Pacific Journal of Mathematics

UNRAMIFIED 3-EXTENSIONS OVER CYCLIC CUBIC FIELDS

Akito Nomura

Volume 230 No. 2 April 2007

PACIFIC JOURNAL OF MATHEMATICS
Vol. 230, No. 2, 2007

UNRAMIFIED 3-EXTENSIONS OVER CYCLIC CUBIC FIELDS

AKITO NOMURA

We study the existence of unramified 3-extensions over cyclic cubic fields. As an application, we study the class number relation between certain cubic fields.

1. Introduction

Let F be a number field and Γ a finite group. We are interested in the problem whether there exists an unramified Galois extension M/F with Galois group isomorphic to Γ. In case when Γ is an abelian group, by class field theory, this problem is closely related to the structure of the ideal class group of F. Thus this problem is interesting in the sight of a generalization of class field theory.

In this article we consider the following problems.

Problem $P(F, \Gamma)$: For a given Galois extension $F/\mathbb{Q}$ and a finite group Γ, does there exists a Galois extension $M/F/\mathbb{Q}$ satisfying the conditions:

(1) $\mathrm{Gal}(M/F)$ is isomorphic to Γ;

(2) M/F is unramified?

By definition, "a Galois extension $M/F/\mathbb{Q}$" means that $M/\mathbb{Q}$, $F/\mathbb{Q}$ are Galois extensions, with F an intermediate field of $M/\mathbb{Q}$.

Problem $P(F, \Gamma, E)$: For a given Galois extension $F/\mathbb{Q}$ and finite groups Γ and E, does there exists a Galois extension $M/F/\mathbb{Q}$ satisfying the conditions:

(1) $\mathrm{Gal}(M/F)$ is isomorphic to Γ;

(2) $\mathrm{Gal}(M/\mathbb{Q})$ is isomorphic to E;

(3) M/F is unramified?

If a Galois extension $M/F/\mathbb{Q}$ satisfies the conditions in $P(F, \Gamma)$, we call the field M a solution of $P(F, \Gamma)$, and likewise for $P(F, \Gamma, E)$.

MSC2000: 12F12, 11R29.

Keywords: cyclic field, cubic field, unramified extension, 3-extension, class number.

This research was partially supported by the Grants-in-Aid for Scientific Research (C), the Japan Society for the Promotion of Science.

In [Nomura 1991; 1993; 2002], we studied these problems in the case where l and p are distinct primes, F is a cyclic field of degree l, and Γ is a p-group. Lemmermeyer [1997] conjectured that for any 2-group Γ there exists a quadratic field F such that the answer to the problem $P(F, \Gamma)$ is affirmative, but this has been disproved by Boston and Leedham-Green [1999].

Here we shall study the problems above for cyclic cubic fields and certain 3-groups. As an application of our main result, we study the class number relations of some cubic fields and the class number of the Hilbert 3-class field of certain cubic fields. We also provide an alternative proof for a part of the result in [Naito 1987] and a slight generalization. We use GAP Version 4.4 for calculations of 3-groups.

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 1968; Neukirch 1973].

Let $\mathfrak{G}$ be the absolute Galois group of a number field k, and L/k a finite Galois extension with Galois group G. For a central extension

$$\varepsilon : 1 \to A \to E \xrightarrow{j} G \to 1,$$

the embedding problem $(L/k, \varepsilon)$ is defined by the diagram

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

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

For each prime $\mathfrak{q}$ of k, we write $k_{\mathfrak{q}}$ for the $\mathfrak{q}$-completion of k, and $L_{\mathfrak{q}}$ for the completion of L relative to an extension of $\mathfrak{q}$ to L. The local problem $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ of $(L/k, \varepsilon)$ is defined by the diagram

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

where $G_{\mathfrak{q}}$ is the Galois group of $L_{\mathfrak{q}}/k_{\mathfrak{q}}$, which is isomorphic to the decomposition group of $\mathfrak{q}$ in L/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 $(L/k, \varepsilon)$, solution and proper solution are defined for $(L_q/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$.

We need some lemmas, which are essential in the theory of embedding problems. Let p be an odd prime and L/k a p-extension. Let $\varepsilon : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbb{Q}) \to 1$ be a central extension.

We denote by $\mathrm{Ram}(L/k)$ the set of all primes of k which are ramified in L/k.

Lemma 2.1 [Neukirch 1973]. *$(L/k, \varepsilon)$ is solvable if and only if $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ are solvable for all primes $\mathfrak{q}$ of $\mathrm{Ram}(L/k)$.*

Lemma 2.2 [Hoechsmann 1968]. *If ε is a nonsplit extension, every solution of $(L/k, \varepsilon)$ is a proper solution.*

Lemma 2.3 [Neukirch 1973]. *Assume that $(L/k, \varepsilon)$ is solvable. Let S be a finite set of primes of k and $M(\mathfrak{q})$ a solution of $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ for $\mathfrak{q}$ of S. Then there exists a solution M of $(L/k, \varepsilon)$ such that the completion of M by $\mathfrak{q}$ is equal to $M(\mathfrak{q})$ for each $\mathfrak{q}$ of S.*

3. Embedding problems with ramification conditions

Let p be an odd prime. In this section, let k be either the rational number field or an imaginary quadratic field with the class number prime to p ($p \neq 3$, when $k = \mathbb{Q}(\sqrt{-3})$).

We now state a key lemma of this article. The idea of the proof is similar to [Nomura 1991], and we sketch it for the reader's convenience.

Lemma 3.1. *Let L/k be a p-extension and $\varepsilon : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \xrightarrow{j} \mathrm{Gal}(L/k) \to 1$ a nonsplit central extension. Assume that the induced extension $\varepsilon_{\mathfrak{q}}$ is split for any prime $\mathfrak{q}$ of $\mathrm{Ram}(L/k)$. Then $(L/k, \varepsilon)$ has a proper solution M such that M/L is unramified.*

Proof. For any prime $\mathfrak{q}$ of $\mathrm{Ram}(L/k)$, the local problem $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ is solvable because $\varepsilon_{\mathfrak{q}}$ is split. By Lemma 2.1, $(L/k, \varepsilon)$ is solvable.

