TOKYO J. MATH.
VOL. 37, NO. 1, 2014

Some Remarks on the Existence of Certain Unramified p-extensions

Akito NOMURA

Kanazawa University

(Communicated by M. Kurihara)

Abstract. We study the inverse Galois problem with restricted ramifications. Let p and q be distinct odd primes. Let E be a non-abelian p-group of order p^3, and let k be a cyclic extension over $\mathbf{Q}$ of degree q. In this paper, we study the existence of unramified extensions over k with the Galois group E.

1. Introduction

Let k be an algebraic number field. Let p be a prime number and G a p-group. Whether there is an unramified Galois extension over k with the Galois group G is an interesting problem in algebraic number theory. In the case when G is an abelian group, by class field theory, this problem is closely related to the ideal class group of k. Bachoc-Kwon[1] and Couture-Derhem[3] studied the case when k is a cyclic cubic field and G is the quaternion group of order 8. The author[10] studied the case when k is a cyclic quintic field and G is a certain non-abelian 2-group of order 32. For an odd prime p, let E_1 be the non-abelian group of order p^3 such that the exponent is equal to p. In [8], the author studied the case when k is a quadratic field and $G = E_1$. Lemmermeyer[6] generalized this result to quadratic extensions over any number field.

Let p and q be distinct odd primes such that $p \equiv -1 \bmod q$. Let E be a non-abelian p-group of order p^3, and let k be a cyclic extension over $\mathbf{Q}$ of degree q. In this paper, we shall study the existence of unramified extensions over k with the Galois group E.

In this paper, we call a field extension $L/K/F$ is a Galois extension if L/F and K/F are Galois extensions.

Received November 7, 2012; revised May 13, 2013
Mathematics Subject Classification: 12F12
Key words and phrases: Inverse Galois problem, unramified extensions, class numbers
Supported by Grand-in-Aid for Scientific Research (C) No. 23540010, Japan Society for the Promotion of Science

2. Preliminary from group theory and embedding problems

We shall focus on some groups. Let p and q be distinct odd primes such that $p \equiv -1 \mod q$. Let

$$E_1 = \langle x, y, z \mid x^p = y^p = z^p = 1,\ xy = yx,\ xz = zx,\ z^{-1}yz = xy \rangle ,$$
$$E_2 = \left\langle x, y \mid x^{p^2} = y^p = 1,\ y^{-1}xy = x^{1+p} \right\rangle .$$

These groups are non-abelian p-groups of order p^3. The exponent of E_1 is p, and the exponent of E_2 is p^2.

Let t be a primitive root in $\mathbf{F}_{p^2}$ of the congruence $t^q \equiv 1 \mod p$, where $\mathbf{F}_{p^2}$ is the finite field with p^2 elements. Since $t^p + t$ is fixed by the action of $\mathrm{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$, $t^p + t$ is contained in $\mathbf{F}_p$. Let

$$\Gamma_0 = \left\langle x, y, w \mid x^p = y^p = w^q = 1,\ xy = yx,\ w^{-1}xw = y,\ w^{-1}yw = x^{-1}y^{t^p+t} \right\rangle ,$$
$$\Gamma_1 = \left\langle x, y, z, w \;\middle|\; \begin{array}{l} x^p = y^p = z^p = w^q = 1,\ xz = zx,\ yz = zy,\ zw = wz \\ y^{-1}xy = zx,\ w^{-1}xw = y,\ w^{-1}yw = x^{-1}y^{t^p+t} \end{array} \right\rangle .$$

For these two groups, we refer Burnside [2] and Western [11]. We shall describe some lemmas which will be needed below.

LEMMA 1 ([2, §59]). *Let p and q be odd primes such that $p \equiv -1 \mod q$, and let G be a finite group. Assume that G satisfies the conditions*:

(1) *The order of G is equal to p^2q.*

(2) *G has a normal subgroup which is isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.*

(3) *G does not have a normal subgroup of order q.*

Then G is isomorphic to Γ_0.

We denote by $Aut(G)$ the automorphism group of a finite group G.

LEMMA 2 ([12, Theorem 1]). *The order of the group $Aut(E_2)$ is $p^3(p-1)$.*

LEMMA 3 ([9, Theorem 8]). *Let p be an odd prime. Assume that the Galois extension $K/k/\mathbf{Q}$ satisfies the conditions*:

(1) *The degree $[k : \mathbf{Q}]$ is prime to p.*

(2) *K/k is an unramified p-extension.*

Let $(\varepsilon) : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(K/\mathbf{Q}) \to 1$ be a non-split central extension. Then there exists a Galois extension $L/K/\mathbf{Q}$ such that

(i) $1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) \to 1$ *coincides with (ε), and*

(ii) *L/K is unramified.*

The following lemma is well-known. See for example Metsänkylä [7].

