi}$, respectively. By Theorem 3.1, $\mathrm{Gal}(K_{S_K}(l)/K)$ is a free pro-l group and hence the embedding problem $(\tilde{P})$ has a solution, which we denote by $\tilde{\psi}$.

Let F and $\tilde{F}$ be the fields corresponding to the kernel of $\tilde{\varphi}$ and $\tilde{\psi}$ respectively. Note that F is also the field corresponding to the kernel of φ. There exists an element $\mu \in F(\zeta_l)^* \setminus (F(\zeta_l)^*)^l$ such that $\tilde{F}(\zeta_l) = F(\zeta_l, \sqrt[l]{\mu})$.

As explained in (2-2), for an arbitrary element a of $K(\zeta_l)^*$ such that $\mu a^T \notin (K(\zeta_l)^*)^l$, $F(\zeta_l, \sqrt[l]{\mu a^T})$ is a Galois extension of K and contains a Galois subextension $\tilde{F}'$ of K which corresponds to another solution of the embedding problem $(\tilde{P})$. Here, T is the element of the group algebra $\mathbb{Z}[\Delta]$, $\Delta = \mathrm{Gal}(K(\zeta_l)/K)$, defined in (2-2). In order for the extension $\tilde{F}'/K$ to be unramified, it is sufficient that the extension $F(\zeta_l, \sqrt[l]{\mu a^T})/F(\zeta_l)$ is unramified. This is because F/K is unramified, $K(\zeta_l)/K$ is unramified ouside S_K and tamely ramified at l, and $l \neq 2$. Therefore, showing that the embedding problem (P) has a solution, and hence the proof of Theorem 3.2, is reduced to proving the following

Proposition 3.1. *There exists an element $a \in K(\zeta_l)^*$ such that $\mu a^T \notin (F(\zeta_l)^*)^l$ and that the extension $F(\zeta_l, \sqrt[l]{\mu a^T})/F(\zeta_l)$ is unramified.*

(3-4) Proposition 3.1 is an unramified version of Proposition 2.1. The proof requires, in addition to that of Proposition 2.1, eliminating the ramifications above l. This part

is given as the following Proposition 3.2. We owe its proof to that of Theorem 1 in Uchida[14]. For the sake of completeness, we shall give details.

First, as F/K is a finite unramified Galois extension, there exist a finite subextension K_0 of $K/\mathbb{Q}$ and a finite unramified Galois extension F_0/K_0 such that $F_0 \cap K = K_0$, $F_0K = F$ and $\mu \in F_0(\zeta_l)$. Further, by the condition (III_l), taking K_0 sufficiently large, we may assume that the following condition is satisfied :

$(\mathrm{SC})_{K_0}$ every l-place of K_0 splits completely in F_0.

Then we have the following

Proposition 3.2. *There exists an element $\alpha \in K_0(\zeta_l)^*$ such that $\mu/\alpha^T \notin (F_0(\zeta_l)^*)^l$ and that every l-place of $F_0(\zeta_l)$ splits completely in the extension $F_0(\zeta_l, \sqrt[l]{\mu/\alpha^T})$.*

We first note that, as $F_0(\zeta_l, \sqrt[l]{\mu})/F_0(\zeta_l)/K_0(\zeta_l)$ is a central extension, there exist elements ν, ξ of $F_0(\zeta_l)^*$ such that $\mu = \nu^T\xi^l$. (Cf. e.g. [2, Lem. 3.2].)

To prove Proposition 3.2, we need several lemmas. Let $\mathfrak{l}_1, ..., \mathfrak{l}_r$ be all primes of $K_0(\zeta_l)$ lying above l.

Lemma 3.1. *For each i, $1 \leq i \leq r$, there exists a prime $\mathfrak{L}_i$ of $F_0(\zeta_l)$ lying above $\mathfrak{l}_i$ such that the set $\{\mathfrak{L}_1, ..., \mathfrak{L}_r\}$ is Δ-invariant, Δ being identified with* $\mathrm{Gal}(K_0(\zeta_l)/K_0)$ ($\simeq \mathrm{Gal}(F_0(\zeta_l)/F_0)$).

Proof. The group Δ acts on the set $\{\mathfrak{l}_1, ..., \mathfrak{l}_r\}$. By decomposing it into orbits, it suffices to prove the lemma assuming that the action of Δ is transitive. As Δ is a cyclic group generated by ρ, we may also assume that $\mathfrak{l}_1^\rho = \mathfrak{l}_2, \mathfrak{l}_2^\rho = \mathfrak{l}_3, ..., \mathfrak{l}_r^\rho = \mathfrak{l}_1$. Let $\mathfrak{L}_1$ be a prime of $F_0(\zeta_l)$ lying above $\mathfrak{l}_1$ and set $\mathfrak{L}_2 = \mathfrak{L}_1^\rho, \mathfrak{L}_3 = \mathfrak{L}_2^\rho, ..., \mathfrak{L}_r = \mathfrak{L}_{r-1}^\rho$. Then $\mathfrak{L}_i$ is lying above $\mathfrak{l}_i$, $1 \leq i \leq r$, and the set $\{\mathfrak{L}_1, ..., \mathfrak{L}_r\}$ is Δ-invariant.

Let $\mathfrak{L}_1, ..., \mathfrak{L}_r$ be primes of $F_0(\zeta_l)$ satisfying the condition in Lemma 3.1.

Lemma 3.2. *There exists an element $\alpha \in K_0(\zeta_l)^*$ such that α/ν is an l-th power in the $\mathfrak{L}_i$-adic completion $F_0(\zeta_l)_{\mathfrak{L}_i}$ for $1 \leq i \leq r$.*

Proof. By the condition $(\mathrm{SC})_{K_0}$, the relative degree of $\mathfrak{L}_i$ in the extension $F_0(\zeta_l)/K_0(\zeta_l)$ is 1. Thus, for any positive number ε and for each $i, 1 \leq i \leq r$, there exists an element $a_i \in K_0(\zeta_l)$ such that $|\nu - a_i|_i < \varepsilon$, $|\ |_i$ being the $\mathfrak{L}_i$-adic absolute value. By the approximation theorem, there exists an element $\alpha \in K_0(\zeta_l)$ such that $|\alpha - a_i|_i < \varepsilon$ for $1 \leq i \leq r$. As $|\nu - \alpha|_i < |\nu - a_i|_i + |\alpha - a_i|_i < 2\varepsilon$, we have, for sufficiently small $\varepsilon > 0$, $\alpha \neq 0$. Furthere, as $|\alpha/\nu - 1|_i \leq 2\varepsilon/|\nu|_i \leq 2\varepsilon/A, A = Min\{|\nu|_i\}$, for sufficiently small $\varepsilon > 0$, α/ν has the property stated in Lemma 3.2.