Next we shall prove that for each prime $\mathfrak{p}$ of k above p the local problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \varepsilon_{\mathfrak{p}})$ has a solution $M(\mathfrak{p})/L_{\mathfrak{p}}/k_{\mathfrak{p}}$ such that $M(\mathfrak{p})/L_{\mathfrak{p}}$ is unramified. If $\varepsilon_{\mathfrak{p}}$ is split, then $L_{\mathfrak{p}}$ is itself a solution. Assume that $\varepsilon_{\mathfrak{p}}$ is not split. Then $\mathfrak{p}$ is unramified in L/k, and $\mathrm{Gal}(L_{\mathfrak{p}}/k_{\mathfrak{p}})$ is cyclic p-group. Hence $E_{\mathfrak{p}}$ is also cyclic p-group. Since the Galois group of the maximal unramified p-extension of $k_{\mathfrak{p}}$ is isomorphic to the ring of p-adic integers, the problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \varepsilon_{\mathfrak{p}})$ has an unramified solution.

By virtue of Lemma 2.2 and 2.3, $(L/k, \varepsilon)$ has a proper solution $M_1/L/k$ such that any prime $\widetilde{\mathfrak{p}}$ of L above p is unramified in M_1/L. If M_1/L is unramified, $M_1/L/k$ is a required solution of $(L/k, \varepsilon)$. Assume that M_1/L is not unramified. Let $\widehat{\mathfrak{q}}$ be a prime of M_1 which is ramified in M_1/L and $\widetilde{\mathfrak{q}}$ (resp. $\mathfrak{q}$) the restriction to L (resp. k). Then $N_{M_1/\mathbb{Q}}\widehat{\mathfrak{q}} \equiv 1 \bmod p$. Since M_1/k is a p-extension, $N_{k/\mathbb{Q}}\mathfrak{q} \equiv 1 \bmod p$. By [Shafarevich 1964, Theorem 1], there exists an extension T/k such that $\mathfrak{q}$ is ramified in T/k and that other primes are unramified. Let $\bar{\mathfrak{q}}$ be an extension of $\mathfrak{q}$ to M_1T and M_2 the inertia field of $\bar{\mathfrak{q}}$ in M_1T/k. By the assumption of $\varepsilon_{\mathfrak{q}}$, $\mathfrak{q}$ is unramified in L/k because the inertia group of $\widehat{\mathfrak{q}}$ in M_1/k is cyclic. Then M_2 is a proper solution of $(L/k, \varepsilon)$ such that $\mathrm{Ram}(M_2/L) \subsetneq \mathrm{Ram}(M_1/L)$. By repeating this process, we can get a required solution. □

4. Lemmas on *p*-extensions

In this section we shall prepare some lemmas and notations.

For each odd prime p, denote by $E(p^3)$ the group of order p^3 defined by

$$\langle x, y, z \mid x^p = y^p = z^p = 1, x^{-1}yx = yz, xz = zx, yz = zy\rangle.$$

The next two lemmas are essential in this article. Lemma 4.2 is a special case of the Chebotarev monodromy theorem; for the proof see [Cohn 1978, Theorem 16.30].

Lemma 4.1. *Let k be a number field and $M/L/k$ a Galois extension such that*

(1) $\mathrm{Gal}(M/k) \cong E(p^3)$,

(2) $\mathrm{Gal}(L/k) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$,

(3) *M/L is unramified.*

Then L/k is locally cyclic, that is to say, any prime ramified in L/k is also decomposed in L/k.

Proof. Assume that there exists a prime $\mathfrak{q}$ of k such that $\mathrm{Gal}(L_{\mathfrak{q}}/k_{\mathfrak{q}}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Let $\widetilde{\mathfrak{q}}$ and $\bar{\mathfrak{q}}$ be primes of M and L, respectively, above $\mathfrak{q}$. We must consider two cases. First assume that $\mathfrak{q}$ is totally ramified in L/k. We remark that this case occur only when $\mathfrak{q}$ is above p. Since M/L is unramified, the order of the inertia group of $\widetilde{\mathfrak{q}}$ in M/k is p^2. Then the inertia group is normal subgroup of $\mathrm{Gal}(M/k)$, so the inertia field is a cyclic extension over k of degree p. Hence it is contained in L. This is a contradiction. Next assume that $\mathfrak{q}$ is inert and ramified in L/k. Since $E(p^3)$ has no cyclic subgroup of order p^2, $\bar{\mathfrak{q}}$ is decomposed in M/L. Then the order of the decomposition group of $\widetilde{\mathfrak{q}}$ in M/k is p^2. Thus the decomposition group is normal subgroup of $\mathrm{Gal}(M/k)$. Hence the decomposition field is contained in L. This is a contradiction. □

Lemma 4.2. *Let p be a prime and k a number field such that the class number is prime to p. Let F/k be a cyclic extension of degree p. If $L/F/k$ is a p-extension such that L/F is unramified, then* $\mathrm{Gal}(L/k)$ *is generated by elements of degree p.*

Notation. In the rest of this article, we write $\Gamma(i, j)$ for the group whose library number in GAP is (i, j), where i is equal to the order of its group. With the commutator notation $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ and the ordinary generator-relator notation, we have