LEMMA 4. *Let p and q be distinct odd primes, and ζ_q a primitive q-th root of unity. Let $G = \langle\sigma\rangle$ be the cyclic group of order q. We consider $\mathbf{Z}[\zeta_q]$ as G-module by $\sigma x = \zeta_q x$. Then the irreducible decomposition of $\mathbf{F}_p[G]$ as G-module is*

$$\mathbf{F}_p[G] \cong \mathbf{F}_p \oplus \bigoplus_{i=1}^{g} \mathbf{Z}[\zeta_q]/\mathfrak{p}_i\mathbf{Z}[\zeta_q]$$

where the $\mathfrak{p}_i$ are prime ideals defined by $p\mathbf{Z}[\zeta_q] = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_g$, and $\mathbf{F}_p$ is the finite field with p elements.

3. Theorems and the proofs

Let p and q be distinct odd primes, and let $k/\mathbf{Q}$ be a cyclic extension of degree q.

THEOREM 1. *Let p and q be odd primes such that $p \equiv -1 \mod q$. Assume that the class number of k is divisible by p. Then there exists a Galois extension $L/k/\mathbf{Q}$ such that*

(1) *L/k is an unramified extension, and*

(2) $\mathrm{Gal}(L/k)$ *is isomorphic to E_1 which is defined in the section* 2.

PROOF. By the assumption of the class number of k, there exists an unramified cyclic extension k_1/k of degree p. Let K_1 be the Galois closure of $k_1/\mathbf{Q}$. Then $\mathrm{Gal}(K_1/k)$ is an elementary abelian p-group, and $\mathrm{Gal}(k/\mathbf{Q})$ acts naturally on the group $\mathrm{Gal}(K_1/k)$. Let $\mathfrak{p}_i$ are prime ideals defined by $p\mathbf{Z}[\zeta_q] = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_g$. Since the order of $p \bmod q$ is 2, $\mathbf{Z}[\zeta_q]/\mathfrak{p}_i\mathbf{Z}[\zeta_q] \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. By Lemma 4, the p-rank of any irreducible $\mathbf{F}_p[G]$-module with non-trivial action is equal to 2. Then there exists a Galois extension $K/k/\mathbf{Q}$ such that K/k is unramified and that $\mathrm{Gal}(K/k) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. We claim that K has no subfield N such that $N/\mathbf{Q}$ is Galois and that $[K : N] = q$. Indeed, let $K/N/\mathbf{Q}$ be a Galois extension such that $[K : N] = q$. Then, by considering the ramification index in $N/\mathbf{Q}$, we see that $N/\mathbf{Q}$ is an unramified extension. This is a contradiction. Therefore $\mathrm{Gal}(K/\mathbf{Q})$ satisfies the conditions (1)(2)(3) in Lemma 1. Hence $\mathrm{Gal}(K/\mathbf{Q}) \cong \Gamma_0$ by Lemma 1.

Let C be the center of Γ_1, then C is a cyclic group of order p generated by z. Let $j : \Gamma_1 \to \Gamma_0$ be the homomorphism defined by $x \mapsto x, y \mapsto y, w \mapsto w, z \mapsto 1$, then j induces the isomorphism $\Gamma_1/C \cong \Gamma_0$. Then there exists a central extension $1 \to \mathbf{Z}/p\mathbf{Z} \to \Gamma_1 \to \mathrm{Gal}(K/\mathbf{Q}) \to 1$. Since Γ_1 is not isomorphic to the direct product $\Gamma_0 \times \mathbf{Z}/p\mathbf{Z}$, this exact sequence is non-split. By Lemma 3, there exists a Galois extension $L/K/\mathbf{Q}$ such that $\mathrm{Gal}(L/\mathbf{Q}) \cong \Gamma_1$ and that L/K is unramified. Since the p-Sylow subgroup of Γ_1 is isomorphic to E_1, $\mathrm{Gal}(L/k)$ is isomorphic to E_1. Therefore L/k is a required extension. This proves the theorem. □

REMARK 1. Assume that $k/\mathbf{Q}$ satisfies the same conditions of Theorem 1. By the proof of Theorem 1, we obtained the following. Let $K/k/\mathbf{Q}$ be a Galois extension such that K/k is unramified and that $\mathrm{Gal}(K/k) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Then there exists a Galois extension $L/K/k$ such that L/k is unramified and that $\mathrm{Gal}(L/k) \cong E_1$.