Lemma 3.3. *Let $\alpha \in K_0(\zeta_l)^*$ be as in Lemma 3.2. Then, for $1 \leq i \leq r$, $(\nu/\alpha)^T$ is an l-th power in $F_0(\zeta_l)_{\mathfrak{L}_i}$.*

Proof. As $\{\mathfrak{L}_1, ..., \mathfrak{L}_r\}$ is Δ-invariant, $(\nu/\alpha)^\rho$ is an l-th power in $F_0(\zeta_l)_{\mathfrak{L}_i}$. The lemma follows immediately from this.

Lemma 3.4. *Let $\alpha \in K_0(\zeta_l)^*$ be as in Lemma 3.2. Then, for $1 \leq i \leq r$ and for every $\sigma \in \mathrm{Gal}(F_0(\zeta_l)/K_0(\zeta_l))$, ν^T/α^T is an l-th power in $F_0(\zeta_l)_{\mathfrak{L}_i^\sigma}$.*

Proof. As $\alpha \in K_0(\zeta_l)$ and T commutes with σ, we have

$$(\nu^T/\alpha^T)^\sigma = \nu^{T(\sigma-1)}\nu^T/\alpha^T = (\mu\xi^{-l})^{\sigma-1}\nu^T/\alpha^T = \mu^{\sigma-1}(\xi^{\sigma-1})^{-l}\nu^T/\alpha^T.$$

As $\mu^{\sigma-1} \in (F_0(\zeta_l)^*)^l$, we have $(\nu^T/\alpha^T)^\sigma(\nu^T/\alpha^T)^{-1} \in (F_0(\zeta_l)^*)^l$. Hence, by Lemma 3.3, $(\nu^T/\alpha^T)^\sigma$ is an l-th power in $F_0(\zeta_l)_{\mathfrak{L}_i}$ and the lemma follows from this.

Proof of Proposition 3.2. Let α be as in Lemma 3.2. We first verify that $\mu/\alpha^T \notin (F_0(\zeta_l)^*)^l$. Assume that $\mu/\alpha^T \in (F_0(\zeta_l)^*)^l$ so that there exists an element $\mu_0 \in (F_0(\zeta_l)^*)^l$ such that $\mu = \alpha^T\mu_0^l$. Then we have $F_0(\zeta_l, \sqrt[l]{\mu}) = F_0(\zeta_l, \sqrt[l]{\alpha^T})$. As $\alpha^T \in K_0(\zeta_l)^*$, $\mathrm{Gal}(F_0(\zeta_l, \sqrt[l]{\mu})/K_0(\zeta_l))$ is isomorphic to $H \times \mathbb{Z}/l\mathbb{Z}$. This contradicts with the assumption that the exact sequence in (P) is non-split. Hence we have $\mu/\alpha^T \notin (F_0(\zeta_l)^*)^l$. As $\mu/\alpha^T = (\nu^T/\alpha^T)\xi^l$, we have $F_0(\zeta_l, \sqrt[l]{\mu/\alpha^T}) = F_0(\zeta_l, \sqrt[l]{\nu^T/\alpha^T})$. Since $\{\mathfrak{L}_i^\sigma\}_{i,\sigma}$ are all l-places of $F_0(\zeta_l)$, Proposition 3.2 follows from Lemma 3.4.

(3-5) Now we shall prove Proposition 3.1. Let $\alpha \in K_0(\zeta_l)$ be as in Proposition 3.2 and replace $F_0(\zeta_l, \sqrt[l]{\mu})$ with $F_0(\zeta_l, \sqrt[l]{\mu/\alpha^T})$. Denoting μ/α^T newly by μ, we may assume that, for every l-place of $F_0(\zeta_l)$, μ is locally an l-th power. The rest of the proof proceeds parallel to that of Proposition 2.1.

Step 1. Similarly to the Step 1 of the proof of Proposition 2.1, we first have $\mu^\sigma \equiv \mu \bmod (F_0(\zeta_l)^*)^l$ for any $\sigma \in H$. It follows from this that there exist an ideal $\mathfrak{m}$ of $F_0(\zeta_l)$ which is H-invariant and an ideal $\mathfrak{a}$ of $F_0(\zeta_l)$ such that $(\mu) = \mathfrak{m}\mathfrak{a}^l$. As the extension $F_0(\zeta_l)/K_0(\zeta_l)$ is everywhere unramified, $\mathfrak{m}$ is an ideal of $K_0(\zeta_l)$.

Further, we may assume that the ideal $\mathfrak{m}$ is prime to l. Indeed, as any l-place $\tilde{\mathfrak{l}}$ of $F_0(\zeta_l)$ is unramified in $F_0(\zeta_l, \sqrt[l]{\mu})$, the exponent of $\tilde{\mathfrak{l}}$ in (μ), and hence that in $\mathfrak{m}$, is a multiple of l. Thus, convolving the $\tilde{\mathfrak{l}}$-component of $\mathfrak{m}$ in $\mathfrak{a}^l$, we may assume that $\mathfrak{m}$ is prime to l.

Step 2. We claim that there exist an ideal $\mathfrak{n}$ of $K_0(\zeta_l)$ prime to l and an ideal $\mathfrak{a}_1$ of $F_0(\zeta_l)$ such that $(\mu) = \mathfrak{n}^T\mathfrak{a}_1^l$, T being an element of $\mathbb{Z}[\Delta]$ defined in (2-2).

Though this is verified in the same way of the proof of [2, Lemma 4.3], to clarify that $\mathfrak{n}$ can be taken to be prime to l, we shall explain details.

First, we have $\mu^{\rho-r} \in (F_0(\zeta_l)^*)^l$. This follows from the fact that the extension $F_0(\zeta_l, \sqrt[l]{\mu})/F_0$ is abelian. Then, as $(\mu)^{\rho-r} = \mathfrak{m}^{\rho-r}(\mathfrak{a}^{\rho-r})^l$, $\mathfrak{m}^{\rho-r}$ is an l-th power of an ideal of $F_0(\zeta_l)$. As $F_0(\zeta_l)/K_0(\zeta_l)$ is an unramified extension, there exist an ideal $\mathfrak{m}_1$ of $K_0(\zeta_l)$ such that $\mathfrak{m}^{\rho-r} = \mathfrak{m}_1^l$. By using that $(\rho-r)T = 1 - r^n = ls$, it follows from this that $\mathfrak{m}^s = \mathfrak{m}_1^T$. As $\mathfrak{m}$ is prime to l, so is $\mathfrak{m}_1$. As $(s,l) = 1$, we can take integers x, y such that $sx + ly = 1$. Then we have $\mathfrak{m} = (\mathfrak{m}_1^x)^T(\mathfrak{m}^y)^l$. Letting $\mathfrak{n} = \mathfrak{m}_1^x$, $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{m}^y$, we see that $\mathfrak{n}$ is prime to l and the claim is settled.