$$\begin{aligned}
\Gamma(3^2, 2) &= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\\
\Gamma(3^3, 2) &= \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\\
\Gamma(3^3, 3) &= \langle x, y, z \mid x^3, y^3, z^3, z[y, x], [x, z], [y, z]\rangle = E(3^3),\\
\Gamma(3^3, 4) &= \langle x, y \mid x^9, y^3, x^3[y, x]\rangle,\\
\Gamma(3^3, 5) &= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\\
\Gamma(3^4, 2) &= \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z},\\
\Gamma(3^4, 3) &= \langle x, y, z \mid y[z, x], x^9, y^3, z^3, [x, y], [z, y]\rangle,\\
\Gamma(3^4, 4) &= \langle x, y \mid x^9, y^9, x^3[y, x]\rangle,\\
\Gamma(3^4, 7) &= \langle x, y, z \mid y[z, x], x^9, y^3, z^3, x^3[y, x], [y, z]\rangle,\\
\Gamma(3^4, 9) &= \langle x, y, z \mid y[z, x], x^9, y^3, z^3, x^3[y, z], [x, y]\rangle,\\
\Gamma(3^4, 10) &= \langle x, y, z \mid y[z, x], x^9, y^3, x^3[y, x], z^3x^3, [y, z]\rangle,\\
\Gamma(3^4, 12) &= \Gamma(3^3, 3) \times \mathbb{Z}/3\mathbb{Z},\\
\Gamma(3^5, 2) &= \langle x, y, z, u, v \mid z[x, y], x^3u^{-1}, y^3v^{-1}, z^3, u^3, v^3,\\
&\qquad [x, z], [y, z], [y, u], [x, v]\rangle,\\
\Gamma(3^5, 3) &= \langle x, y, z, u, v \mid z[x, y], u[x, z], v[y, z], x^3, y^3, z^3, u^3, v^3,\\
&\qquad [y, u], [z, u], [x, u], [y, v], [z, v], [u, v], [x, v]\rangle,\\
\Gamma(3^5, 15) &= \langle x, y, z, u, v \mid z[x, y], v[x, z], x^3u^{-1}, y^3v, z^3, u^3, v^3,\\
&\qquad [y, z], [y, u], [z, u], [x, v], [z, v]\rangle,\\
\Gamma(3^5, 26) &= \langle x, y, z, u, v \mid z[x, y], u[x, z], x^3, u^3, v^3, z^3v, (xy)^3,\\
&\qquad [y, z], [y, u], [z, u], [x, v], [u, v]\rangle,\\
\Gamma(3^5, 28) &= \langle x, y, z, u, v \mid u[x, z], v[y, z], z[x, y], x^3, u^3, v^3, y^3u, z^3v,\\
&\qquad [z, u], [x, v], [y, v]\rangle,\\
\Gamma(3^5, 53) &= \langle x, y, z, u, v \mid u[x, y], v[x, u], y^3v, x^3, z^3, u^3, v^3,\\
&\qquad [x, z], [y, z], [y, u], [z, u], [x, v], [u, v]\rangle,\\
\Gamma(3^6, 40) &= \langle x, y, z, u, v, w \mid v[y, z], u[x, z], v[x, w], z[x, y], z^3w,\\
&\qquad x^3, y^3, v^3, u^3, w^3, [z,v], [u,v], [z,u], [y,w], [u,w], [v,w], [x,w]\rangle,
\end{aligned}$$

Using GAP, we locate all nonabelian 3-groups Γ satisfying three conditions:

(G1) Γ is generated by elements of order 3.

(G2) The 3-rank of Γ is equal to 2.

(G3) The order of Γ is between 3^2 and 3^5.

We list in Table 1 their maximal subgroups. By condition (G2), there are always four of them.

Γ	maximal subgroups of Γ
$\Gamma(3^3, 3)$	$\Gamma(3^2, 2) \times 4$
$\Gamma(3^4, 7)$	$\Gamma(3^3, 3),\ \Gamma(3^3, 4) \times 2,\ \Gamma(3^3, 5)$
$\Gamma(3^4, 9)$	$\Gamma(3^3, 2),\ \Gamma(3^3, 3) \times 3$
$\Gamma(3^5, 3)$	$\Gamma(3^4, 3) \times 2,\ \Gamma(3^4, 12) \times 2$
$\Gamma(3^5, 26)$	$\Gamma(3^4, 2),\ \Gamma(3^4, 9) \times 3$
$\Gamma(3^5, 28)$	$\Gamma(3^4, 4),\ \Gamma(3^4, 9) \times 2,\ \Gamma(3^4, 10)$

Table 1. 3-groups satisfying conditions (G1), (G2), and (G3). The notation $\Gamma(i, j) \times r$, for $r > 1$, means that there exist r maximal subgroups isomorphic to $\Gamma(i, j)$.

Let $L/F/\mathbb{Q}$ be a Galois extension such that $F/\mathbb{Q}$ is a cyclic cubic extension and L/F is an unramified 3-extension. Then by Lemma 4.2, $\mathrm{Gal}(L/\mathbb{Q})$ must satisfy condition (G1).

Remark 4.3. Let x, y, z be generators of $\Gamma(3^4, 9)$ as in the presentation of the previous page. The maximal subgroups of $\Gamma(3^4, 9)$ are $\langle x, y\rangle$, $\langle y, z\rangle$, $\langle xz, y\rangle$, and $\langle x^2 z, y\rangle$, where the first is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the others are isomorphic to $\Gamma(3^3, 3)$. If we replace xz (or $x^2 z$) by z, then x, y, z satisfy the same relations as in the original presentation.

5. Unramified 3-extensions over cyclic cubic fields

Let $F/\mathbb{Q}$ be a cyclic cubic extension. For some finite 3-groups Γ and E, we shall consider the problems $P(F, \Gamma)$ and $P(F, \Gamma, E)$ defined in the Introduction.

First we define some conditions concerning the Galois extension $L_0/F/\mathbb{Q}$:

(C1) $\mathrm{Gal}(L_0/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(C2) $L_0/\mathbb{Q}$ is locally cyclic.

(C3) L_0/F is an unramified cubic extension.

(C4) There exists a cubic subfield F' of L_0 such that $F' \neq F$ and that L_0/F' is unramified.

Remark 5.1. Under (C1), condition (C2) is equivalent to that any prime of $\mathbb{Q}$ ramified in $L_0/\mathbb{Q}$ is decomposed in $L_0/\mathbb{Q}$.

Remark 5.2. Assume that $L_0/F/\mathbb{Q}$ satisfies conditions (C1), (C2) and (C3). If only two primes of $\mathbb{Q}$ are ramified in $F/\mathbb{Q}$, then condition (C4) is always satisfied.

Proposition 5.3. *Assume that the Galois extension $L_0/F/\mathbb{Q}$ satisfies the conditions (C1) and (C3). There is equivalence between*

(a) *$L_0/F/\mathbb{Q}$ satisfies condition (C2);*

(b) *$P(F, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$ has a solution L_1 such that $L_1 \supset L_0$.*

Proof. The implication (b) ⇒ (a) is clear by Lemma 4.1. We shall prove (a) ⇒ (b). There exists a nonsplit central extension

$$\varepsilon : 1 \to \mathbb{Z}/3\mathbb{Z} \to \Gamma(3^3, 3) \xrightarrow{j} \mathrm{Gal}(L/\mathbb{Q}) \to 1.$$

The explicit construction of ε is as follows. Let F' be an any cubic subfield of L_0 such that $F' \neq F$, and put $\mathrm{Gal}(L_0/F) = \langle a \rangle$, $\mathrm{Gal}(L_0/F') = \langle b \rangle$. Let $\Gamma(3^3, 3) = \langle x, y, z \mid x^3, y^3, z^3, z[y, x], [x, z], [y, z] \rangle$. Then j is defined by $x \mapsto a$, $y \mapsto b$.

