Notes on the existence of unramified non-abelian p-extensions over cyclic fields

By Akito NOMURA

Institute of Science and Engineering, Kanazawa University, Kakuma-machi, Kanazawa 920-1192, Japan

(Communicated by Masaki KASHIWARA, M.J.A., March 12, 2014)

Abstract: We study the inverse Galois problem with restricted ramifications. Let p and q be distinct odd primes such that $p \equiv 1 \bmod q$. Let $E(p^3)$ be the non-abelian group of order p^3 such that the exponent is equal to p, 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 $E(p^3)$. We also give some numerical examples computed with PARI.

Key words: Unramified p-extension; inverse Galois problem; ideal class group; cyclic cubic field.

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. 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 [8] 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 $E(p^3)$ be the non-abelian group of order p^3 such that the exponent is equal to p. In [6], the author studied the case when k is a quadratic field and $G = E(p^3)$. Let p and q be distinct odd primes and $k/\mathbf{Q}$ a cyclic extension of degree q. The author [9] studied the case when $p \equiv -1 \bmod q$ and $G = E(p^3)$. In this paper, we shall study the case when $p \equiv 1 \bmod q$ and $G = E(p^3)$.

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

2. Some lemmas. We shall describe some lemmas which will be needed below.

Lemma 1 ([7, 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 $(\epsilon) : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(K/\mathbf{Q}) \to 1$ 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.*

Since the multiplicative group $\mathbf{F}_p^*$ contains a primitive $(p-1)$-th root of unity, it is easy to see the following lemma.

Lemma 2. *Let p and q be odd primes such that $p \equiv 1 \bmod q$. Let G be the cyclic group of order q. Then the p-rank of any irreducible $\mathbf{F}_p[G]$-module is equal to 1.*

3. Main theorem. Let p and q be odd primes such that $p \equiv 1 \bmod q$. Let $k/\mathbf{Q}$ be a cyclic extension of degree q, and $Cl(k)$ the ideal class group of k. Let $M_k = Cl(k)/Cl(k)^p$ and $G = \mathrm{Gal}(k/\mathbf{Q})$, then M_k is a $\mathbf{F}_p[G]$-module in a natural sense. Let σ be a generator of G. For $1 \leqq j \leqq p-1$, we put $M_k(j) := \{c \in M_k \mid c^\sigma = c^j\}$.

It is easy to see that if $j^q \not\equiv 1 \bmod p$ then $M_k(j) = \{1\}$. Since the class number of $\mathbf{Q}$ is 1, $M_k(1) = \{1\}$.

We shall focus on some groups. Let

$$E(p^3) = \left\langle x, y, z \;\middle|\; \begin{array}{l} x^p = y^p = z^p = 1,\ xy = yx, \\ xz = zx,\ z^{-1}yz = xy \end{array} \right\rangle.$$

This group is a non-abelian p-group of order p^3 such that the exponent is p.

Let t be a primitive q-th root of the congruence $t^q \equiv 1 \bmod p$. Let

$$\Gamma_0 = \left\langle x, y, w \;\middle|\; \begin{array}{l} x^p = y^p = w^q = 1,\ xy = yx, \\ w^{-1}xw = x^t,\ w^{-1}yw = y^{t^{q-1}} \end{array} \right\rangle,$$

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

2010 Mathematics Subject Classification. Primary 12F12; Secondary 11R16, 11R29.

doi: 10.3792/pjaa.90.67

These groups are independent of t. The center of Γ_1 is the cyclic group of order p generated by z. Let $j:\Gamma_1\to\Gamma_0$ be the homomorphism defined by $x\mapsto x, y\mapsto y, z\mapsto 1, w\mapsto w$. Then j induces a non-split central extension $1\to\mathbf{Z}/p\mathbf{Z}\to\Gamma_1\to\Gamma_0\to 1$. Further, the p-Sylow subgroup of Γ_1 is isomorphic to $E(p^3)$.