Step 3. Instead of the absolute ideal class group, we consider the ray class group modulo l^2 of $K_0(\zeta_l)$. Let c_0 be its ideal class to which $\mathfrak{n}$ belongs. There exists a prime ideal $\mathfrak{q}$ in c_0 satisfying the same conditions (a), (b) in the proof of Proposition 2.1. We have

$\mathfrak{q} = \mathfrak{n}(\beta)$ with some element β of $K_0(\zeta_l)^*$ such that $\beta \equiv 1 \bmod l^2$. Using this β, we consider the extension $F_0(\zeta_l, \sqrt[l]{\mu\beta^T})$ of $F_0(\zeta_l)$. This extension has the same properties (i), (ii), (iii) in Lemma 2.2, the proof being the same as that of Lemma 2.2.

Further, it has the following property :

$(\mathrm{SC})_{F_0(\zeta_l)}$ every l-place of $F_0(\zeta_l)$ splits completely in $F_0(\zeta_l, \sqrt[l]{\mu\beta^T})$.

In fact, let $\mathfrak{L}$ be any prime ideal of $F_0(\zeta_l)$ lying above l with absolute ramification index e. As $\beta \equiv 1 \bmod l^2$, we have $\beta^T \equiv 1 \bmod l^2$, hence $\beta^T \equiv 1 \bmod \mathfrak{L}^{2e}$. Thus, as $l > 2$, β^T is an l-th power in $F_0(\zeta_l)_{\mathfrak{L}}$. (Cf. e.g. Serre[11, XIV Prop. 9].) As μ is also an l-th power in $F_0(\zeta_l)_{\mathfrak{L}}$, the property $(\mathrm{SC})_{F_0(\zeta_l)}$ follows.

Step 4. Let $\mathfrak{q}_0 = \mathfrak{q} \cap K_0$ and K_0' be a finite subextension of K/K_0 satisfying the condition in Lemma 2.3. Let $F_0' = F_0K_0'$ and consider the extension $F_0'(\zeta_l, \sqrt[l]{\mu\beta^T})/F_0'(\zeta_l)$, which is of degree l. Finally we have the following lemma, and this completes the proof of Proposition 3.1.

Lemma 3.5. *The extension $F_0'(\zeta_l, \sqrt[l]{\mu\beta^T})/F_0'(\zeta_l)$ is everywhere unramified.*

Proof. The proof that the extension is unramified outside l is the same of that of Lemma 2.4. By the property $(\mathrm{SC})_{F_0(\zeta_l)}$ in Step 3, the extension is also unramified at every l-place of $F_0'(\zeta_l)$.

4. Pro-l abelian Galois groups

(4-1) Let k_0 be an algebraic number field of finite degree and l be a fixed prime. Let L be an abelian extension of k_0 satisfying the conditions (I_1) and (I_2) in (1-2) and L_D be the decomposition field of $\mathfrak{p}$ in L/k_0. Let $D = \mathrm{Gal}(L/L_D)$ and $\mathcal{A}_l$ be the completed group algebra of D over $\mathbb{Z}_l$.

Let M be a pro-l abelian extension of L such that M/L_D is also a Galois extension. Then D acts on the Galois group $\mathrm{Gal}(M/L)$ in the obvious manner. As $\mathrm{Gal}(M/L)$ is naturally a $\mathbb{Z}_l$-module, this makes $\mathrm{Gal}(M/L)$ into an $\mathcal{A}_l$-module. In this section, we shall investigate the structures as $\mathcal{A}_l$-modules of various pro-l abelian Galois groups over L.

For each $n \geq 1$, let C_n denote the unique quotient of D such that C_n is cyclic of order n. Let $\mathbb{F}_l[C_n]$ denote the group algebra of C_n over the prime field $\mathbb{F}_l$ of characteristic l. Via the projection $D \to C_n$, $\mathbb{F}_l[C_n]$ is naturally regarded as a D-module, and hence as an $\mathcal{A}_l$-module. We denote this module by $E_n(l)$.

We shall first prove the following

Theorem 4.1. *Let l be an odd prime. Let L be an abelian extension of k_0 satisfying the conditions (I_1) and (I_2) such that $[L(\zeta_l) : L] = l - 1$. Let m and n be any positive integers. Then there exists a finite unramified abelian extension M of L which is a Galois extension of L_D such that the Galois group $\mathrm{Gal}(M/L)$ is isomorphic to $E_n(l)^{\oplus m}$ as $\mathcal{A}_l$-modules.*

(4-2) In this subsection we shall give the proof of Theorem 4.1. The proof proceeds similarly to that of Proposition 5.1 in [2].

Let L_n be the unique subextension of L/L_D such that $[L_n : L_D] = n$ so that we have $C_n = \mathrm{Gal}(L_n/L_D)$. Let K_0'/k_0' be a finite Galois extension of algebraic number fields of finite degree such that $k_0 \subset k_0' \subset K_0', L_D \cap K_0' = k_0'$, and $L_D K_0' = L_n$. As L_n/L_D is unramified, we may assume that K_0'/k_0' is unramified. We may also assume that k_0' is a proper extension of k_0.

Let us consider the extension $K_0'(\zeta_l)/k_0'(\zeta_l)$. As $[L(\zeta_l) : L] = l-1$, $\mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$ is canonically isomorphic to $\mathrm{Gal}(K_0'/k_0')$, and hence to C_n ; $\mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l)) \simeq \mathrm{Gal}(K_0'/k_0') \simeq C_n$.

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

Let $C_\mathfrak{m}$ be the ray class group of $K_0'(\zeta_l)$ modulo $\mathfrak{m}$. By the density theorem and the condition (I_1) of L, there exist principal prime ideals $\mathfrak{Q}_1, ..., \mathfrak{Q}_m$, $\mathfrak{Q}_i = (\alpha_i), 1 \leq i \leq m$, in the principal class of $C_\mathfrak{m}$ satisfying the following conditions :

(a) Every $\mathfrak{Q}_i$ is of absolute degree one, is unramified over $\mathbb{Q}$, and is prime to 2. Further, let $\mathfrak{Q}_i \cap \mathbb{Q} = (q_i)$. Then $q_1, ..., q_m$ are distinct primes.
(b) The order of the inertia group of the prime $\mathfrak{Q}_i \cap k_0$ for the extension L/k_0 is $q_i - 1$.

By the assumption on l, the Galois group $\mathrm{Gal}(K_0'(\zeta_l)/K_0')$ is cyclic of order $l-1$. Let ρ be its generator such that $\zeta_l^\rho = \zeta_l^r$ with $r^{l-1} = 1 + ls, (l, s) = 1$, and as in (2-2), let

$$T = \rho^{l-2} + r\rho^{l-3} + ... + r^{l-3}\rho + r^{l-2},$$

which is an element of the group algebra $\mathbb{Z}[\mathrm{Gal}(K_0'(\zeta_l)/K_0')]$.