Since the exponent of the group $\Gamma(3^3, 3)$ is equal to 3, the induced extension ε_q is split for any prime q. By applying Lemma 3.1 to the embedding problem $(L_0/\mathbb{Q}, \varepsilon)$, we can find a Galois extension $L_1/L_0/\mathbb{Q}$ such that $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic to $\Gamma(3^3, 3)$ and that L_1/L_0 is unramified. Since L_0/F is unramified, L_1/F is also unramified. Further $\mathrm{Gal}(L_1/F) = j^{-1}(\langle a \rangle) = \langle x, z \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

Corollary 5.4. *Let q and l be prime numbers such that $q \equiv l \equiv 1 \bmod 3$, $q^{(l-1)/3} \equiv 1 \bmod l$, and $l^{(q-1)/3} \equiv 1 \bmod q$. Let $F/\mathbb{Q}$ be a cyclic cubic extension. If $F/\mathbb{Q}$ is unramified outside $\{q, l\}$ and q, l are ramified in $F/\mathbb{Q}$, then the answer of the problem $P(F, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$ is affirmative.*

This is a direct consequence of Proposition 5.3.

Theorem 5.5. *Let $L_0/F/\mathbb{Q}$ be a Galois extension satisfying the conditions (C1), (C2), and (C3). Assume that $P(F, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$ has a solution L_1 such that $L_1 \supset L_0$. There is equivalence between*

(a) *Any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_1/F;*

(b) *$P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$ has a solution L_2 such that $L_2 \supset L_1$.*

Proof. (a) ⇒ (b). Let C be the center of $\Gamma(3^4, 9)$, then the order of C is 3 and $\Gamma(3^4, 9)/C$ is isomorphic to $\Gamma(3^3, 3)$. The group $\Gamma(3^4, 9)$ has four maximal subgroups, one is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the others are isomorphic to $\Gamma(3^3, 3)$. Hence there exists a central extension

$$\varepsilon : 1 \to \mathbb{Z}/3\mathbb{Z} \to \Gamma(3^4, 9) \xrightarrow{j} \mathrm{Gal}(L_1/\mathbb{Q}) \to 1$$

such that $j^{-1}(\mathrm{Gal}(L_1/F))$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. The explicit construction of ε is as follows. We recall that

$$\Gamma(3^4, 9) = \langle x, y, z \mid y[z, x], x^9, y^3, z^3, x^3[y, z], [x, y]\rangle,$$
$$\Gamma(3^3, 3) = \langle a, b, c \mid a^3, b^3, c^3, c[b, a], [a, c], [b, c]\rangle.$$

We can assume that $\mathrm{Gal}(L_1/F) = \langle a, c\rangle$. Indeed maximal subgroups of $\Gamma(3^3, 3)$ are $\langle a, c\rangle$, $\langle ba, c\rangle$, $\langle b^2a, c\rangle$ and $\langle b, c\rangle$. If we replace ba (or b^2a) by a, then a, b, c satisfy the same relations. And if we replace b by a and a by b^{-1}, then a, b, c also satisfy the same relations. Then j is defined by $x \mapsto a$, $y \mapsto c$, $z \mapsto b$.

We shall consider the embedding problem $(L_1/\mathbb{Q}, \varepsilon)$. Let q be a prime of $\mathbb{Q}$ ramified in $L_1/\mathbb{Q}$, and let $\widehat{q}$ be an extension of q to L_1. Then $\mathrm{Gal}(L_{1q}/\mathbb{Q}_q)$ is isomorphic to the decomposition group of $\widehat{q}$ in $L_1/\mathbb{Q}$. Since L_1/F is unramified and $\widehat{q}$ is completely decomposed in L_1/F, $\mathrm{Gal}(L_{1q}/\mathbb{Q}_q)$ is the cyclic group of order 3 and is not contained in $\mathrm{Gal}(L_1/F)$. Thus $j^{-1}(\mathrm{Gal}(L_{1q}/\mathbb{Q}_q))$ is a subgroup of $\Gamma(3^3, 3)$. Hence the group extension

$$\varepsilon_q : 1 \to \mathbb{Z}/3\mathbb{Z} \to j^{-1}(\mathrm{Gal}(L_{1q}/\mathbb{Q}_q)) \xrightarrow{j} \mathrm{Gal}(L_{1q}/\mathbb{Q}_q) \to 1$$

is split because the exponent of $\Gamma(3^3, 3)$ is 3. In view of Lemma 3.1, the proof of (a) $\Rightarrow$ (b) is complete .

(b) $\Rightarrow$ (a). Let q be a prime of $\mathbb{Q}$ ramified in $F/\mathbb{Q}$, and let F' be the decomposition field of q in $L_0/\mathbb{Q}$. Then F' is a cubic field not equal to F. Since $\mathrm{Gal}(L_2/F)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ and other maximal subgroups of $\Gamma(3^4, 9)$ are isomorphic to $\Gamma(3^3, 3)$, $\mathrm{Gal}(L_2/F')$ is isomorphic to $\Gamma(3^3, 3)$. Let $\widehat{\mathfrak{q}}$ be a prime of L_0 lying above q. By Lemma 4.1, $\widehat{\mathfrak{q}}$ is completely decomposed in L_1/L_0. □

Theorem 5.6. *Let $L_0/F/\mathbb{Q}$ be a Galois extension satisfying the conditions (C1), (C2), (C3), and (C4). Assume that $P(F, \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$ has a solution L_1 such that $L_1 \supset L_0$. There is equivalence between*

(a) *Any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_1/F;*

(b) *$P(F, \Gamma(3^3, 3), \Gamma(3^4, 9))$ has a solution L_2 such that $L_2 \supset L_1$.*

Proof. Since the proof is similar to that of Theorem 5.5, we merely sketch it. We consider (a) $\Rightarrow$ (b). Let $F'/\mathbb{Q}$ be the cyclic cubic extension as in condition (C4). Then there exists a central extension $\varepsilon : 1 \to \mathbb{Z}/3\mathbb{Z} \to \Gamma(3^4, 9) \xrightarrow{j} \mathrm{Gal}(L_1/\mathbb{Q}) \to 1$ such that $j^{-1}(\mathrm{Gal}(L_1/F)) \cong \Gamma(3^3, 3)$ and that $j^{-1}(\mathrm{Gal}(L_1/F')) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