For these two groups, we refer Burnside [2] and Western [13].

Theorem 3. *Let p and q be odd primes such that $p\equiv 1 \bmod q$, and let $k/\mathbf{Q}$ be a cyclic extension of degree q. Assume that there exist integers α and β satisfying the following conditions:*

(1) $1<\alpha\leqq p-1,\ 1<\beta\leqq p-1$,

(2) $\alpha^q\equiv 1 \bmod p,\ \alpha\beta\equiv 1 \bmod p$,

(3) $M_k(\alpha)\neq\{1\},\ M_k(\beta)\neq\{1\}$.

Then there exists a Galois extension $L/k/\mathbf{Q}$ such that

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

(ii) $\mathrm{Gal}(L/k)$ *is isomorphic to* $E(p^3)$.

Proof. By the assumption (3) and Lemma 2, there exist Galois extensions $k_\alpha/k/\mathbf{Q}$ and $k_\beta/k/\mathbf{Q}$ satisfying the conditions: (a) k_α/k and k_β/k are unramified cyclic extensions of degree p, (b) $\mathrm{Gal}(k_\alpha/\mathbf{Q})$ and $\mathrm{Gal}(k_\beta/\mathbf{Q})$ are isomorphic to $\langle x,w|x^p=w^q=1,w^{-1}xw=x^\alpha\rangle$ and $\langle y,w|y^p=w^q=1,w^{-1}yw=y^\beta\rangle$, respectively. Let $K=k_\alpha k_\beta$. By the assumptions (1) and (2), α is a primitive q-th root of the congruence $\alpha^q\equiv 1 \bmod p$. Then $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to Γ_0. As mentioned above, there exists a non-split central extension $1\to\mathbf{Z}/p\mathbf{Z}\to\Gamma_1\to\mathrm{Gal}(K/\mathbf{Q})\to 1$. By Lemma 1, 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 $E(p^3)$, $\mathrm{Gal}(L/k)\cong E(p^3)$. Therefore $L/k/\mathbf{Q}$ is a required extension. □

Remark 4. Let k be a cyclic cubic field, and p an odd prime such that $p\equiv 1 \bmod 3$. Let $k(p)$ be the Hilbert p-class field of k. Miyake [5] studied the p-rank of the ideal class group $Cl(k(p))$ and the action of $\mathrm{Gal}(k/\mathbf{Q})$ on $Cl(k(p))$. Theorem 4 is a generalization of a part of Miyake's results in [5].

Let $E'(p^3)$ be the non-abelian group of order p^3 such that the exponent is equal to p^2. The following proposition is a generalization of [9, Theorem 3]. These proofs are essentially same. For the convenience of the reader, we give a sketch of the proof. We denote by $[G,G]$ the commutator subgroup of G.

Proposition 5. *Let p be an odd prime and k an algebraic number field of finite degree such that the p-rank of $Cl(k)$ is equal to 2. Assume that there exists an unramified Galois extension L_1/k such that $\mathrm{Gal}(L_1/k)\cong E(p^3)$. 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 $\mathrm{Gal}(L/k)\cong E'(p^3)$.*

Sketch of the proof. First, we show that the assertion (1) implies (2). 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 an unramified Galois extension L_2/k such that $\mathrm{Gal}(L_2/k)\cong\mathbf{Z}/p^2\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}$. □

Let $M=L_1L_2$ and $K=L_1\cap L_2$, then M/k is a p-extension and $\mathrm{Gal}(K/k)\cong\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}$. Let L_3 be a subfield of M satisfying the conditions: (i) $L_3\supset K$ and $[L_3:K]=p$, (ii) $L_3\neq L_i (i=1,2)$. Then L_3/k is an unramified Galois extension. We see that L_3/k is a non-abelian extension of degree p^3 and that the exponent of $\mathrm{Gal}(L_3/k)$ is equal to p^2. Hence $\mathrm{Gal}(L_3/k)$ is isomorphic to $E'(p^3)$.