For each $i, 1 \leq i \leq m$, and $\sigma \in \mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$, consider the element $\alpha_i^{T\sigma}$ of $K_0'(\zeta_l)$. The principal ideal $(\alpha_i^{T\sigma}) = \mathfrak{Q}_i^{T\sigma}$ is decomposed as

$$(*)_{i,\sigma} \qquad (\alpha_i^{T\sigma}) = \mathfrak{Q}_i^{\sigma\rho^{l-2}} (\mathfrak{Q}_i^{\sigma\rho^{l-3}})^r \cdots (\mathfrak{Q}_i^\sigma)^{r^{l-2}}.$$

Let $F_{i,\sigma}$ be the field obtained by adjoining to $K_0'(\zeta_l)$ an l-th root of $\alpha_i^{T\sigma}$; $F_{i,\sigma} = K_0'(\zeta_l, \sqrt[l]{\alpha_i^{T\sigma}})$. Let $H_{i,\sigma}$ be the subgroup of $K_0'(\zeta_l)^*/(K_0'(\zeta_l)^*)^l$ generated by the class of $\alpha_i^{T\sigma}$.

Lemma 4.1. *The extension $F_{i,\sigma}/K_0'(\zeta_l)$ has the following properties :*
(i) *$F_{i,\sigma}/K_0'(\zeta_l)$ is of degree l.*
(ii) *$F_{i,\sigma}/K_0'(\zeta_l)$ is unramified outside $\mathfrak{Q}_i^\sigma, \mathfrak{Q}_i^{\sigma\rho}, ..., \mathfrak{Q}_i^{\sigma\rho^{l-2}}$ and $\mathfrak{Q}_i^\sigma, \mathfrak{Q}_i^{\sigma\rho}, ..., \mathfrak{Q}_i^{\sigma\rho^{l-2}}$ are totally ramified in $F_{i,\sigma}$. The primes $\mathfrak{l}_1, ..., \mathfrak{l}_g$ split completely in $F_{i,\sigma}$.*
(iii) *$F_{i,\sigma}/K_0'$ is an abelian extension.*

Proof. We first note that, by the condition (a) of $\mathfrak{Q}_i$, the righthand side of $(*)_{i,\sigma}$ is the product of powers of mutually distinct primes of $K_0'(\zeta_l)$. As $(r, l) = 1$, the property (i) and the first half of (ii) follow immediately from this.

As $\alpha_i \equiv 1 \bmod \mathfrak{m}$ and $\mathfrak{m}$ is invariant by the action of $\mathrm{Gal}(K_0'(\zeta_l)/k_0')$, we have $\alpha_i^{T\sigma} \equiv 1 \bmod \mathfrak{m}$. Hence $\mathfrak{l}_1, ..., \mathfrak{l}_g$ split completely in $F_{i,\sigma}$.

For the property (iii), we observe that, as $(\rho - r)T = \rho^{l-1} - r^{l-1} = -ls$,

$$(\alpha_i^{T\sigma})^\rho \equiv (\alpha_i^{T\sigma})^r \bmod (K_0'(\zeta_l)^*)^l.$$

This shows first that $H_{i,\sigma}$ is invariant by the action of $\mathrm{Gal}(K_0'(\zeta_l)/K_0')$. Hence $F_{i,\sigma}$ is a Galois extension of K_0'. It also shows that $\mathrm{Gal}(K_0'(\zeta_l)/K_0')$ acts on $H_{i,\sigma}$ via the cyclotomic character. From this, as the degrees $[F_{i,\sigma} : K_0'(\zeta_l)]$ and $[K_0'(\zeta_l) : K_0']$ are coprime, it follows that $F_{i,\sigma}$ is an abelian extension of K_0'. (Cf. e.g. [2, Lemma 3.1].)

Let F_i be the composite of $F_{i,\sigma}$ for all $\sigma \in \mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$. Then F_i is a Galois extension of $k_0'(\zeta_l)$ and is an abelian extension of K_0' by Lemma 4.1 (iii). Hence F_i is a Galois extension of k_0'. The Galois group $\mathrm{Gal}(F_i/K_0')$ is naturally a $\mathrm{Gal}(K_0'/k_0')$-module and the Galois group $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ is naturally a $\mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$-module. Thus these are both C_n-modules. As the degree $[K_0'(\zeta_l) : K_0']$ is $l-1$, there exists a unique subextension F_i' of F_i/K_0' such that $[F_i : F_i'] = l - 1$.

Lemma 4.2. (i) *The extension F_i'/k_0' is Galois so that $\mathrm{Gal}(F_i'/K_0')$ is naturally a C_n-module.*
(ii) *As C_n-modules, $\mathrm{Gal}(F_i'/K_0')$ is isomorphic to $\mathrm{Gal}(F_i/K_0'(\zeta_l))$.*

Proof. (i) The Galois group $\mathrm{Gal}(F_i/F_i')$ is the subgroup of the C_n-module $\mathrm{Gal}(F_i/K_0')$ consisting of those elements whose orders are prime to l. Hence it is a C_n-submodule of $\mathrm{Gal}(F_i/K_0')$, which shows that F_i'/k_0' is Galois.
(ii) By the proof of (i), as C_n-modules, $\mathrm{Gal}(F_i/K_0')$ is the direct product of $\mathrm{Gal}(F_i/F_i')$ and $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ and (ii) follows from this.

As $F_i/K_0'(\zeta_l)$ is a Kummer extension with exponent l, $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ is an $\mathbb{F}_l[C_n]$-module.

Lemma 4.3. *The C_n-module $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ is regular, i.e. it is isomorphic to $\mathbb{F}_l[C_n]$.*

Proof. Let H_i be the subgroup of $K_0'(\zeta_l)^*/(K_0'(\zeta_l)^*)^l$ generated by $H_{i,\sigma}$ for all $\sigma \in \mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$. Then H_i is the direct product of $H_{i,\sigma}$ for all σ, for, by the condition (a) of $\mathfrak{Q}_i$, there are no common primes in the righthand side of $(*)_{i,\sigma_1}$ and $(*)_{i,\sigma_2}$ if $\sigma_1 \neq \sigma_2$. From this it follows that, as C_n-modules, H_i is isomorphic to $\mathbb{F}_l[C_n]$.

Now $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ is isomorphic to $\mathrm{Hom}(H_i, \mu_l)$, the group of homomorphisms from H_i to μ_l, not only as abelian groups but as C_n-modules. As C_n acts trivially on μ_l, this shows that $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ is contragredient to H_i. As is well-known, the regular representation is self-contragredient. Hence $\mathrm{Gal}(F_i/K_0'(\zeta_l))$ is isomorphic to $\mathbb{F}_l[C_n]$.

Let F be the composite of F_i for all i, $1 \leq i \leq m$, and H be the subgroup of $K_0'(\zeta_l)^*/(K_0'(\zeta_l)^*)^l$ generated by $H_{i,\sigma}$ for all $\sigma \in \mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$ and for all i, $1 \leq i \leq m$.