An application of Lemma 3.1 completes the proof of (a) $\Rightarrow$ (b). We omit the proof of the converse. □

Theorem 5.7. *Let $L_0/F/\mathbb{Q}$ be a Galois extension satisfying the conditions (C1), (C2), (C3), and (C4). Assume that $P(F, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$ has a solution L_1 such that $L_1 \supset L_0$. If any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_1/F, then $P(F, \Gamma(3^3, 4), \Gamma(3^4, 7))$ has a solution L_2 such that $L_2 \supset L_1$.*

Proof. Let $F'/\mathbb{Q}$ be the cyclic cubic extension as in condition (C4). The maximal subgroups of $\Gamma(3^4, 7)$ are $\Gamma(3^3, 3)$, $\Gamma(3^3, 4)$, $\Gamma(3^3, 4)$, and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Then there exists a central extension

$$\varepsilon : 1 \to \mathbb{Z}/3\mathbb{Z} \to \Gamma(3^4, 7) \xrightarrow{j} \mathrm{Gal}(L_1/\mathbb{Q}) \to 1$$

such that $j^{-1}(\mathrm{Gal}(L_1/F)) \cong j^{-1}(\mathrm{Gal}(L_1/F')) \cong \Gamma(3^3, 4)$. The explicit construction of ε is as follows. We recall that

$$\Gamma(3^4, 7) = \langle x, y, z \mid y[z, x], x^9, y^3, z^3, x^3[y, x], [y, z]\rangle,$$
$$\Gamma(3^3, 3) = \langle a, b, c \mid a^3, b^3, c^3, c[b, a], [a, c], [b, c]\rangle.$$

Here we can assume that $\mathrm{Gal}(L_1/F) = \langle a, c\rangle$ and $\mathrm{Gal}(L_1/F') = \langle ab, c\rangle$. Let j is the group homomorphism defined by $x \mapsto a$, $y \mapsto c$, $z \mapsto b$, then $j^{-1}(\mathrm{Gal}(L_1/F)) = \langle x, y\rangle \cong \Gamma(3^3, 4)$ and $j^{-1}(\mathrm{Gal}(L_1/F')) = \langle xz, y\rangle \cong \Gamma(3^3, 4)$.

If q is a prime of $\mathbb{Q}$ which is ramified in $L_1/\mathbb{Q}$, then $\mathrm{Gal}(L_{1q}/\mathbb{Q}_q)$ is the cyclic group of order 3. Since $j^{-1}(\mathrm{Gal}(L_{1q}/\mathbb{Q}_q))$ is contained in $\Gamma(3^3, 3)$ or $\Gamma(3^3, 5)$, the exponent of $j^{-1}(\mathrm{Gal}(L_{1q}/\mathbb{Q}_q))$ is equal to 3. Then the group extension

$$\varepsilon_q : 1 \to \mathbb{Z}/3\mathbb{Z} \to j^{-1}(\mathrm{Gal}(L_{1q}/\mathbb{Q}_q)) \xrightarrow{j} \mathrm{Gal}(L_{1q}/\mathbb{Q}_q) \to 1$$

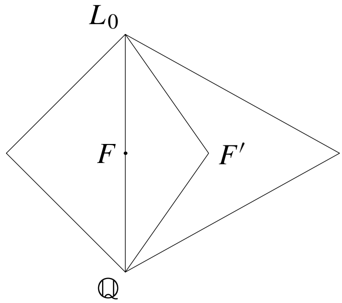
is split. By virtue of Lemma 3.1, the proof is complete. □

6. Unramified extensions of degree 81 over cyclic cubic fields

Let $F/\mathbb{Q}$ be a cyclic cubic extension. We consider the case of a Galois extension $L_3/F/\mathbb{Q}$ such that L_3/F is unramified extension of degree 81, and the 3-rank of $\mathrm{Gal}(L_3/\mathbb{Q})$ is 2.

Under these conditions $\mathrm{Gal}(L_3/\mathbb{Q})$ is isomorphic to one of $\Gamma(3^5, 3)$, $\Gamma(3^5, 26)$, or $\Gamma(3^5, 28)$.

In this section we always assume that $L_0/F/\mathbb{Q}$ satisfies conditions (C1), (C2), (C3), and (C4). Let F' be the cubic field as in condition (C4).



Theorem 6.1. *Assume that the problem* $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$ *has a solution* L_2 *such that* $L_2 \supset L_0$. *The following conditions are equivalent.*

(a) *Any prime of* F *which is ramified in* $F/\mathbb{Q}$ *is completely decomposed in* L_2/F.

(b) $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \Gamma(3^5, 26))$ *has a solution* L_3 *such that* $L_3 \supset L_2$.

(c) $P(F, \Gamma(3^4, 4), \Gamma(3^5, 28))$ *has a solution* L_3 *such that* $L_3 \supset L_2$.

Lemma 6.2. *Let* F, F' *and* L_0 *be as in condition* (C4). *Let* L_2 *be a solution of* $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$ *such that* $L_2 \supset L_0$, *and let* $L_3/L_2/\mathbb{Q}$ *be a Galois extension such that* L_3/F *and* L_3/F' *are unramified.*

(1) *If* $\mathrm{Gal}(L_3/\mathbb{Q})$ *is isomorphic to* $\Gamma(3^5, 26)$, *we have the equivalence*

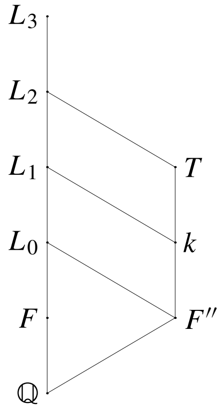
$$\mathrm{Gal}(L_3/F) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \Longleftrightarrow \mathrm{Gal}(L_3/F') \cong \Gamma(3^4, 9).$$

(2) *If* $\mathrm{Gal}(L_3/\mathbb{Q})$ *is isomorphic to* $\Gamma(3^5, 28)$, *we have the equivalence*

$$\mathrm{Gal}(L_3/F) \cong \Gamma(3^4, 4) \Longleftrightarrow \mathrm{Gal}(L_3/F') \cong \Gamma(3^4, 10).$$

Proof. (1) Since one of the maximal subgroups of $\Gamma(3^5, 26)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and the others are isomorphic to $\Gamma(3^4, 9)$, the forward implication is trivial. We consider the reverse implication. Assume that $\mathrm{Gal}(L_3/F) \cong \Gamma(3^4, 9)$. Let F'' be the subfield of L_3 corresponding to the subgroup $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Then L_0/F'' is not unramified because F'' is not equal to F and F'. Since $\mathrm{Gal}(L_3/F'') \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, there exists a cyclic extension M/F'' of degree 9 such that $L_3 \supset M \supset L_0$. Since L_0/F'' is not unramified, M/L_0 is not also unramified. This contradicts that L_3/L_0 is unramified.