Next, we show that the assertion (2) implies (1). By the assumption, there exists an unramified Galois extension L_2/k such that $\mathrm{Gal}(L_2/k)\cong E'(p^3)$. Let $M=L_1L_2$ and $K=L_1\cap L_2$. We put $G_M=\mathrm{Gal}(M/k)$. Let C_M be the center of G_M. Then we see that $C_M=\mathrm{Gal}(M/K)$. 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 [4, Proposition 2.1.7].) 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, $[G_M,G_M]$ is contained in $C_M=\mathrm{Gal}(M/K)$. Since M/k is non-abelian, $[G_M,G_M]=C_M\cap[G_M,G_M]\cong\mathbf{Z}/p\mathbf{Z}$. Hence $[M:K^*]=p$, and $\mathrm{Gal}(K^*/k)\cong\mathbf{Z}/p^2\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}$.

4. Cyclic cubic fields. In this section we consider the case that $q=3$. Let p be an odd prime such that $p\equiv 1 \bmod 3$. The number of the primitive roots of the congruence $t^3\equiv 1 \bmod p$ is two. Let $k/\mathbf{Q}$ be a cyclic cubic field, and $K/k/\mathbf{Q}$ 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 the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to a group

$$\Gamma(\alpha,\beta)=\left\langle x,y,w\ \middle|\ \begin{array}{l} x^p=y^p=w^3=1,\ xy=yx,\\ w^{-1}xw=x^\alpha,\ w^{-1}yw=y^\beta \end{array}\right\rangle,$$

where α and β are primitive roots of $t^3\equiv 1 \bmod p$. We call the group $\Gamma(\alpha,\beta)$ Type A (resp. Type B), if

Table I

Type of $\mathrm{Gal}(k(7)/\mathbf{Q})$	n
Type A	744
Type B	193, 295, 508, 523, 525, 532, 548, 762, 852, 983

$\alpha \equiv \beta \bmod p$ (resp. $\alpha \not\equiv \beta \bmod p$). We remark that if $\alpha \not\equiv \beta$ then $\alpha\beta \equiv 1 \bmod p$, so that it is nothing but the group Γ_0 for $q = 3$.

Remark 6. Let $K/k/\mathbf{Q}$ be a Galois extension such that $\mathrm{Gal}(K/\mathbf{Q})$ is Type A. If F is a number field such that $k \subset F \subset K$, then $F/\mathbf{Q}$ is a Galois extension.

Proposition 7. *Let p be an odd prime such that $p \equiv 1 \bmod 3$, and $k/\mathbf{Q}$ be a cyclic cubic extension. Assume that there exists an unramified Galois extension F/k such that $[F : k] = p$ and that $F/\mathbf{Q}$ is non-Galois. Then there exists a Galois extension $L/k/\mathbf{Q}$ such that*

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

(ii) *$\mathrm{Gal}(L/k)$ is isomorphic to $E(p^3)$.*

Proof. Let α, β be distinct primitive roots of $t^3 \equiv 1 \bmod p$. By the assumption concerning the existence of F, we see $M_k(\alpha) \neq \{1\}$ and $M_k(\beta) \neq \{1\}$. Thus the proposition follows from Theorem 3. □

5. Numerical examples. In this section, we give some examples computed with PARI [10]. Let $Cl_p(k)$ be the p-Sylow subgroup of the ideal class group $Cl(k)$.

Example 8. Let n be an integer, and let k be the simplest cubic field defined by the equation

$$x^3 - nx^2 - (n+3)x - 1 = 0 \ (1 \leqq n \leqq 1000).$$

For the simplest cubic fields, we refer Shanks [12].

