Illinois Journal of Mathematics
Volume 46, Number 4, Winter 2002, Pages 1279–1286
S 0019-2082

NOTES ON THE EXISTENCE OF CERTAIN UNRAMIFIED 2-EXTENSIONS

AKITO NOMURA

Abstract. We study the inverse Galois problem with restricted ramification. Let K be an algebraic number field and G be a 2-group. We consider the question whether there exists an unramified Galois extension M/K with Galois group isomorphic to G. We study this question using the theory of embedding problems. Let L/k be a Galois extension and $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/k) \to 1$ a central extension. We first investigate the existence of a Galois extension $M/L/k$ such that the Galois group $\mathrm{Gal}(M/k)$ is isomorphic to E and any finite prime is unramified in M/L. As an application, we prove the existence of an unramified extension over cyclic quintic fields with Galois group isomorphic to $32\Gamma_5 a_2$ under the condition that the class number is even. We also consider the Fontaine-Mazur-Boston Conjecture in the case of abelian l-extensions over $\mathbf{Q}$.

1. Introduction

An interesting problem in Number Theory is the inverse Galois problem with restricted ramification, which can be described as follows. Let K be an algebraic number field, and G a finite group. Does there exist an unramified Galois extension M/K with Galois group isomorphic to G? In the case when G is abelian, by class field theory, this problem is closely related to the ideal class group of K. In this paper, we shall study the case when G is a non-abelian 2-group.

Bachoc-Kwon [2] and Couture-Derhem [5] studied the case where K is a cyclic cubic field and G is the quaternion group of order 8. First we shall give an alternative proof of their result. This proof is based on the theory of embedding problems, which is applicable to more general cases. As an application, we shall prove the existence of unramified extensions over cyclic quintic fields with Galois group isomorphic to $32\Gamma_5 a_2$ under the condition that the class number is even. Our proof is also applicable to the Fontaine-Mazur-Boston Conjecture. This conjecture states that the pro-p group $\mathrm{Gal}(K^{(\infty)}(p)/K)$ is

Received April 2, 2002; received in final form June 16, 2002.
2000 *Mathematics Subject Classification.* 12F12, 11R29.

not powerful under the condition that it is infinite, where $K^{(\infty)}(p)$ is the maximal unramified p-extension of K. A pro-p group G is called powerful if p is odd and $G/\overline{G^p}$ is abelian, or if $p = 2$ and $G/\overline{G^4}$ is abelian. The main references for the Fontaine-Mazur-Boston Conjecture are [3], [4], and [8]. See also [6] for powerful pro-p groups.

We shall also prove that the Galois group $\mathrm{Gal}(K_+^{(\infty)}(2)/K)$ is not powerful under certain conditions, where $K_+^{(\infty)}(2)$ is the maximal unramified 2-extension in narrow sense.

2. Embedding problems

Let k be an algebraic number field of finite degree, and $\mathfrak{G}$ its absolute Galois group. Let L/k be a finite Galois extension with Galois group G, and $(\varepsilon) : 1 \to A \to E \xrightarrow{j} G \to 1$ a group extension with an abelian kernel A. Then an embedding problem $(L/k, \varepsilon)$ is defined by the diagram

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

where φ is the canonical surjection. A solution of the embedding problem $(L/k, \varepsilon)$ is, by definition, a continuous homomorphism ψ of $\mathfrak{G}$ to E satisfying the condition $j \circ \psi = \varphi$. A solution ψ is called a proper solution if it is surjective. We remark that the existence of a proper solution is equivalent to the existence of a Galois extension $M/L/k$ such that the canonical sequence $1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/k) \to \mathrm{Gal}(L/k) \to 1$ coincides with (ε). A main reference for embedding problems is [15].

In our previous papers [16], [17], [18], we studied the case when A is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ (p an odd prime), and proved the existence of certain unramified non-abelian p-extensions. In the present paper, we shall study the case when A is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and k is the rational number field $\mathbf{Q}$.

Our main theorem is the following.