THEOREM 2. *Assume that* $p \not\equiv 1 \mod q$. *Then there exists no Galois extension* $L/k/\mathbf{Q}$ *such that* L/k *is unramified and* $\mathrm{Gal}(L/k) \cong E_2$.

PROOF. Assume that there exists a such Galois extension $L/k/\mathbf{Q}$. Let $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$ and $E = \mathrm{Gal}(L/k)$. Then E is isomorphic to E_2. Since the order of Γ is p^3q, there exists a non-trivial element τ of Γ such that $\tau^q = 1$. Let $\theta_\tau(x) = \tau^{-1}x\tau$ $(x \in E)$. Since E is a normal subgroup of Γ, θ_τ is an automorphism of E. Since $(\theta_\tau)^q(x) = \tau^{-q}x\tau^q = x$, then $(\theta_\tau)^q = 1$. By Lemma 2 and the assumption $p \not\equiv 1 \mod q$, there is no automorphism of E of order q. Hence, $\theta_\tau = 1$. Then $\tau^{-1}x\tau = x$ for all x in E. Since $\Gamma = \langle E, \tau\rangle$, then $\langle\tau\rangle$ is a normal subgroup of Γ. Hence the fixed field of $\langle\tau\rangle$ in L is an unramified Galois extension over $\mathbf{Q}$. This is a contradiction. □

We denote by $Cl(k)$ the ideal class group of k. We also denote by $exp(G)$ the exponent of the group G.

THEOREM 3. *Assume that* $p \equiv -1 \mod q$ *and the* p*-rank of* $Cl(k)$ *is equal to* 2. *Then the following two conditions are equivalent.*

(1) $Cl(k)$ *has an element of order* p^2.

(2) *There exists an unramified Galois extension* L/k *such that* $\mathrm{Gal}(L/k) \cong E_2$.

PROOF. At first, we show that the assertion (1) implies (2). By the assumption p-rank $Cl(k) = 2$, there exists an unramified Galois extension K/k such that K is a Galois extension over $\mathbf{Q}$ and that $\mathrm{Gal}(K/k) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. By Theorem 1 and the Remark, there exists a Galois extension $L_1/K/k$ such that L_1/k is unramified and that $\mathrm{Gal}(L_1/k) \cong E_1$. On the other hand, by the condition (1), $Cl(k)$ has a subgroup isomorphic to $\mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Then there exists a Galois extension $L_2/K/k$ such that L_2/k is unramified and that $\mathrm{Gal}(L_2/k) \cong \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

Let $M = L_1L_2$, then M/k is a p-extension. Let L_3 be a subfield of M satisfying the conditions: (i) $L_3 \supset K$ and $[L_3 : K] = p$, (ii) $L_3 \neq L_i (i = 1, 2)$. Since $\mathrm{Gal}(M/L_i)(i = 1, 2)$ are normal subgroups of $\mathrm{Gal}(M/k)$ of order p, $\mathrm{Gal}(M/L_i)$ are contained in the center of $\mathrm{Gal}(M/k)$. Then $\mathrm{Gal}(M/K)$ is contained in the center of $\mathrm{Gal}(M/k)$. Hence $\mathrm{Gal}(M/L_3)$ is a normal subgroup of $\mathrm{Gal}(M/k)$ and L_3/k is an unramified Galois extension. Since L_2/k is an abelian extension and M/k is a non-abelian extension, then L_3/k is a non-abelian extension. We remark that $\mathrm{Gal}(M/k)$ is isomorphic to a subgroup of the direct product $\mathrm{Gal}(L_1/k) \times \mathrm{Gal}(L_2/k)$. Since $exp(\mathrm{Gal}(L_1/k)) = p$ and $exp(\mathrm{Gal}(L_2/k)) = p^2$, then $exp(\mathrm{Gal}(M/k)) = p$ or p^2. On the other hand, $\mathrm{Gal}(L_2/k)$ is isomorphic to a factor group of $\mathrm{Gal}(M/k)$. Therefore $exp(\mathrm{Gal}(M/k)) = p^2$. Since $\mathrm{Gal}(M/k)$ is isomorphic to a subgroup of $\mathrm{Gal}(L_1/k) \times \mathrm{Gal}(L_3/k)$ and $exp(\mathrm{Gal}(L_1/k)) = p$, then $exp(\mathrm{Gal}(L_3/k)) = p^2$. Thus $\mathrm{Gal}(L_3/k)$ is a non-abelian p-group such that the order is equal to p^3 and that $exp(\mathrm{Gal}(L_3/k)) = p^2$. Hence $\mathrm{Gal}(L_3/k)$ is isomorphic to E_2.

