Advanced Studies in Pure Mathematics 2, 1983
Galois Groups and their Representations
pp. 99-102

Galois Groups of Unramified Solvable Extensions

Kôji Uchida

Introduction

Throughout this paper, $\boldsymbol{Q}$, Z and ζ_n denote the rational numbers, the rational integers and a primitive n-th root of unity for a positive integer n. Let F be an algebraic number field of finite degree. We do not know any general method of determining the structure of the Galois group of the maximal unramified (solvable) extension of F. We mean by "unramified" that every finite or infinite prime is unramified. Let $F_n=F(\zeta_n)$ and let $F_\infty=\bigcup_n F_n$. A. Brumer recently proved that

Theorem [1]. *The ideal class group C_∞ of F_∞ is isomorphic to a countable direct sum of copies of $\boldsymbol{Q}/Z$.*

In the above, C_∞ is the direct limit $\varinjlim C_n$ of the ideal class groups C_n of F_n. This theorem suggests that the Galois group of the maximal unramified abelian extension of F_∞ be isomorphic to a countable direct product of copies of $\hat{Z}=\varprojlim Z/nZ$. If this is true, it is natural to ask what we can say about the Galois group of the maximal unramified (solvable) extension of F_∞. We will see an answer in the following for more general ground fields. For the details, see [5].

§ 1. The field $\boldsymbol{Q}^{(m)}$

Let m be a positive integer and let q be a prime number such that $q\equiv 1 \pmod{m}$. Then the cyclotomic field $\boldsymbol{Q}(\zeta_q)$ contains a unique subfield $\boldsymbol{Q}(\eta_q)$ such that $[\boldsymbol{Q}(\zeta_q):\boldsymbol{Q}(\eta_q)]=m$. Let $\boldsymbol{Q}^{(m)}$ be the field composed by $\boldsymbol{Q}(\eta_q)$ for all prime numbers q such that $q\equiv 1 \pmod{m}$. We note that $\boldsymbol{Q}^{(m)}$ depends only on m, and it is real if m is even.

Lemma 1. *Let l be a prime number and let $\boldsymbol{Q}_l$ be the l-adic number field. Then $\boldsymbol{Q}_l^{(m)}=\boldsymbol{Q}^{(m)}\cdot\boldsymbol{Q}_l$ contains the maximal unramified extension of $\boldsymbol{Q}_l$.*

Received November 30, 1982.

§ 2. Construction of p-extensions.

We will see below that a field containing $\boldsymbol{Q}^{(m)}$ for some m is sufficiently large for our argument. We will construct unramified p-extensions of such fields for any prime number p following Reichardt's method. So we briefly recall his method.

Let K be an algebraic number field and let F be a finite p-extension of K. Let $H=G(F/K)$ be the Galois group and let

$$1\longrightarrow Z/pZ\longrightarrow E\xrightarrow{\pi}H\longrightarrow 1$$

be a central group extension corresponding to a cocycle class $\{\alpha_{\sigma,\tau}\}\in H^2(H, Z/pZ)$. A solution of this imbedding problem is a Galois extension L of K containing F such that $E\cong G(L/K)$ and π coincides with the restriction map $G(L/K)\to G(F/K)$. Let $K_1=K(\zeta_p)$, $F_1=F(\zeta_p)$ and $n=[F_1: F]$. Then F_1 is a Galois extension of K whose Galois group is the direct product of $G(F_1/K_1)\cong H$ and $G(F_1/F)\cong G(K_1/K)$. As $H\cong G(F_1/K_1)$ operates trivially on ζ_p, Z/pZ can be identified with the group generated by ζ_p as H-modules. Hence there exists a natural homomorphism

$$\phi\colon H^2(H, Z/pZ)\longrightarrow H^2(H, F_1^{\times})\,.$$

The imbedding problem given by the above group extension has a solution over K_1 if and only if $\phi\{\alpha_{\sigma,\tau}\}=\{0\}$. If $F_1(\sqrt[p]{\mu})$, $\mu\in F_1$, is a solution, there exists an element $\nu\in F_1$ such that $F_1(\sqrt[p]{\nu})$ is also a solution of the same imbedding problem, and it is a Galois extension of K whose Galois group is isomorphic to the direct product of E and $G(K_1/K)$. Then $F_1(\sqrt[p]{\nu})$ contains a subfield which is a solution of the given imbedding problem over K.

§ 3. Theorems

We now investigate the structure of Galois groups of maximal unramified (solvable) extensions of algebraic number fields containing $\boldsymbol{Q}^{(m)}$ for some integer m.