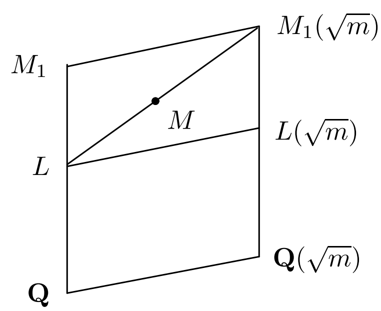
THEOREM 1. *Let $L/K/\mathbf{Q}$ be a Galois extension such that L/K is an unramified 2-extension and the degree $[K : \mathbf{Q}]$ is odd. Let $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$ be a non-split central extension. Then there exists a Galois extension $M/\mathbf{Q}$ such that*

(1) *$M/\mathbf{Q}$ gives a proper solution of $(L/\mathbf{Q}, \varepsilon)$, and*
(2) *M/L is unramified at all finite primes.*

REMARK 1. There does not always exist a non-split central extension $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$. The existence of such an extension is equivalent to the condition $\mathrm{H}^2(\mathrm{Gal}(L/\mathbf{Q}), \mathbf{Z}/2\mathbf{Z}) \neq 0$.

Proof of Theorem 1. By using the local-global theory of central embedding problems, we can prove that $(L/\mathbf{Q}, \varepsilon)$ has a solution and take a Galois extension $M_1/L/\mathbf{Q}$ corresponding to a proper solution such that any prime above 2 is unramified in M_1/L. This method is similar to [17, Theorem 8], so we omit details.

Let p_i $(i = 1, 2, \ldots, t)$ be all the primes of $\mathbf{Q}$ such that some primes of L lying above p_i are ramified in M_1/L. By the choice of M_1, p_i is odd for all i. Let $m = \pm p_1 p_2 \cdots p_t$, where the sign is determined by the condition $m \equiv 1 \pmod 4$. Then $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$ is unramified outside $\{p_1, \ldots, p_t\}$. Let M be the field such that $M_1(\sqrt{m}) \supsetneqq M \supsetneqq L$, $M \neq L(\sqrt{m})$, $M \neq M_1$.



Since the Galois group of $M_1(\sqrt{m})/L$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, M is uniquely determined.

Let $\mathfrak{P}_i$ be a prime of $M_1(\sqrt{m})$ lying above p_i, and $\mathfrak{p}_i$ the restriction of $\mathfrak{P}_i$ to L. Since $\mathfrak{p}_i$ is ramified in M_1/L and $L(\sqrt{m})/L$, the inertia field of $\mathfrak{P}_i$ in $M_1(\sqrt{m})/L$ is equal to M. Therefore M/L is unramified at all finite primes. Since (ε) is a central extension, M gives a proper solution of $(L/\mathbf{Q}, \varepsilon)$. We have thus proved the theorem. □

We can easily generalize Theorem 1 to the following.

THEOREM 2. *Let $L/K/\mathbf{Q}$ be a Galois extension such that L/K is a 2-extension and the degree $[K : \mathbf{Q}]$ is odd. Let $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$ be a non-split central extension and S_L a finite set of primes of L which contains all primes ramified in L/K and all infinite primes. Assume that $(L/\mathbf{Q}, \varepsilon)$ has a solution. Then there exists a Galois extension $M/\mathbf{Q}$ such that*

(1) *$M/\mathbf{Q}$ gives a proper solution of $(L/\mathbf{Q}, \varepsilon)$, and*
(2) *M/L is unramified outside S_L.*

3. Applications

As an application of Theorem 1, we study the existence of unramified non-abelian 2-extensions.

Proposition 3. *Let l be an odd prime such that the order of* 2 *mod* l *is even, and* K *an abelian* l*-extension over* $\mathbf{Q}$ *with even class number. Then there exists a Galois extension* M/K *such that the Galois group is a non-abelian* 2*-group and* M/K *is unramified at all finite primes.*

For the proof, we need some lemmas.

Let l be an odd prime and f the order of 2 mod l. For each positive integer i, denote by f_i the order of 2 mod l^i.

Lemma 4 ([17, Proposition 6]). *Let $L/K/k$ be a Galois extension satisfying the following conditions:*

(1) *K/k is an abelian l-extension;*
(2) *L/K is an elementary abelian 2-extension;*
(3) *there is no Galois extension L_1/k such that $L \supsetneqq L_1 \supsetneqq K$.*

Let l^e be the exponent of the group $\mathrm{Gal}(K/k)$*. Then the* 2*-rank of* $\mathrm{Gal}(L/K)$ *is equal to one of* $1, f_1, f_2, \ldots, f_e$*. If L/K is a quadratic extension, then* $\mathrm{Gal}(L/k)$ *is isomorphic to the direct product of* $\mathrm{Gal}(K/k)$ *and* $\mathrm{Gal}(L/K)$*.*

Remark 2. In [17, Proposition 6] we assumed that p is an odd prime, but the proof is applicable to the case $p = 2$.