Lemma 4.4. (i) *The C_n-module* $\mathrm{Gal}(F/K_0'(\zeta_l))$ *is isomorphic to* $\mathbb{F}_l[C_n]^{\oplus m}$.
(ii) *We have* $F \cap L(\zeta_l) = K_0'(\zeta_l)$.

Proof. (i) By the condition (a) of $\mathfrak{Q}_i, 1 \leq i \leq m$, there are no common primes in the righthand side of $(*)_{i_1,\sigma_1}$ and $(*)_{i_2,\sigma_2}$ if $(i_1,\sigma_1) \neq (i_2,\sigma_2)$. Thus, H is the direct product of $H_{i,\sigma}$ for all σ and all i, i.e. H is the product of the subgroups H_i, $1 \leq i \leq m$, H_i being as in the proof of Lemma 4.3. Hence, as C_n-modules, $\mathrm{Gal}(F/K_0'(\zeta_l))$ is isomorphic to the direct product of $\mathrm{Gal}(F_i/K_0'(\zeta_l))$, $1 \leq i \leq m$, and (i) follows from Lemma 4.3.
(ii) We first claim that $F/K_0'(\zeta_l)$ contains no non-trivial unramified subextension. In fact, F is the composite of $F_{i,\sigma}$ for all i, $1 \leq i \leq m$, and all $\sigma \in \mathrm{Gal}(K_0'(\zeta_l)/k_0'(\zeta_l))$. Further, each $F_{i,\sigma}/K_0'(\zeta_l)$ has the properties (i) and (ii) in Lemma 4.1, and there are no common primes in $\{\mathfrak{Q}_{i_1}^{\sigma_1\rho^j}\}_j$ and $\{\mathfrak{Q}_{i_2}^{\sigma_2\rho^j}\}_j$ if $(i_1,\sigma_1) \neq (i_2,\sigma_2)$. From this the claim follows easily.

Now let $F \cap L(\zeta_l) = K'$ and assume that $K' \neq K_0'(\zeta_l)$. By the above claim, there exists at least one prime of $K_0'(\zeta_l)$ ramfied in K', which must be $\mathfrak{Q}_i^{\sigma'}$ for some i and $\sigma' \in \mathrm{Gal}(K_0'(\zeta_l)/k_0')$. Let $\mathfrak{Q} = \mathfrak{Q}_i^{\sigma'} \cap k_0$ and $\mathfrak{Q}_0 = \mathfrak{Q}_i^{\sigma'} \cap k_0'$. As $\mathfrak{Q}_i^{\sigma'}$ is of absolutely degree one and is unramified over $\mathbb{Q}$, and as $k_0' \neq k_0$, there exists a prime $\mathfrak{Q}_0'$ of k_0' lying above $\mathfrak{Q}$ such that $\mathfrak{Q}_0' \neq \mathfrak{Q}_0$. Let $\tilde{\mathfrak{Q}}$ be a prime of $K_0'(\zeta_l)$ lying above $\mathfrak{Q}_0'$. Then, we see easily that $\tilde{\mathfrak{Q}}$ is, over k_0', neither conjugate to $\mathfrak{Q}_i$ nor to $\mathfrak{Q}_j$ for $j \neq i$. Thus, by Lemma 4.1(ii), $\tilde{\mathfrak{Q}}$ is unramified in F, and hence in K'. As $\mathfrak{Q}_i^{\sigma'}$ and $\tilde{\mathfrak{Q}}$ are both lying above $\mathfrak{Q}$, and as K' is abelian over k_0, this is a contradiction. Thus we have $F \cap L(\zeta_l) = K_0'(\zeta_l)$.

For each i, $1 \leq i \leq m$, let $\mathfrak{q}_i = \mathfrak{Q}_i \cap k_0'$.

Lemma 4.5. *There exists a finite extension k_i' of k_0' contained in L_D such that for every prime of k_i' lying above $\mathfrak{q}_i$, its ramification index in k_i'/k_0' is $q_i - 1$.*

Proof. Let L_I be the inertia field of $\mathfrak{Q}_i$ in L_D. By Lemma 2.1 (i), L/L_D is unramified. Thus, by the condition (I_1), L_D/L_I is a finite extension of degree $q_i - 1$. Hence there exists a finite extension k_i'/k_0' such that $k_i'L_I = L_D$ and this k_i' satisfies the condition in Lemma 4.5.

Let us consider the composite of k_i', $1 \leq i \leq m$, in Lemma 4.5 and denote it newly by k_1'. Then k_1' is a finite extension of k_0' contained in L_D such that for every prime of k_1' lying above $\mathfrak{q}_i$, $1 \leq i \leq m$, its ramification index in k_1'/k_0' is $q_i - 1$.

We extend k_0' to k_1' and let $K_1' = k_1'K_0'$. We have $k_1' \subset K_1'$, $L_D \cap K_1' = k_1'$ and $L_DK_1' = L_n$. Consider the extension F_iK_1' of $K_1'(\zeta_l)$. It is the composite of F_i and $K_1'(\zeta_l)$, and by Lemma 4.4 (ii), we have $F_i \cap K_1'(\zeta_l) = K_0'(\zeta_l)$.

Lemma 4.6. *The extension $F_iK_1'/K_1'(\zeta_l)$ is unramified.*

Proof. It follows from Lemma 4.1 (ii) that $F_i/K_0'(\zeta_l)$ is unramified outside $\mathfrak{Q}_i^{\sigma\rho^j}, j = 0, 1, ..., l-2$, and the ramification index of $\mathfrak{Q}_i^{\sigma\rho^j}$ is l. On the other hand, as $\mathfrak{q}_i$ is unramified in $K_0'(\zeta_l)$, by Lemma 4.5, the ramification index of $\mathfrak{Q}_i^{\sigma\rho^j}$ in $K_1'(\zeta_l)$ is $q_i - 1$. By noting that q_i splits completely in the subfield $\mathbb{Q}(\zeta_l)$ of K_0', the proof is done in the same way as that of Lemma 2.4.

Now we shall complete the proof of Theorem 4.1. By Lemma 4.2 (ii) and Lemma 4.3, the C_n-module $\mathrm{Gal}(F_i'/K_0')$ is isomorphic to $\mathbb{F}_l[C_n]$. Let F' be the composite of $F_1', ..., F_m'$. Then we have $F'K_0'(\zeta_l) = F$ and it follows from Lemma 4.4 (i) that $\mathrm{Gal}(F'/K_0')$ is isomorphic to $\mathbb{F}_l[C_n]^{\oplus m}$. Consider the extension $M = F'L$ of L. We have $M(\zeta_l) = FL(\zeta_l)$ and, by Lemma 4.4 (ii), it follows that $\mathrm{Gal}(FL(\zeta_l)/L(\zeta_l))$ is, as an $\mathcal{A}_l$-module, isomorphic to $E_n(l)^{\oplus m}$. Hence $\mathrm{Gal}(M/L)$ is isomorphic to $E_n(l)^{\oplus m}$. It remains to show that M/L is unramified. It follows from Lemma 4.6 that $FL(\zeta_l)/L(\zeta_l)$ is unramified. For the extension $L(\zeta_l)/L$, it is unramified outside l and the ramification index of any l-place is $l-1$. As M/L is an l-extension, it is unramified.