Theorem 1. *Let K be an algebraic number field containing $\boldsymbol{Q}^{(m)}$ for some m. Let L be the maximal unramified extension (or the maximal unramified solvable extension) of K. Then the cohomological dimension of the Galois group $G(L/K)$ is at most* 1.

Let p be any prime number. Let M be the maximal unramified p-extension of K. If $\mathrm{cd}\ G(M/K)\leqq 1$, the same is true over any finite extension of K. Then $\mathrm{cd}_p\ G(L/K)\leqq 1$ follows which proves Theorem 1. Hence

we only need to show cd $G(M/K)\leqq 1$. Let F be any finite Galois extension of K contained in M. Let $H=G(F/K)$ and let

$$1\longrightarrow Z/pZ\longrightarrow E\xrightarrow{\pi} H\longrightarrow 1$$

be a group extension which does not split. It suffices to show that this imbedding problem has a solution in M. Class field theory shows

$$H^2(H, F_1^\times)\longrightarrow \coprod_v H^2(H_v, F_{1,v}^\times)$$

is injective, where H_v is the decomposition subgroup of a prime v of $K_1=K(\zeta_p)$. Lemma 1 shows every $H_v=1$ because F_v/K_v is unramified. Hence $H^2(H, F_1^\times)=0$. Then Reichardt's argument shows there exists a solution of the above imbedding problem (not necessarily in M). We can follow Reichardt's or Shafarevich's argument to obtain an unramified solution of the imbedding problem as our ground field is sufficiently large.

We now show that the Galois group of the maximal unramified solvable extension is free if the ground field is sufficiently but not too large.

Lemma 2 [2]. *Let G be a pro-solvable group with at most countable open subgroups. Then G is a free pro-solvable group with countable generators, if it satisfies the conditions*:

i) cd $G\leqq 1$.

ii) *Let U be any open normal subgroup and let p be any prime number. Let $H=G/U$, and let*

$$1\longrightarrow (Z/pZ)H\longrightarrow E\xrightarrow{\pi} H\longrightarrow 1$$

be a split group extension with the natural action of H on $(Z/pZ)H$. Then there exists an open normal subgroup V of G contained in U such that $G/V\cong E$ and the natural projection $G/V\to G/U$ coincides with π.

Theorem 2. *Let K be an algebraic number field containing $\boldsymbol{Q}^{(m)}$ for some integer m. We further assume that K contains a subfield K_0 of finite degree over $\boldsymbol{Q}$ such that K is a subfield of the maximal nilpotent extension of K_0. Let L be the maximal unramified solvable extension of K. Then the Galois group $G(L/K)$ is a free pro-solvable group with countable generators.*

As $G(L/K)$ has at most countable open subgroups and as cd $G(L/K)\leqq 1$ by Theorem 1, we only need to show the condition (ii) of Lemma 2. Let F be any finite Galois extension of K contained in L. Let

$$1\longrightarrow (Z/pZ)H\longrightarrow E\xrightarrow{\pi} H\longrightarrow 1$$

be a split group extension of $H=G(F/K)$ as in Lemma 2. Let $F_1=F(\zeta_p)$ and let $n=[F_1: F]$. We can find a subfield $\mathfrak{k}$ of K such that

i) $[\mathfrak{k}: Q]$ is finite.

ii) There exists a finite unramified Galois extension $\mathfrak{f}$ of $\mathfrak{k}$ such that $F=\mathfrak{f}\cdot K$, $\mathfrak{f}\cap K=\mathfrak{k}$, i.e., $G(\mathfrak{f}/\mathfrak{k})\cong H$.

iii) Let $\mathfrak{f}_1=\mathfrak{f}(\zeta_p)$. Then $n=[\mathfrak{f}_1: \mathfrak{f}]$.

iv) $\mathfrak{k}$ contains a subfield $\mathfrak{k}_0$ which is an extension of K_0 such that $\mathfrak{k}$ is a proper Galois extension of $\mathfrak{k}_0$ of degree prime to p.

It is not difficult to find a solution $\mathfrak{m}$ of the imbedding problem given by the above group extension over $\mathfrak{k}$. It is also easy to choose $\mathfrak{m}$ as $\mathfrak{m}\cdot K$ is unramified over K. The condition iv) shows $\mathfrak{m}\cap K=\mathfrak{k}$, that is, $\mathfrak{m}\cdot K$ is the solution of the required imbedding problem.

References

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

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

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

[4] I. R. Shafarevich, On the construction of fields with given Galois group of order l^a, Izv. Akad. Nauk SSSR, **18** (1954) 261–296, AMS Translation **4** (1956), 107–142.

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

Department of Mathematics
College of General Education
Tôhoku University
Sendai 980, Japan