

Title	On the existence of unramified p -extensions with prescribed Galois group
Author(s)	Nomura, Akito
Citation	Osaka Journal of Mathematics. 2010, 47(4), p. 1159-1165
Version Type	VoR
URL	https://doi.org/10.18910/4603
rights	
Note	

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University

ON THE EXISTENCE OF UNRAMIFIED p -EXTENSIONS WITH PRESCRIBED GALOIS GROUP

AKITO NOMURA

(Received April 21, 2009, revised September 1, 2009)

Abstract

We shall prove that for any finite p -group G , there exists an elementary abelian p -extension k/\mathbf{Q} and an unramified extension K/k such that the Galois group $\text{Gal}(K/k)$ is isomorphic to G .

1. Introduction

Let p be a prime number. For an odd prime number p , Scholz [9] and Reichardt [8] proved that every finite p -group G can be realized as the Galois group of some extension M of the rational number field \mathbf{Q} . Fröhlich [2] proved that for any positive integer n , there exists a number field F of finite degree and an unramified extension K/F such that the Galois group $\text{Gal}(K/F)$ is isomorphic to the symmetric group S_n of degree n . Uchida [11] and Yamamoto [13] studied the existence of an unramified extension over a quadratic field whose Galois group is isomorphic to the alternating group A_n . By using their results, we see that the base field F of an unramified S_n -extension can be chosen as a quadratic field. These results imply that any finite p -group can be realized as the Galois group of some unramified extension K/k . Uchida [12] studied the Galois groups of maximal unramified solvable extensions of certain algebraic number fields of infinite degree over \mathbf{Q} . His result implies that for any finite p group G , there exists a cyclotomic field k of finite degree over \mathbf{Q} having a finite unramified Galois extension with the Galois group G . Recently, Ozaki [7] proved that for any finite p -group G , there exists a number field of finite degree such that the Galois group of its maximal unramified p -extension is isomorphic to G . In [7], he also proved that for any pro- p -group G , there exists a number field (not necessarily finite degree) such that the Galois group of its maximal unramified pro- p -extension is isomorphic to G .

In Fröhlich [2], Uchida [11], Yamamoto [13] and Ozaki [7], the degree of the base field k is high in general. In Uchida [12], the degree of k over \mathbf{Q} does not be explicit. We want to reduce the degree of the base field k as much as possible. In this article, we shall prove that for any finite p -group G , there exists an elementary abelian p -extension k/\mathbf{Q} and an unramified extension K/k such that the Galois group $\text{Gal}(K/k)$ is isomorphic to G . More precisely, it follows from the proof that the base

field k can be chosen such that $[k : \mathbf{Q}] = p^{m+1}$, where $|G^p[G, G]| = p^m$.

2. Preliminary from embedding problems

In this section, we quote some results about embedding problems. General studies on embedding problems can be found in Hoechsmann [4] and Neukirch [5].

Let k be a number field of finite degree and \mathfrak{G} the absolute Galois group of k . Let K/k be a finite Galois extension with the Galois group G . For a central extension $(\varepsilon): 1 \rightarrow A \rightarrow E \xrightarrow{j} G \rightarrow 1$ of finite groups, the embedding problem $(K/k, \varepsilon)$ is defined by the diagram

$$\begin{array}{ccccccc}
 & & & & \mathfrak{G} & & \\
 & & & & \downarrow \varphi & & \\
 (\varepsilon): & 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G & \longrightarrow & 1,
 \end{array}$$

where φ is the canonical surjection. A continuous homomorphism ψ of \mathfrak{G} to E is called a solution of $(K/k, \varepsilon)$ if it satisfies the condition $j \circ \psi = \varphi$. When $(K/k, \varepsilon)$ has a solution, we call $(K/k, \varepsilon)$ is solvable. A solution ψ is called a proper solution if it is surjective. A field M is called a solution field (resp. a proper solution field) of $(K/k, \varepsilon)$ if M is corresponding to the kernel of a solution (resp. a proper solution).

Let p be a prime number. In case when $p = 2$, we assume that k is totally imaginary. Let K/k be a p -extension, and let $(\varepsilon): 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(K/k) \rightarrow 1$ be a central extension. We remark that all infinite primes are not ramified in K/k . We assume that (ε) and k satisfy these conditions from Lemma 1 to Lemma 4.