(4-3) Let $L_{S_L}^{ab}(l)$ and $L_{ur}^{ab}(l)$ denote the maximal pro-l abelian extension of L unramified outside S_L and the maximal unramified pro-l abelian extension of L respectively. These are both Galois extensions of L_D. Hence, as explained in (4-1), the Galois groups $\mathrm{Gal}(L_{S_L}^{ab}(l)/L)$ and $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ are $\mathcal{A}_l$-modules.

Our main result in this paper is the following

Theorem 4.2. *Let l be an odd prime. Let L be an abelian extension of k_0 satisfying the conditions* (I_1) *and* (I_2) *such that* $[L(\zeta_l) : L] = l - 1$.
(i) *Assume that the condition* (II_l) *is satisfied. Then the $\mathcal{A}_l$-module* $\mathrm{Gal}(L_{S_L}^{ab}(l)/L)$ *is isomorphic to the direct product of a countable number of copies of $\mathcal{A}_l$.*
(ii) *Assume that the conditions* (II_l) *and* (III_l) *are satisfied. Then the $\mathcal{A}_l$-module* $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ *is isomorphic to the direct product of a countable number of copies of $\mathcal{A}_l$.*

Proof. By Corollaries to Theorems 3.1 and 3.2, $\mathrm{Gal}(L_{S_L}(l)/L_D)$ and $\mathrm{Gal}(L_{ur}(l)/L_D)$ are both projective profinite groups. By the argument given in [1, 3.1], it follows from this that $\mathrm{Gal}(L_{S_L}^{ab}(l)/L)$ and $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ are projective $\mathcal{A}_l$-modules. By Theorem 4.1, $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$, and hence $\mathrm{Gal}(L_{S_L}^{ab}(l)/L)$ also, have quotient $\mathcal{A}_l$-modules isomorphic to $E_n(l)^{\oplus m}$ for any $m, n \geq 1$. Further $\mathrm{Gal}(L_{S_L}^{ab}(l)/L)$ and $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ are both pro-l $\mathcal{A}_l$-modules with countable open $\mathcal{A}_l$-submodules. Therefore, by a characterization of such $\mathcal{A}_l$-modules ([1, Theorems 1.2, 1.3]), these Galois groups are isomorphic to the direct product of a countable number of copies of $\mathcal{A}_l$.

Let L' be the maximal unramified abelian extension of L_D in $L_{ur}^{ab}(l)$. Then we have $L \subset L' \subset L_{ur}^{ab}(l)$ and the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L')$ is an $\mathcal{A}_l$-submodule of $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$. For the structure of this submodule, we have the following

Corollary. *Assumptions being as in Theorem 4.2* (ii), $\mathrm{Gal}(L_{ur}^{ab}(l)/L')$ *is isomorphic to the direct product of a countable number of copies of* I_D, *where* I_D *denotes the augmentation ideal of $\mathcal{A}_l$.*

Proof. Let $X_l = \mathrm{Gal}(L_{ur}^{ab}(l)/L)$ and σ be a topological generator of $D = \mathrm{Gal}(L/L_D)$. Then $X_l/(\sigma - 1)X_l$ is the maximal quotient of X_l on which D acts trivially. Let L'' be the subextension of $L_{ur}^{ab}(l)/L$ such that $\mathrm{Gal}(L''/L) = X_l/(\sigma - 1)X_l$. Obviously, L' is contained in L''. Consider the exact sequence

$$1 \to \mathrm{Gal}(L''/L) \to \mathrm{Gal}(L''/L_D) \to D \to 1.$$

Since D is isomorphic to $\hat{\mathbb{Z}}$, the sequence splits. As D acts on $\mathrm{Gal}(L''/L)$ trivially, $\mathrm{Gal}(L''/L_D)$ is isomorphic to the direct product of $\mathrm{Gal}(L''/L)$ and D. Let $\mathrm{Gal}(L''/L_D) = \mathrm{Gal}(L''/L) \times D'$, D' being a subgroup of $\mathrm{Gal}(L''/L_D)$ isomorphic to D, and L_1 be the subextension of L''/L_D corresponding to D'. Then L_1/L_D is an unramified pro-l abelian extension. Hence L_1 is contained in L' and we have $LL_1 \subset L'$. As $LL_1 = L''$, we have $L'' \subset L'$, and hence $L'' = L'$. Thus we have $\mathrm{Gal}(L_{ur}^{ab}/L') = (\sigma - 1)X_l$ and the corollary follows from Theorem 4.2 (ii).

(4-4) Let k_0 be an algebraic number field of finite degree and l be a fixed prime. In the following, we shall verify that the field obtained by adjoining to k_0 primitive q-th roots of unity, where q runs over all primes except for certain primes of a finite number, satisfy the assumptions of Theorem 4.2 (ii). Thus, by that theorem, we can determine the structure of the Galois groups as $\mathcal{A}_l$-modules of the maximal unramified pro-l abelian extensions of those algebraic number fields.

Let $S_0 = \{p_1, ..., p_s\}$ be a finite set of distinct primes with $s \geq 1$. Let L_{S_0} be the field obtained by adjoining to k_0 all primitive q-th root of unity, where q does not belong to S_0. For each i, $1 \leq i \leq s$, let $\mathfrak{p}_i$ be a prime of k_0 lying above p_i and let $N\mathfrak{p}_i = p_i^{f_i}$, $f_i \geq 1$. Let D_i be the decomposition group of $\mathfrak{p}_i$ for the extension L_{S_0}/k_0. Then we have the following

Proposition 4.1. (i) *The group D_i is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of the additive group of rational integers.*
(ii) *If $s \geq 2$, we have $D_i \cap \langle D_j \rangle_{j \neq i} = \{1\}$, where $\langle D_j \rangle_{j \neq i}$ denotes the closed subgroup of* $\mathrm{Gal}(L_{S_0}/k_0)$ *generated by D_j, $j \neq i$.*

This proposition is verified by using a theorem of Chevalley, which we shall recall. (Cf. also Bass[3].)

Let k be an algebraic number field of finite degree and E be a finitely generated subgroup of the multiplicative group k^* of k. For any integers $a, m \geq 1$, let

$$E^m = \{\ x^m \mid x \in E\ \},$$

$$E_a = \{\ x \in E \mid x \equiv 1 \bmod a\ \}.$$

Then Chevalley[4] proved the following

Theorem. *Given any integers $m, b \geq 1$, there exists a squarefree integer $a \geq 1$ such that $(a,\ b) = 1$ and $E_a \subset E^m$.*

Remark. The proof shows that the integer a can be taken to be squarefree, though it is not explicitly stated.