Next, we show that the assertion (2) implies (1). By Theorem 1, there exists a Galois extension $L_1/K/k$ such that L_1/k is unramified and that $\mathrm{Gal}(L_1/k) \cong E_1$. By the assumption, there exists a Galois extension $L_2/K/k$ such that L_2/k is unramified and that $\mathrm{Gal}(L_2/k) \cong E_2$. Let $M = L_1L_2$ and $G_M = \mathrm{Gal}(M/k)$. Let C_M be the center of G_M, and $[G_M, G_M]$ the commutator subgroup of G_M. Since $\mathrm{Gal}(M/L_i)(i = 1, 2)$ are contained in C_M, $\mathrm{Gal}(M/K) \subset C_M \subset G_M$.

We claim that $C_M = \mathrm{Gal}(M/K)$. Indeed, if $\mathrm{Gal}(M/K) \subsetneq C_M$, then G_M/C_M is a cyclic group. Therefore G_M is abelian. This is a contradiction.

Let K^* be the subfield of M corresponding to the group $C_M \cap [G_M, G_M]$. It is well known that $C_M \cap [G_M, G_M]$ is isomorphic to a quotient group of the Schur multiplier of G_M/C_M. (See for example Karpilovsky[5, Proposition 2.1.7] or Furuta[4].) The Schur multiplier of the group $G_M/C_M \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Since K/k is abelian, then $[G_M, G_M]$ is contained in $C_M = \mathrm{Gal}(M/K)$. Since M/k is non-abelian, then $[G_M, G_M] = C_M \cap [G_M, G_M] \cong \mathbf{Z}/p\mathbf{Z}$. Hence $[M : K^*] = p$, and $\mathrm{Gal}(K^*/k) \cong \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. □

COROLLARY 1. *Assume that $p \not\equiv 1 \mod q$. If L/k is an unramified Galois extension such that* $\mathrm{Gal}(L/k) \cong E_2$, *then the class number of L is divisible by p.*

PROOF. Let $\hat{k}$ be the maximal unramified p-extension of k. Then $\hat{k}/\mathbf{Q}$ is a Galois extension and $L \subset \hat{k}$. By Theorem 2, $L/\mathbf{Q}$ is not a Galois extension. Then $L \subsetneq \hat{k}$, and the class number of L is divisible by p. □

ACKNOWLEDGMENT. The author should like to express my gratitude to Professor Katsushi Waki for his useful advice about automorphism groups of p-groups. The author also thanks the referee for her/his careful reading and for her/his advice.

References

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

[2] W. BURNSIDE, *Theory of groups of finite order*, Cambridge University Press, 1911.

[3] R. COUTURE and A. DERHEM, Un problème de capitulation, C. R. Acad. Sci. Paris **314** (1992), 785–788.

[4] Y. FURUTA, Supplementary notes on Galois groups of central extensions of algebraic number fields, Science Reports of Kanazawa Univ. **29** (1984), 9–14. (Kanazawa University Repository for Academic resources, http://hdl.handle.net/2297/10540)

[5] G. KARPILOVSKY, *The Schur multiplier*, London Mathematical Society Monographs New Series 2, Oxford Science Publications, 1987.

[6] F. LEMMERMEYER, Class groups of dihedral extensions, Math. Nachr. **278** (2005), 679–691.

[7] T. METSÄNKYLÄ, On the history of the study of ideal class groups, Expo. Math. **25** (2007), 325–340.

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

[9] A. NOMURA, On the class number of certain Hilbert class fields, Manuscripta Math. **79** (1993), 379–390.

[10] A. NOMURA, Notes on the existence of certain unramified 2-extensions, Illinois J. Math. **46** (2002), 1279–1286.

[11] A. E. WESTERN, Groups of order p^3q, Proc. London Math. Soc. Ser.1, **30** (1899), 209–263.

[12] D. L. WINTER, The automorphism group of an extraspecial p-group, Rocky Mountain J. Math. **2** (1972), 159–168.

Present Address:
INSTITUTE OF SCIENCE AND ENGINEERING,
KANAZAWA UNIVERSITY,
KAKUMA-MACHI, KANAZAWA, 920–1192 JAPAN.
e-mail: nomura@se.kanazawa-u.ac.jp