Lemma 1 (Neukirch [5, Satz 2.2, Satz 4.7, Satz 5.1]). *If K/k is an unramified extension, then $(K/k, \varepsilon)$ is solvable.*

Lemma 2 (Hoechsmann [4, Satz 2.3]). *If (ε) is a non-split extension, then every solution of $(K/k, \varepsilon)$ is a proper solution.*

For each prime \mathfrak{q} of k , we denote by $k_{\mathfrak{q}}$ (resp. $K_{\mathfrak{q}}$) the completion of k (resp. K) by \mathfrak{q} (resp. an extension of \mathfrak{q} to K). Then the local problem $(K_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ of $(K/k, \varepsilon)$ is defined by the diagram

$$\begin{array}{ccccccc}
 & & & & \mathfrak{G}_{\mathfrak{q}} & & \\
 & & & & \downarrow \varphi|_{\mathfrak{G}_{\mathfrak{q}}} & & \\
 (\varepsilon_{\mathfrak{q}}): & 1 & \longrightarrow & A & \longrightarrow & E_{\mathfrak{q}} & \xrightarrow{j|_{E_{\mathfrak{q}}}} & G_{\mathfrak{q}} & \longrightarrow & 1,
 \end{array}$$

where $G_{\mathfrak{q}}$ is the Galois group of $K_{\mathfrak{q}}/k_{\mathfrak{q}}$, which is isomorphic to the decomposition

group of \mathfrak{q} in K/k , $\mathfrak{G}_{\mathfrak{q}}$ is the absolute Galois group of $k_{\mathfrak{q}}$, and $E_{\mathfrak{q}}$ is the inverse of $G_{\mathfrak{q}}$ by j .

In the same manner as the case of $(K/k, \varepsilon)$, solutions, solution fields etc. are defined for $(K_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$.

For a finite set S of primes of k , we define

$$B_k(S) = \{\alpha \in k^* \mid (\alpha) = \mathfrak{a}^p \text{ for some ideal } \mathfrak{a} \text{ of } k, \text{ and } \alpha \in k_{\mathfrak{q}}^p \text{ for } \mathfrak{q} \in S\}.$$

For a Galois extension K/k , we denote by $Ram(K/k)$ (resp. $Ram_K(K/k)$) the set of primes of k (resp. K) which are ramified in K/k .

Lemma 3 (Neukirch [5, Beispiel 1, Korollar 6.4]). *Assume that $(K/k, \varepsilon)$ is solvable. Let T be a finite set of primes of k , and $M(\mathfrak{q})$ be a solution field of $(K_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ for \mathfrak{q} of T . Then there exists a solution field M of $(K/k, \varepsilon)$ such that the completion of M by \mathfrak{q} is equal to $M(\mathfrak{q})$ for each \mathfrak{q} of T .*

The following lemma is a special case of the main theorem in Nomura [6]. For the convenience of the reader, we give a sketch of the proof.

Lemma 4. *Let S be a finite set of primes of k satisfying the conditions:*

- (1) $B_k(S) = k^{*p}$,
- (2) any prime of k lying above p is not contained in S .

Assume that K/k is an unramified p -extension and (ε) is a non-split central extension. Then $(K/k, \varepsilon)$ has a proper solution field M such that M/k is unramified outside S .

Proof. By Lemmas 1 and 2, $(K/k, \varepsilon)$ has a proper solution. Let \mathfrak{p} be a prime of k lying above p . Since K/k is unramified, $K_{\mathfrak{p}}/k_{\mathfrak{p}}$ is an unramified cyclic extension. Then local extension $(\varepsilon_{\mathfrak{p}})$ is split or $E_{\mathfrak{p}}$ is cyclic. Hence $(K_{\mathfrak{p}}/k_{\mathfrak{p}}, \varepsilon_{\mathfrak{p}})$ has a solution field $M(\mathfrak{p})$ such that $M(\mathfrak{p})/k_{\mathfrak{p}}$ is unramified. By Lemmas 2 and 3, there exists a proper solution field M_1 of $(K/k, \varepsilon)$ such that any prime of k lying above p is unramified in M_1/k . If M_1/k is unramified outside S , then M_1 is a required solution. Assume that $\mathfrak{q} \notin S$ is ramified in M_1/k . By Shafarevich's formula [10, Theorem 1], there exists a cyclic extension F/k of degree p such that F/k is unramified outside $S \cup \{\mathfrak{q}\}$ and that \mathfrak{q} is ramified in F/k . Let Ω be an extension of \mathfrak{q} to M_1F , and let M_2 be the inertia field of Ω in M_1F/k . Then M_2 is also a proper solution field and $Ram(M_1/k) \cup S \supsetneq Ram(M_2/k) \cup S$. By repeating this process, we obtain a required proper solution. \square

3. Main theorem and some applications

In this section, we shall prove the main theorem and its application to the structure of ideal class groups.