Proof of Proposition 4.1. The cyclotomic character induces an embedding

$$\mathrm{Gal}(L_{S_0}/k_0) \to \prod_{q \notin S_0} (\mathbb{Z}/(q))^*$$

of the Galois group $\mathrm{Gal}(L_{S_0}/k_0)$. The image of the subgroup D_i is the closed subgroup generated by the diagonal element $(p_i^{f_i})$. Let E be the subgroup of $\mathbb{Q}^*$, the multiplicative group of rationals, generated by all $p_i^{f_i}, 1 \leq i \leq s$. Consider the diagonal embedding

$$E \to \prod_{q \notin S_0} (\mathbb{Z}/(q))^*.$$

Applying Chevalley's theorem to the case that $K = \mathbb{Q}$ and $b = p_1 ... p_s$, we see that the closure of the image of E is isomorphic to the profinite completion $\hat{E}$ of E. As E is a free abelian group of rank s, $\hat{E}$ is isomorphic to $\hat{\mathbb{Z}}^{\oplus s}$. From this the proposition follows.

Now we shall assume that $s \geq 2$ and p, l be distinct primes in S_0. Let $\mathfrak{p}$ and $\mathfrak{l}$ be primes of k_0 lying above p and l respectively. Let $D_\mathfrak{p}$ be the decomposition group of $\mathfrak{p}$ for the extension L_{S_0}/k_0 and $L_{D_\mathfrak{p}}$ be the decomposition field of $\mathfrak{p}$.

Proposition 4.2. *Let $\mathfrak{l}'$ be a prime of $L_{D_\mathfrak{p}}$ lying above $\mathfrak{l}$. Then the residue field of $\mathfrak{l}'$ is the algebraic closure $\bar{\mathbb{F}}_l$ of the prime field $\mathbb{F}_l$.*

Proof. Let $D_\mathfrak{l}$ be the decomposition group of $\mathfrak{l}$ for the extension L_{S_0}/k_0 and $L_{D_\mathfrak{l}}$ be the decomposition field of $\mathfrak{l}$. By Proposition 4.1 (ii), we have $D_\mathfrak{p} \cap D_\mathfrak{l} = \{1\}$. As $\mathfrak{l}$ splits completely in $L_{D_\mathfrak{l}}$, $\mathfrak{l}'$ splits completely in L_{S_0}. By the remark after Lemma 2.1, the residue field of an extension of $\mathfrak{l}$ to L_{S_0} is $\bar{\mathbb{F}}_l$. Hence the residue field of $\mathfrak{l}'$ is also $\bar{\mathbb{F}}_l$.

Let $L_{ur}^{ab}(l)$ be the field as in the beginning of (4-3) for $L = L_{S_0}$. Then the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is naturally an $\mathcal{A}_l$-module and we have the following

Theorem 4.3. *Assume that l is odd and is unramified in k_0. Let p be a prime different from l and assume that S_0 contains p and l. Then the Galois group $\mathrm{Gal}(L_{ur}^{ab}(l)/L_{S_0})$ is isomorphic to the direct product of a countable number of copies of $\mathcal{A}_l$.*

Proof. It suffices to verify that the assumptions in Theorem 4.2 (ii) are satisfied. Obviously, L_{S_0} satisfies the condition (I_1) in (2-1). By Proposition 4.1 (i), L_{S_0} with $\mathfrak{p}_i$, for any i, satisfies the condition (I_2) in (2-1). By Proposition 4.2, L_{S_0} with $\mathfrak{p}$ being given, l satisfies the condition (III_l) in (3-2). By the assumption that l is unramified in k_0, the condition (II_l) in (3-1) is satisfied. Further, we have $[L_{S_0}(\zeta_l) : L_{S_0}] = l - 1$ and the proof is completed.

5. Decomposition groups

(5-1) Let k_0 be an algebraic number field of finite degree and l be an odd prime. Let L be an abelian extension of k_0 satisfying the conditions (I_1) and (I_2) in §2 and L_D be the decomposition field of $\mathfrak{p}$ in L/k_0. Let $L_{ur}^{ab}(l)$ be the maximal unramified pro-l abelian extension of L. As L/L_D is unramified by Lemma 2.1 (i), $L_{ur}^{ab}(l)/L_D$ is an umramified Galois extension. Assume that $[L(\zeta_l) : L] = l - 1$ and that the conditions (II_l) and (III_l) in §3 are satisfied.

In this section, by using Theorem 4.2 (ii), we shall give some remarks on the decomposition group for the extension $L_{ur}^{ab}(l)/L_D$ of a prime of $L_{ur}^{ab}(l)$ lying above $\mathfrak{p}$.

We fix a prime $\mathfrak{p}_0$ of L_D lying above $\mathfrak{p}$. Let $\mathfrak{p}_0'$ be the unique prime of L lying above $\mathfrak{p}_0$ and $\mathfrak{p}_0^*$ be a prime of $L_{ur}^{ab}(l)$ lying above $\mathfrak{p}_0'$. Let D_0^* be the decomposition group of $\mathfrak{p}_0^*$ for the extension $L_{ur}^{ab}(l)/L_D$. By the remark after Lemma 2.1, the residue field of $\mathfrak{p}_0'$ is $\bar{\mathbb{F}}_p$. Hence $\mathfrak{p}_0'$ splits completely in $L_{ur}^{ab}(l)$. Thus we have $D_0^* \cap \mathrm{Gal}(L_{ur}^{ab}(l)/L) = \{1\}$ and the projection $\mathrm{Gal}(L_{ur}^{ab}(l)/L_D) \to \mathrm{Gal}(L/L_D) = D$ induces an isomorphism $D_0^* \simeq D$. Namely D_0^* gives a splitting of the exact sequence

$$1 \to \mathrm{Gal}(L_{ur}^{ab}(l)/L) \to \mathrm{Gal}(L_{ur}^{ab}(l)/L_D) \to D \to 1$$

and we have the semi-direct decomposition of $\mathrm{Gal}(L_{ur}^{ab}(l)/L_D)$; $\mathrm{Gal}(L_{ur}^{ab}(l)/L_D) = \mathrm{Gal}(L_{ur}^{ab}(l)/L) \cdot D_0^*$.

The following two propositions are direct consequences of the properties of the subgroup $\mathrm{Gal}(L_{ur}^{ab}(l)/L)$ of $\mathrm{Gal}(L_{ur}^{ab}(l)/L_D)$.