(2) We prove only the forward implication; the converse is similar. Assume that $\mathrm{Gal}(L_3/F')$ is not isomorphic to $\Gamma(3^4, 10)$. Let F'' be the subfield of L_3 corresponding to the subgroup $\Gamma(3^4, 10)$, then L_0/F'' is not unramified. Let $\mathfrak{q}$ be a prime of F'' which is ramified in L_0/F'' and $\widehat{\mathfrak{q}}$ an extension of $\mathfrak{q}$ to L_2. Let T be the inertia field of $\widehat{\mathfrak{q}}$ in L_2/F'' and k the intersection of L_1 and T. Then $F'' \subsetneq k \subsetneq T$.



The group $\Gamma(3^5, 28)$ has only one normal subgroup of order 9, which is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Hence $\mathrm{Gal}(L_3/L_1)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Since all maximal subgroups of $\mathrm{Gal}(L_3/F) \cong \Gamma(3^4, 4)$ are isomorphic to $\Gamma(3^3, 2)$, the Galois group $\mathrm{Gal}(L_3/L_0)$ is isomorphic to $\Gamma(3^3, 2)$. Further one of the maximal subgroups of $\mathrm{Gal}(L_3/F'')$ is isomorphic to $\Gamma(3^3, 2)$ and the others are isomorphic to $\Gamma(3^3, 4)$. Then $\mathrm{Gal}(L_3/k)$ is isomorphic to $\Gamma(3^3, 4)$. Hence L_3/T is a cyclic extension of degree 9, because one maximal subgroup of $\Gamma(3^3, 4)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the other three groups are isomorphic to $\mathbb{Z}/9\mathbb{Z}$. Since $\widehat{\mathfrak{q}}$ is ramified in L_2/T, $\widehat{\mathfrak{q}}$ is also ramified in L_3/L_2. This contradicts that L_3/L_2 is unramified, proving the desired implication. □

Proof of Theorem 6.1. We first consider (a) ⇒ (b). Let C be the center of $\Gamma(3^5, 26)$, then the order of C is equal to 3 and the quotient group $\Gamma(3^5, 26)/C$ is isomorphic to $\Gamma(3^4, 9)$. The group $\Gamma(3^5, 26)$ has four maximal subgroups, one is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and the others are isomorphic to $\Gamma(3^4, 9)$. Then there exists a central extension

$$\varepsilon : 1 \to \mathbb{Z}/3\mathbb{Z} \to \Gamma(3^5, 26) \xrightarrow{j} \mathrm{Gal}(L_2/\mathbb{Q}) \to 1$$

such that $j^{-1}(\mathrm{Gal}(L_2/F)) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and that $j^{-1}(\mathrm{Gal}(L_2/F')) \cong \Gamma(3^4, 9)$. The explicit construction of ε is as follows. Let $\Gamma(3^5, 26)$ be as on page 171, and

$$\Gamma(3^4, 9) = \langle a, b, c \mid b[c, a], a^9, b^3, c^3, a^3[b, c], [a, b]\rangle.$$

By Remark 4.3 we can assume that $\mathrm{Gal}(L_2/F) = \langle a, b\rangle$, $\mathrm{Gal}(L_2/F') = \langle b, c\rangle$. Then j is defined by $x \mapsto c$, $y \mapsto a$, $z \mapsto b$.

Let q be a prime of $\mathbb{Q}$ which is ramified in $L_2/\mathbb{Q}$, and $\widehat{q}$ an extension of q to L_2. Then $\mathrm{Gal}(L_{2q}/\mathbb{Q}_q)$ is isomorphic to the decomposition group of $\widehat{q}$ in $L_2/\mathbb{Q}$. Since L_2/F is unramified and $\widehat{q}$ is completely decomposed in L_2/F, $\mathrm{Gal}(L_{2q}/\mathbb{Q}_q)$ is the cyclic group of order 3 and is not contained in $\mathrm{Gal}(L_2/F)$. Now, we see from Table 1 that a subgroup H of $\Gamma(3^4, 9)(\cong \mathrm{Gal}(L_3/F'))$ having order 27 and not contained in $\Gamma(3^4, 2)(\cong \mathrm{Gal}(L_3/F))$ must be isomorphic to $\Gamma(3^3, 3)$. Thus $j^{-1}(\mathrm{Gal}(L_{2q}/\mathbb{Q}_q))$ is a subgroup of $\Gamma(3^3, 3)$. Since the exponent of $\Gamma(3^3, 3)$ is 3, the group extension

$$\varepsilon_q : 1 \to \mathbb{Z}/3\mathbb{Z} \to j^{-1}(\mathrm{Gal}(L_{2q}/\mathbb{Q}_q)) \xrightarrow{j} \mathrm{Gal}(L_{2q}/\mathbb{Q}_q) \to 1$$

is split. In view of Lemma 3.1, the embedding problem $(L_2/\mathbb{Q}, \varepsilon)$ has a proper solution L_3 such that L_3/L_2 is unramified. Since $\mathrm{Gal}(L_3/F)$ is isomorphic to $j^{-1}(\mathrm{Gal}(L_2/F)) = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, L_3 is a required field.