Theorem 5. *For any finite p -group G , there exist infinitely many number fields k and unramified Galois extensions K/k satisfying the conditions:*

- (1) k/\mathbf{Q} is an elementary abelian p -extension,
- (2) $\text{Gal}(K/k)$ is isomorphic to G .

Lemma 6. *Let T be any finite set of primes of k . Then there exists a finite set S of primes of k satisfying the conditions:*

- (1) $S \cap T = \emptyset$,
- (2) $B_k(S) = k^{*p}$,
- (3) $N(\mathfrak{q}) \equiv 1 \pmod{p}$ for $\mathfrak{q} \in S$, where $N(\mathfrak{q})$ is the absolute norm of \mathfrak{q} .

Proof. Let $M = k(\sqrt[p]{\alpha}; \alpha \in B_k(\emptyset))$. Then $M \supset k(\zeta_p)$ and $\text{Gal}(M/k(\zeta_p))$ is an elementary abelian p -group. By Chebotarev's density theorem, there exist primes $\Omega_1, \Omega_2, \dots, \Omega_r$ of M such that the Frobenius $[(M/k)/\Omega_i]$ ($i = 1, 2, \dots, r$) generate $\text{Gal}(M/k(\zeta_p))$ and that the restriction to k are not contained in T . Let \mathfrak{q}_i be the restriction of Ω_i to k . Then $S = \{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\}$ is a required set. \square

For a finite set S of primes of k , we denote by $S|_{\mathbf{Q}}$ the set of primes which are the restriction to \mathbf{Q} of \mathfrak{q} in S .

Lemma 7. *Let k/\mathbf{Q} be a p -extension and K/k an unramified p -extension. In case when $p = 2$ we assume that k is totally imaginary. Let $(\varepsilon): 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(K/k) \rightarrow 1$ be a non-split central extension. Assume that the finite set S of primes of k satisfies the conditions:*

- (1) $S \cap \text{Ram}_k(k/\mathbf{Q}) = \emptyset$,
- (2) $B_k(S) = k^{*p}$,
- (3) $N(\mathfrak{q}) \equiv 1 \pmod{p}$ for $\mathfrak{q} \in S$.

Let F/\mathbf{Q} be a cyclic extension of degree p such that any prime $\mathfrak{q} \in S|_{\mathbf{Q}}$ is ramified in F/\mathbf{Q} .

Then there exists an unramified Galois extension M/kF such that the Galois group $\text{Gal}(M/kF)$ is isomorphic to E .

Proof. By the condition (3), any prime lying above p is not contained in S . By Lemmas 1 and 4, the embedding problem $(K/k, \varepsilon)$ has a proper solution field which is unramified outside S . Namely, there exists a Galois extension $L/K/k$ satisfying the conditions:

- (a) $\text{Gal}(L/k) \cong E$,
- (b) L/k is unramified outside S .

By the assumption of F and the condition (1), we see that $F \cap k = \mathbf{Q}$. Hence $\text{Gal}(LF/kF) \cong \text{Gal}(L/k) \cong E$. Let $M = LF$. Since K/k is unramified, the ramification index of \mathfrak{q} in L/k is at most p . By virtue of Abhyankar's lemma (cf., e.g. Cornell [1, Theorem 1]), M/kF is unramified. \square

Proof of Theorem 5. Let $G_1 = \Phi(G)$ be the Frattini subgroup of G , which is defined by $G^p[G, G]$. Let $G \supset G_1 \supset G_2 \supset G_3 \supset \dots \supset G_m = \{1\}$ be a series of normal subgroups of G such that $G_i/G_{i+1} \cong \mathbf{Z}/p\mathbf{Z}$ ($i = 1, 2, \dots, m - 1$). Then G/G_1 is an elementary abelian p -group and the canonical sequence $1 \rightarrow G_i/G_{i+1} \rightarrow G/G_{i+1} \rightarrow G/G_i \rightarrow 1$ is a non-split central extension.

We prove the existence of an unramified extension with Galois group isomorphic to G/G_i . We use induction on i . First, by genus theory (cf., e.g. Furuta [3]), there exists a cyclic extension k_1/\mathbf{Q} of degree p and an unramified extension K_1/k_1 such that $\text{Gal}(K_1/k_1)$ is isomorphic to G/G_1 . In case when $p = 2$, we can take k_1 to be an imaginary quadratic field. We remark that there exist infinitely many such fields k_1 .