Lemma 5. *Let G be a split extension of an abelian* 2*-group A by an l-group B. Assume that f is even and the* 2*-rank of A is fn for some odd integer n. Then the cohomology group* $\mathrm{H}^2(G, \mathbf{Z}/2\mathbf{Z})$ *is non-trivial.*

Proof. By Hall's theorem on the decomposition of cohomology groups,

$$\mathrm{H}^2(G, \mathbf{Z}/2\mathbf{Z}) \cong \mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z})^B \oplus \mathrm{H}^2(B, (\mathbf{Z}/2\mathbf{Z})^A)$$

(cf. Babakhanian [1, 55.1]). Since the order of B is odd, $\mathrm{H}^2(B, (\mathbf{Z}/2\mathbf{Z})^A) = 0$. Therefore

$$\mathrm{H}^2(G, \mathbf{Z}/2\mathbf{Z}) \cong \mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z})^B.$$

Since the 2-rank of A is fn,

$$\mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z}) \cong (\mathbf{Z}/2\mathbf{Z})^{fn(fn+1)/2}.$$

By the assumption that f is even, $fn(fn+1)/2$ is not divisible by f. Hence

$$(**) \qquad 2^{fn(fn+1)/2} \not\equiv 1 \pmod{l}.$$

We consider the orbit decomposition with respect to the action of B to $\mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z})$,

$$\mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z})^B \cup B \cdot t_1 \cup \cdots \cup B \cdot t_m,$$

where the cardinality of $B \cdot t_i$ is divisible by l.

By using $(**)$, we have $\mathrm{H}^2(A, \mathbf{Z}/2\mathbf{Z})^B \neq 0$. This completes the proof of Lemma 5. □

LEMMA 6 ([7, Theorem 2.3]). *Let A be a p'-group of automorphisms of the abelian p-group P. Let $C_P(A) = \{x \in P | x^a = x \text{ for all } a \in A\}$, and let $[P, A]$ be the subgroup of P generated by all elements $x^a x^{-1} (a \in A, x \in P)$. Then $P = C_P(A) \times [P, A]$.*

Proof of Proposition 3. Let K_1/K be an unramified quadratic extension, and $\widetilde{K_1}$ the Galois closure of $K_1/\mathbf{Q}$. Then $\widetilde{K_1}/K$ is an elementary abelian 2-extension. We take a Galois extension $L/K/\mathbf{Q}$ satisfying the following conditions:

(1) L/K is an elementary abelian 2-extension;
(2) there is no Galois extension $L_1/\mathbf{Q}$ such that $L \supsetneqq L_1 \supsetneqq K$.

By Lemma 4, the 2-rank of $\mathrm{Gal}(L/K)$ is equal to one of $f_1, f_2, \ldots, f_e$. It is easy to see that $f_j = fl^r$ for some non-negative integer r. Then, by virtue of Lemma 5, $\mathrm{H}^2(\mathrm{Gal}(L/\mathbf{Q}), \mathbf{Z}/2\mathbf{Z})$ is non-trivial. Hence there exists a non-split central extension $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$. By Theorem 1, there exists a Galois extension $M/L/\mathbf{Q}$ such that M/L is unramified at all finite primes and $\mathrm{Gal}(M/\mathbf{Q})$ is isomorphic to E.