Next we consider (b) $\Rightarrow$ (a). Let q be a prime of $\mathbb{Q}$ which is ramified in $F/\mathbb{Q}$, and $\widehat{q}$ an extension of q to L_2. Assume that $\widehat{q}$ is not completely decomposed in L_2/F. Let L_1 be the field such that $L_0 \subset L_1 \subset L_2$ and that $\mathrm{Gal}(L_1/\mathbb{Q}) \cong \Gamma(3^3, 3)$. Then by Theorem 5.5 and the assumption, $\widehat{q}$ is completely decomposed in L_1/F and is inert in L_2/L_1. Let F'' be the decomposition field of q in $L_0/\mathbb{Q}$. Let T be the inertia field of $\widehat{q}$ in $L_2/\mathbb{Q}$ and k be the intersection of L_1 and T. Then $F'' \subsetneq k \subsetneq T$. We refer the field diagram in the proof of Lemma 6.2.

Since $\mathrm{Gal}(L_3/F'')$ is a maximal subgroup of $\mathrm{Gal}(L_3/\mathbb{Q})$ and $\mathrm{Gal}(L_3/F) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $\mathrm{Gal}(L_3/F'')$ is isomorphic to $\Gamma(3^4, 9)$. Since $\mathrm{Gal}(L_3/k)$ is a maximal subgroup of $\mathrm{Gal}(L_3/F'')$ and $\mathrm{Gal}(L_3/L_0) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathrm{Gal}(L_3/k)$ is isomorphic to $\Gamma(3^3, 3)$. This contradicts Lemma 4.1.

The proof of (a) $\Longleftrightarrow$ (c) is similar to that of (a) $\Longleftrightarrow$ (b), so we only sketch it. Consider (a) $\Rightarrow$ (c). There exists a central extension

$$\varepsilon : 1 \to \mathbb{Z}/3\mathbb{Z} \to \Gamma(3^5, 28) \xrightarrow{j} \mathrm{Gal}(L_2/\mathbb{Q}) \to 1$$

such that $j^{-1}(\mathrm{Gal}(L_2/F)) \cong \Gamma(3^4, 4)$ and $j^{-1}(\mathrm{Gal}(L_2/F')) \cong \Gamma(3^4, 10)$. The explicit construction of ε is as follows. Let $\Gamma(3^5, 28)$ be as on page 171, and set

$$\Gamma(3^4, 9) = \langle a, b, c \mid b[c, a], a^9, b^3, c^3, a^3[b, c], [a, b]\rangle.$$

We can assume that $\mathrm{Gal}(L_2/F) = \langle a, b\rangle$, $\mathrm{Gal}(L_2/F') = \langle b, c\rangle$. Then j is defined by $x \mapsto ca^{-1}$, $y \mapsto a$, $z \mapsto b$. In the same manner as for (a) $\Rightarrow$ (b), we can prove that the embedding problem $(L_2/\mathbb{Q}, \varepsilon)$ has a proper solution L_3 such that L_3/L_2 is unramified. Since $\mathrm{Gal}(L_3/F)$ is isomorphic to $j^{-1}(\mathrm{Gal}(L_2/F)) = \Gamma(3^4, 4)$, L_3 is a required field. We have thus proved (a) $\Rightarrow$ (c).

Next we consider (c) $\Rightarrow$ (a). Let q be a prime of $\mathbb{Q}$ which is ramified in $F/\mathbb{Q}$, and $\widehat{q}$ an extension of q to L_2. Assume that $\widehat{q}$ is not completely decomposed in L_2/F. Let L_1, T, k and F'' be the same as in the proof of (b) $\Rightarrow$ (a). The group $\mathrm{Gal}(L_3/F'')$ is a maximal subgroup of $\mathrm{Gal}(L_3/\mathbb{Q})$ and $\mathrm{Gal}(L_3/F) \cong \Gamma(3^4, 4)$. Since $\mathrm{Gal}(L_3/F') \cong \Gamma(3^4, 10)$ by Lemma 6.2(2), $\mathrm{Gal}(L_3/F'') \cong \Gamma(3^4, 9)$. Since the group $\mathrm{Gal}(L_3/k)$ is a maximal subgroup of $\mathrm{Gal}(L_3/F'')$ and $\mathrm{Gal}(L_3/L_0) \cong$

$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathrm{Gal}(L_3/k)$ is isomorphic to $\Gamma(3^3, 3)$. This contradicts Lemma 4.1. □

Theorem 6.3. *Assume that the problem $P(F, \Gamma(3^3, 3), \Gamma(3^4, 9))$ has a solution L_2 such that $L_2 \supset L_0$. The following conditions are equivalent.*

(a) *Any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_2/F.*

(b) *$P(F, \Gamma(3^4, 9), \Gamma(3^5, 26))$ has a solution L_3 such that $L_3 \supset L_2$.*

(c) *$P(F, \Gamma(3^4, 10), \Gamma(3^5, 28))$ has a solution L_3 such that $L_3 \supset L_2$.*

This follows trivially from Theorem 6.1 and Lemma 6.2.

Proposition 6.4. *Let $L_2/\mathbb{Q}$ be a solution of $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$ or $P(F, \Gamma(3^3, 3), \Gamma(3^4, 9))$ such that $L_2 \supset L_0$. If any prime ramified in $F/\mathbb{Q}$ is completely decomposed in L_2/F, then the problem $P(F, \Gamma(3^4, 3), \Gamma(3^5, 3))$ has a solution L_3 such that $L_3 \supset L_2$.*

The proof is similar to that of Theorem 6.1 (a) ⇒ (b), so we omit it.

7. Class number relations of cubic fields

In this section, let $L/\mathbb{Q}$ be a Galois extension such that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and that only two primes of $\mathbb{Q}$ are ramified in $L/\mathbb{Q}$. Let F and F' be cubic subfields of L such that L/F and L/F' are unramified.

Naito [1987] studied the class number relation of F and F', and proved parts (1) and (2) of the following proposition for a general odd prime p (not just $p = 3$). We give an alternative proof and a slight generalization when $p = 3$.