Let $\mathfrak{p}_0^{**}$ be a prime of $L_{ur}^{ab}(l)$ lying above $\mathfrak{p}_0'$ other than $\mathfrak{p}_0^*$ and D_0^{**} be the decomposition group of $\mathfrak{p}_0^{**}$ for the extension $L_{ur}^{ab}(l)/L_D$. We have the following

Proposition 5.1. *If $\mathfrak{p}_0^* \neq \mathfrak{p}_0^{**}$, then we have $D_0^* \neq D_0^{**}$.*

For the proof, we first recall the following. Let G be a group which is the semi-direct product of a normal subgroup H and a subgroup K. Let $N_G(K)$ and $C_H(K)$ denote the normalizer of K in G and the centralizer of K in H respectively ;

$$N_G(K) = \{\sigma \in G \mid \sigma K \sigma^{-1} = K\},$$
$$C_H(K) = \{h \in H \mid hk = kh \ for \ any \ k \in K\}.$$

As is easily verified, we have the direct product $N_G(K) = C_H(K) \times K$.

Let $G = \mathrm{Gal}(L_{ur}^{ab}(l)/L_D)$, $H = \mathrm{Gal}(L_{ur}^{ab}(l)/L)$, and $K = D_0^*$. As we have seen above, $G = H \cdot K$.

Lemma 5.1. *We have $C_H(K) = \{1\}$, and hence $N_G(K) = K$.*

Proof. The group K acts on H by conjugation, so that H is a K-group. By Theorem 4.2 (ii), H is isomorphic to $\prod_{N=1}^{\infty} \mathbb{Z}_l[[K]]$ as K-groups. For an element h of H, let $(f_N)_N$ be the element of $\prod_{N=1}^{\infty} \mathbb{Z}_l[[K]]$ corresponding to h. Assume that $h \in C_H(K)$. Then we have $k(f_N) = (f_N)$, i.e. $(k-1)f_N = 0$ for all $k \in K$. Take k to be a topological generator of K. As the order of k is divisible by a supernatural number l^∞, $k-1$ is not a zero-divisor of $\mathbb{Z}_l[[K]]$ (Ihara[6, Lemma 3.1]). Hence $f_N = 0$ for $N \geq 1$, i.e. h is the identity.

Proof of Proposition 5.1. As $\mathfrak{p}_0^*$ and $\mathfrak{p}_0^{**}$ are both lying above $\mathfrak{p}_0$, there exists an element σ of G such that $\mathfrak{p}_0^{**} = \mathfrak{p}_0^{*\sigma}$, and hence $D_0^{**} = \sigma^{-1} D_0^* \sigma$. By the assumption that $\mathfrak{p}_0^* \neq \mathfrak{p}_0^{**}$, we have $\sigma \notin D_0^*$. As $N_G(K) = K$ by Lemma 5.1, we conclude that $D_0^{**} \neq D_0^*$.

(5-2) As in (4-3), let L' be the maximal unramified abelian extension of L_D in $L_{ur}^{ab}(l)$. Let D_0' be the image of D_0^* under the projection $\mathrm{Gal}(L_{ur}^{ab}(l)/L_D) \to \mathrm{Gal}(L'/L_D)$ and L_0' be the intermediate field of L'/L_D corresponding to D_0'. Then L_0' is the decomposition field of $\mathfrak{p}_0$ in the abelian extension L'/L_D, i.e. L_0' is the maximal subextension of L'/L_D in which $\mathfrak{p}_0$ splits completely.

Let L_0'' be the maximal subextension of $L_{ur}^{ab}(l)/L_D$ in which $\mathfrak{p}_0$ splits completely. Obviously L_0'' contains L_0', but we have the following

Proposition 5.2. *The field L_0'' coincides with L_0'.*

Again, in general, let G be a group which is the semi-direct product of a normal subgroup H and a subgroup K. The group K acts on H by conjugation. Let $\mathcal{U} = \{U\}$ be the set of all normal subgroups of G satisfying

(1) U is contained in H.
(2) K acts on the quotient H/U trivially.

On the other hand, let $\mathcal{N} = \{N\}$ be the set of all normal subgroups of G containing K. Then we have the following

Lemma 5.2. (i) *Let U be an element of $\mathcal{U}$. Then $UK = \{\ uk \mid u \in U, k \in K\ \}$ belongs to $\mathcal{N}$. The correspondence $U \to UK$ gives a bijection between $\mathcal{U}$ and $\mathcal{N}$.*
(ii) *Let N_K be the normal subgroup of G generated by K. Then we have $N_K = U_K K$, where U_K is the element of $\mathcal{U}$ such that H/U_K is the maximal quotient group of H on which K acts trivially.*

Proof. (i) This does not seem to be well-known but the proof is elementary, and hence we omit the details here.
(ii) As N_K is the smallest normal subgroup of G containing K, this follows from (i).

Note that this lemma is also valid in the category of profinite groups.

Proof of Proposition 5.2. Again, let $G = \mathrm{Gal}(L_{ur}^{ab}(l)/L_D)$, $H = \mathrm{Gal}(L_{ur}^{ab}(l)/L)$, and $K = D_0^*$, so that we have $G = H \cdot K$. Let N_K be the normal subgroup of G generated by K. Then L_0'' is the intermediate field of $L_{ur}^{ab}(l)/L_D$ corresponding to N_K. By Lemma 5.2 (ii), we have $N_K = U_K K$, where U_K being the subgroup of G as in that lemma. The proof of Corollary to Theorem 4.2 shows that $U_K = \mathrm{Gal}(L_{ur}^{ab}(l)/L')$. Thus the intermediate field of $L_{ur}^{ab}(l)/L_D$ corresponding to N_K is L_0'. Hence L_0'' coincides with L_0'.

References

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

[2] M. Asada, *On the ideal class groups of the maximal cyclotomic extensions of algebraic number fields*, J. of Math. Soc. of Japan. **66** (2014), 1091–1103.

[3] H. Bass, *A remark on an arithmetic theorem of Chevalley*, Proc. Amer. Math. Soc. **60** (1965), 875–878.

[4] C. Chevalley, *Deux theoremes d'arithmetique*, J. Math. Soc. Japan. **3** (1951), 36–44.

[5] 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.

[6] Y. Ihara, *On Galois representations arising from towers of coverings of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$*, Invent. Math. **86** (1986), 427–459.

[7] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.

[8] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields, Second edition*, Springer, 2008.
[9] O. Neumann, *On p-closed number fields and an analogue of Riemann's existence theorem*, In : A. Fröhlich(ed.), Algebraic Number Fields, Academic Press London (1977), 625–647.
[10] H. Reichardt, *Konstruction von ZahlKörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math. **177** (1937), 1–5.
[11] J.P. Serre, *Corps locaux*, Hermann, 1962.
[12] J.P. Serre, *Cohomologie Galoisienne, Lecture Notes in Mathematics*, vol. 5, Springer, 1964 (5. edition 1994).
[13] I.R. Shafarevich, *On the construction of fields with a given Galois group of order l^{α}*, Izv. Akad. NaukSSSR, Ser. Mat. **18** (1954), 261–296.
[14] K. Uchida, *Galois groups of unramified solvable extensions*, Tohoku Math. J. **34** (1982), 311–317.

e-mail address : asada @ kit.ac.jp