We claim that M/K is a non-abelian extension. Assume that M/K is abelian. Since $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathrm{Gal}(M/K)$, we can regard $\mathrm{Gal}(K/\mathbf{Q})$ as a group of automorphisms of $\mathrm{Gal}(M/K)$. By Lemma 6,

$$\mathrm{Gal}(M/K) \cong C_{\mathrm{Gal}(M/K)}(\mathrm{Gal}(K/\mathbf{Q})) \times [\mathrm{Gal}(M/K), \mathrm{Gal}(K/\mathbf{Q})].$$

Since

$$1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/\mathbf{Q}) \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$$

is a non-split central extension, $\mathrm{Gal}(M/K) \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \cdots \times \mathbf{Z}/2\mathbf{Z}$ and $C_{\mathrm{Gal}(M/K)}(\mathrm{Gal}(K/\mathbf{Q})) = \mathrm{Gal}(M/L) \cong \mathbf{Z}/2\mathbf{Z}$. It is easy to see that the exponent of $[\mathrm{Gal}(K/\mathbf{Q}), \mathrm{Gal}(M/K)]$ is two. Therefore the exponent of $C_{\mathrm{Gal}(M/K)}(\mathrm{Gal}(K/\mathbf{Q})) \times [\mathrm{Gal}(M/K), \mathrm{Gal}(K/\mathbf{Q})]$ is also two. On the other hand, the exponent of $\mathrm{Gal}(M/K)$ is four. This is a contradiction.

Hence M/K is non-abelian, which is a required extension. This concludes the proof. □

In the following, we shall study the case when K is a cyclic field.

Let $\mathcal{Q}$ be the quaternion group given by the presentation $\langle \sigma, \ \tau \mid \sigma^4 = 1, \ \tau^2 = \sigma^2, \ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$.

The following proposition was first proved by Bachoc–Kwon [2] and Couture–Derhem [5]. The proof in [2] is more explicit, and we can find there some numerical examples of defining equations. Here we shall give another approach to this proposition, which is applicable to more general cases.

PROPOSITION 7. *Let K be a cyclic cubic field with even class number. Then there exists a Galois extension M/K such that the Galois group is isomorphic to $\mathcal{Q}$ and M/K is unramified at all finite primes.*

Proof. Let K_1/K be an unramified quadratic extension. Suppose that $K_1/\mathbf{Q}$ is Galois. Since the group of order 6 having a normal subgroup of order 2 is abelian, there exists an unramified 2-extension over $\mathbf{Q}$. This contradicts the fact that the class number of $\mathbf{Q}$ is 1. Hence $K_1/\mathbf{Q}$ is non-Galois. We denote by L the Galois closure of $K_1/\mathbf{Q}$. By Lemma 4, $\mathrm{Gal}(L/K)$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. (See also [12] and [20].) Then $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to $A_4 \cong PSL(2,3)$. The canonical sequence $1 \to \mathbf{Z}/2\mathbf{Z} \to SL(2,3) \to PSL(2,3) \to 1$ is a non-split central extension. By Theorem 1, there exists a Galois extension $M/\mathbf{Q}$ such that $\mathrm{Gal}(M/\mathbf{Q})$ is isomorphic to $SL(2,3)$ and M/L is unramified at all finite primes. The unique Sylow subgroup of E is isomorphic to $\mathcal{Q}$ and the fixed field of $\mathcal{Q}$ is equal to K. This completes the proof of Proposition 6. □

Remark 3. The class number of Galois fields of this type was studied well in [14]. Unramified quaternion extensions of quadratic fields were studied by many authors; see, for example, [10] and [13].

Proposition 8. *Let K be a cyclic quintic field with even class number. Then there exists a Galois extension M/K such that the Galois group is isomorphic to*

$$32\Gamma_5 a_2 = \left\langle a, b, c, d \;\middle|\; \begin{array}{l} d^2 = 1, a^2 = b^2 = c^2 = [b,c] = [a,d], \\ [a,b] = [a,c] = [b,d] = [c,d] = 1 \end{array} \right\rangle$$

and M/K is unramified at all finite primes.

Proof. The order of 2 mod 5 is 4. Then, by Lemma 4, there exists a Galois extension $L/K/\mathbf{Q}$ such that $\mathrm{Gal}(L/K) \cong (\mathbf{Z}/2\mathbf{Z})^4$ and L/K is unramified. By Lemma 5, we can take a non-split central extension $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$. By virtue of Theorem 1, there exists a Galois extension $M/\mathbf{Q}$ such that $\mathrm{Gal}(M/\mathbf{Q}) \cong E$ and M/K is unramified at all finite primes. Let H be the unique 2-Sylow subgroup of E. Then H satisfies the following conditions:

(1) the order of H is 32;
(2) the 2-rank of H is 4;
(3) H has an automorphism of order 5.