Let k_i/\mathbf{Q} be an elementary abelian p -extension and K_i/k_i an unramified extension such that $\text{Gal}(K_i/k_i)$ is isomorphic to G/G_i . We consider the central extension $(\varepsilon): 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow G/G_{i+1} \rightarrow G/G_i \rightarrow 1$. By Lemma 6, there exists a finite set S of primes of k_i satisfying the conditions:

- (1) $S \cap \text{Ram}_{k_i}(k_i/\mathbf{Q}) = \emptyset$,
- (2) $B_{k_i}(S) = k_i^{*p}$,
- (3) $N(\mathfrak{q}) \equiv 1 \pmod p$ for any $\mathfrak{q} \in S$.

Let q be the characteristic of the residue field of \mathfrak{q} in S . Since k_i/\mathbf{Q} is a p -extension, $N(\mathfrak{q}) = q^{p^t}$ for some non-negative integer t . Then $q \equiv 1 \pmod p$ because $N(\mathfrak{q}) \equiv 1 \pmod p$.

Therefore there exists a cyclic extension F/\mathbf{Q} of degree p such that any prime $q \in S|_{\mathbf{Q}}$ is ramified. By Lemma 7, there exists a number field k_{i+1} and an unramified extension K_{i+1}/k_{i+1} such that $\text{Gal}(K_{i+1}/k_{i+1}) \cong G/G_{i+1}$. We have thus proved. \square

REMARK. Let $|G^p[G, G]| = p^m$. It follows from the proof of Theorem 5 that the base field k can be chosen such that $\text{Gal}(k/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^{m+1}$. If the sets S_i such that $B_{k_i}(S_i) = k_i^{*p}$ ($i = 1, 2, \dots, m - 1$) can be find, the base field k can be constructed explicitly.

Corollary 8. *For any positive integer n , there exist infinitely many number fields k such that $\text{Gal}(k/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^n$ and that the ideal class group Cl_k contains an element of order p^n .*

Proof. Let $G = \mathbf{Z}/p^n\mathbf{Z}$. By virtue of Theorem 5 combined with Remark above, the corollary follows. \square

Corollary 9. *Let k/\mathbf{Q} and F/\mathbf{Q} be cyclic extensions of degree p , and S be a finite set of primes of k . We assume the conditions:*

- (1) *at least three finite primes are ramified in k/\mathbf{Q} ,*
- (2) $S \cap \text{Ram}_k(k/\mathbf{Q}) = \emptyset$,
- (3) $B_k(S) = k^{*p}$,
- (4) $N(\mathfrak{q}) \equiv 1 \pmod p$ for any $\mathfrak{q} \in S$,

(5) any prime in $S|\mathbf{Q}$ is ramified in F/\mathbf{Q} ,

(6) k is imaginary quadratic field when $p = 2$.

Let E be any p -group such that $|E| = p^3$ and that the rank is equal to 2. Then there exists an unramified Galois extension of kF with the Galois group isomorphic to E .

Proof. By the condition (1) and the genus theory, there exists an unramified extension K/k such that $\text{Gal}(K/k) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Since the rank of E is 2, there exists a non-split central extension $(\varepsilon): 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(K/k) \rightarrow 1$. By applying Lemma 7, the corollary follows. \square

ACKNOWLEDGMENT. I should like to express my gratitude to Professor Mamoru Asada for his useful advice on Abhyankar's lemma. I also thank the referee for her/his careful reading and the advices.

References

- [1] G. Cornell: *Abhyankar's lemma and the class group*; in Number Theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math. **751**, Springer, Berlin, 82–88, 1979.
- [2] A. Fröhlich: *On non-ramified extensions with prescribed Galois group*, Mathematika **9** (1962), 133–134.
- [3] Y. Furuta: *The genus field and genus number in algebraic number fields*, Nagoya Math. J. **29** (1967), 281–285.
- [4] K. Hoehsmann: *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.
- [5] J. Neukirch: *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.
- [6] A. Nomura: *On embedding problems with restricted ramifications*, Arch. Math. (Basel) **73** (1999), 199–204.
- [7] M. Ozaki: *Construction of maximal unramified p -extensions with prescribed Galois groups*, to appear in Invent. Math.
- [8] H. Reichardt, *Konstruktion vom Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math. **177** (1937), 1–5.
- [9] A. Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*, Math. Z. **42** (1936), 161–188.
- [10] I.R. Shafarevich, *Extensions with given points of ramification*, Amer. Math. Soc. Translation, Ser. 2 **59** (1966), 128–149.
- [11] K. Uchida: *Unramified extensions of quadratic number fields II*, Tôhoku Math. J. (2) **22** (1970), 220–224.
- [12] K. Uchida: *Galois groups of unramified solvable extensions*, Tôhoku Math. J. (2) **34** (1982), 311–317.
- [13] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

Graduate School of Natural Science and Technology
Kanazawa University
Kanazawa 920-1192
Japan
e-mail: anomura@t.kanazawa-u.ac.jp