The number of the field such that the rank of $Cl_7(k)$ is greater than or equal to 2 is 11. The group $Cl_7(k)$ of these fields are isomorphic to $\mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z}$. Let $k(7)$ be the Hilbert 7-class field of k.

Then for the case $n = 193$, 295, 508, 523, 525, 532, 548, 762, 852, 983, there exists an unramified Galois extension L/k such that $\mathrm{Gal}(L/k) \cong E(7^3)$. (see Table I).

Example 9. Let k be the simplest cubic field defined by the equation $x^3 + 269x^2 + 266x - 1 = 0$.

Then the class number of k is 343, and $Cl(k) \cong Cl_7(k) \cong \mathbf{Z}/49\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z}$. Let σ be a generator of $\mathrm{Gal}(k/\mathbf{Q})$. By computing with PARI, we see that there exist ideal classes a and b such that $a^7 \neq 1$, $b^7 = 1, \sigma(a) = a^{-10}b^6, \sigma(b) = a^{-7}b^2$.

Let K/k be the unramified Galois extension such that $\mathrm{Gal}(K/k) \cong \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z}$. By observing the action of σ on $Cl(k)/Cl(k)^7$, we see that $\mathrm{Gal}(K/\mathbf{Q})$ is Type B. Then there exists an unramified Galois extension L/k such that $\mathrm{Gal}(L/k) \cong E(7^3)$. By Proposition 6, there exists an unramified Galois extension L'/k such that $\mathrm{Gal}(L'/k) \cong E'(7^3)$.

Example 10. Let k be a quintic field defined by the equation

$$x^5 + 324x^4 + 9890x^3 + 79115x^2 - 4706x + 1 = 0.$$

The class number of k is calculated in Schoof-Washington [11]. The class number of k is $37631 = 11^2 \cdot 311$, and $Cl_{11}(k) \cong \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z}$. The solution of the congruence $t^5 \equiv 1 \bmod 11$ are 3, 4, 5 and 9. By observing the action of $\mathrm{Gal}(k/\mathbf{Q})$ on the group $Cl_{11}(k)$, we see $\mathrm{Gal}(k(11)/\mathbf{Q})$ is isomorphic to $\Gamma(3,4)$, which is Type B. Thus there exists an unramified Galois extension L/k such that $\mathrm{Gal}(L/k)$ is $E(11^3)$.

Acknowledgment. I should like to express my gratitude to the referee for her/his careful reading and for her/his advice.

References

[1] C. Bachoc and S.-H. Kwon, Sur les extensions de groupe de Galois $\tilde{A}_4$, Acta Arith. **62** (1992), no. 1, 1–10.

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

[3] R. Couture and A. Derhem, Un problème de capitulation, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 11, 785–788.

[4] G. Karpilovsky, *The Schur multiplier*, London Mathematical Society Monographs. New Series, 2, Oxford Univ. Press, New York, 1987.

[5] K. Miyake, Notes on the ideal class groups of the p-class fields of some algebraic number fields, Proc. Japan Acad. Ser. A Math. Sci. **68** (1992), no. 4, 79–84.

[6] A. Nomura, On the existence of unramified p-extensions, Osaka J. Math. **28** (1991), no. 1, 55–62.

[7] A. Nomura, On the class numbers of certain Hilbert class fields, Manuscripta Math. **79** (1993), no. 3–4, 379–390.

[8] A. Nomura, Notes on the existence of certain unramified 2-extensions, Illinois J. Math. **46** (2002), no. 4, 1279–1286.

[9] A. Nomura, Some remarks on the existence of certain unramified p-extensions. (to appear in Tokyo J. Math.).

[10] The PARI Group, PARI/GP, Bordeaux, 2004. (`http://pari.math.u-bordeaux.fr/`).

[11] R. Schoof and L. C. Washington, Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comp. **50** (1988), no. 182, 543–556.

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

[13] A. E. Western, Groups of Order p^3q, Proc. London Math. Soc. **S1-30** no. 1, 209-263.