Assume that H is abelian. Then H is isomorphic to $\mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^3$, and the order of $\mathrm{Aut}(H)$ is $21504 = 2^{10} \cdot 3 \cdot 7$. This contradicts condition (3). Thus H is non-abelian. The non-abelian group satisfying the above conditions (1)–(3) is unique and isomorphic to $32\Gamma_5 a_2$ (cf. [9] and [19]). This completes the proof. □

Example. In [11], we can find a table of class numbers of quintic fields. For example:

conductor	941	1771	3091	3931	23411	31861
class number	2^4	$2^4 \cdot 5$	$2^4 \cdot 5$	2^8	$2^4 \cdot 5^3$	$2^4 \cdot 5 \cdot 11^2$

Corollary 9. *Let l be an odd prime such that the order of 2 mod l is even, and let K be an abelian l-extension over $\mathbf{Q}$. Assume that the class number of K is even. Then the Galois group $\mathrm{Gal}(K_+^{(\infty)}(2)/K)$ is not powerful.*

Proof. By Proposition 3 and its proof, there exists a Galois extension $M/L/K$ satisfying the following conditions:

(1) M/K is unramified at all finite primes;
(2) $\mathrm{Gal}(M/K)$ is a non-abelian 2-group;
(3) $\mathrm{Gal}(L/K)$ is an elementary abelian 2-group;
(4) M/L is a quadratic extension.

Then the exponent of $\mathrm{Gal}(M/K)$ is four. Hence $\mathrm{Gal}(M/K)$ is not powerful. Since quotient groups of powerful groups are also powerful, $\mathrm{Gal}(K_+^{(\infty)}(2)/K)$ is not powerful. This completes the proof. □

Acknowledgement. I should like to express my gratitude to Professor Ken Yamamura for his useful advice.

References

[1] A. Babakhanian, *Cohomological methods in group theory*, Dekker, New York, 1972.

[2] C. Bachoc and S. H. Kwon, *Sur les extensions de group de Galois $\widetilde{A}_4$*, Acta Arith. **62** (1992), 1–10.

[3] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory **42** (1992), 285–291.

[4] ———, *Some cases of the Fontaine-Mazur conjecture II*, J. Number Theory **75** (1999), 161–169.

[5] R. Couture and A. Derhem, *Un problème de capitulation*, C. R. Acad. Sci. Paris **314** (1992), 785–788.

[6] J. Dixon, M. P.F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, London Math. Soc. Lecture Note Series, vol. 157, Cambridge Univ. Press, Cambridge, 1991.

[7] D. Gorenstein, *Finite groups*, Chelsea, New York, 1980.

[8] F. Hajir, *On the growth of p-class groups in p-class field towers*, J. Algebra **188** (1996), 256–271.

[9] M. Hall and J. K. Senior, *The groups of order $2^n (n \leq 6)$*, Macmillan, New York, 1964.

[10] M. Horie, *On central extensions of elementary abelian fields*, J. Number Theory **36** (1990), 95–107.

[11] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer*, J. Théor. Nombres Bordeaux **8** (1996), 75–92.

[12] T. Komatsu and S. Nakano, *On the Galois module structure of ideal class groups*, Nagoya Math. J. **164** (2001), 133–146.

[13] F. Lemmermeyer, *Unramified quaterinon extensions of quadratic number fields*, J. Théor. Nombres Bordeaux **9** (1997), 51–68.

[14] F. Lemmermeyer, S. Louboutin, and R. Okazaki, *The class number one problem for some non-abelian normal CM-fields of degree 24*, J. Théor. Nombres Bordeaux **11** (1999), 387–406.

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

[16] A. Nomura, *On the existence of unramified p-extensions*, Osaka J. Math. **28** (1991), 55–62.

[17] ______, *On the class numbers of certain Hilbert class fields*, Manuscripta Math. **79** (1993), 379–390.

[18] ______, *On embedding problems with restricted ramifications*, Arch. Math. **73** (1999), 199–204.

[19] T. W. Sag and J. W. Wamsley, *Minimal presentations for groups of order* $2^n, n \leq 6$, J. Austral. Math. Soc. **15**(1973), 461–469.

[20] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

Department of Mathematics, Kanazawa University, Kanazawa 920-1192, Japan
E-mail address: anomura@t.kanazawa-u.ac.jp