Proposition 7.1. *Let L, F, F' be as above.*

(1) *The class number of F is divisible by 9 if and only if the class number of F' is divisible by 9. Further in this case, the ideal class group of F and F' has a subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

(2) *The class number of F is divisible by 27 if and only if the class number of F' is divisible by 27. Further in this case, the ideal class group of F and F' has a subgroup $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

(3) *The class number of F is divisible by 81 if and only if the answer of the problem $P(F', \Gamma(3^4, 10))$ is affirmative. Further in this case, the ideal class group of F has a subgroup $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.*

Lemma 7.2. *Let p be an odd prime and $F/\mathbb{Q}$ a p-extension. If the class number of F is divisible by p^r for some integer r, then there exists a Galois extension $M/F/\mathbb{Q}$ such that M/F is unramified abelian and the degree $[M : F]$ is equal to p^r.*

Proof. By class field theory, there exists an unramified abelian extension K/F such that the degree $[K : F]$ is equal to p^r. Let $M_1/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$. Then $M_1/F/\mathbb{Q}$ is a Galois extension such that M_1/F is unramified abelian p-extension and the degree $[M_1 : F]$ is greater than or equal to p^r. If $[M_1 : F] = p^r$ then $M_1/F/\mathbb{Q}$ is a required field. Assume that $[M_1 : F] > p^r$. Let $C(\mathrm{Gal}(M_1/\mathbb{Q}))$ be the center of $\mathrm{Gal}(M_1/\mathbb{Q})$. Since $\mathrm{Gal}(M_1/\mathbb{Q})$ is a p-group and $\mathrm{Gal}(M_1/F)$ is a normal subgroup of $\mathrm{Gal}(M_1/\mathbb{Q})$, the intersection $\mathrm{Gal}(M_1/F) \cap C(\mathrm{Gal}(M_1/\mathbb{Q}))$ is nontrivial. Then there exists a Galois extension $M_2/F/\mathbb{Q}$ such that M_2/F is unramified p-extension and the degree $[M_2 : F]$ is equal to $[M_1 : F]/p$. By repeating this process, we get the required extension $M/F/\mathbb{Q}$. □

Proof of Proposition 7.1. (1) Assume that the class number of F is divisible by 9. By Lemma 7.2 there exists a Galois extension $L_1/F/\mathbb{Q}$ such that L_1/F is unramified abelian and that $[L_1 : F] = 9$. By Lemma 4.2 and the assumption for the number of ramified primes, $\mathrm{Gal}(L_1/\mathbb{Q})$ is generated by two elements of order 3. Then $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic to $\Gamma(3^3, 3)$. Thus L_1/F' is unramified and $\mathrm{Gal}(L_1/F') \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, because all maximal subgroups of $\Gamma(3^3, 3)$ are isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The proof of the converse is similar.

(2) Assume that the class number of F is divisible by 27. By Lemma 7.2 there exists a Galois extension $L_2/F/\mathbb{Q}$ such that L_2/F is unramified abelian and that $[L_2 : F] = 27$. Since $\mathrm{Gal}(L_2/\mathbb{Q})$ is generated by two elements of order 3, $\mathrm{Gal}(L_2/\mathbb{Q})$ is isomorphic to $\Gamma(3^4, 7)$ or $\Gamma(3^4, 9)$. We claim that $\mathrm{Gal}(L_2/\mathbb{Q})$ is not isomorphic to $\Gamma(3^4, 7)$. We assume $\mathrm{Gal}(L_2/\mathbb{Q}) \cong \Gamma(3^4, 7)$. Since $\Gamma(3^4, 7)$ has two maximal subgroups which are isomorphic to $\Gamma(3^3, 4)$, there exists a cubic field F'' such that $\mathrm{Gal}(L_2/F'') \cong \Gamma(3^3, 4)$ and that $F'' \neq F, F'$. Then only one prime ramifies in $F''/\mathbb{Q}$. By Iwasawa [Iwasawa 1956] the class number of F'' is prime to 3. Since $\Gamma(3^3, 4)$ is not generated by elements of order 3, this contradicts Lemma 4.2. Then L_2 is a solution of $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$.

Let C be the center of $\Gamma(3^4, 9)$, and L_1 the subfield of L_2 corresponding to C. Since $\Gamma(3^4, 9)/C$ is isomorphic to $\Gamma(3^3, 3)$, L_1 is a solution of the problem $P(F, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$. By Theorem 5.5 any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_1/F. Since all maximal subgroups of $\Gamma(3^3, 3)$ are isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, L_1 is also a solution of the problem $P(F', \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^3, 3))$. Then $P(F', \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$ has a solution L_2' by Theorem 5.5. Hence the class number of F' is divisible by 27. The proof of the converse is similar.

(3) Assume that the class number of F is divisible by 81. By Lemma 7.2 there exists a Galois extension $L_3/F/\mathbb{Q}$ such that L_3/F is unramified abelian and that $[L_3 : F] = 81$. Since $\mathrm{Gal}(L_3/\mathbb{Q})$ is generated by two elements of order 3, $\mathrm{Gal}(L_3/\mathbb{Q})$ is isomorphic to $\Gamma(3^5, 26)$ and $\mathrm{Gal}(L_3/F)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Let

C be the center of $\Gamma(3^5, 26)$, and L_2 the subfield of L_3 corresponding to C. Since $\Gamma(3^5, 26)/C$ is isomorphic to $\Gamma(3^4, 9)$, L_2 is a solution of the problem $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$. By Theorem 6.1 any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_2/F, and L_2 is also a solution of $P(F', \Gamma(3^3, 3), \Gamma(3^4, 9))$. By Theorem 6.3 the problem $P(F', \Gamma(3^4, 10), \Gamma(3^5, 28))$ has a solution L_3'.

For the converse we assume that L_3 is a solution of $P(F', \Gamma(3^4, 10))$. Then $\Gamma := \mathrm{Gal}(L_3/\mathbb{Q})$ has order 243 and 3-rank 2, and it has a maximal subgroup isomorphic to $\Gamma(3^4, 10)$. The group satisfying these conditions is isomorphic to $\Gamma(3^5, 28)$.

We claim that the Galois group $\mathrm{Gal}(L_3/F)$ is isomorphic to $\Gamma(3^4, 4)$, which is a maximal subgroup of $\Gamma(3^5, 28)$. For the proof, we assume that $\mathrm{Gal}(L_3/F)$ is not isomorphic to $\Gamma(3^4, 4)$, and let F'' be the subfield of L_3 corresponding to $\Gamma(3^4, 4)$. Then F'' is not equal to F and F'. Hence, by [Iwasawa 1956], the class number of F'' is prime to 3. By Lemma 4.2, $\mathrm{Gal}(L_3/F'')$ must be generated by elements of order 3. But $\Gamma(3^4, 4)$ is not generated by elements of order 3. This is a contradiction.

Let L_2 be the subfield of L_3 corresponding to the center of $\mathrm{Gal}(L_3/\mathbb{Q})$, then $\mathrm{Gal}(L_2/\mathbb{Q}) \cong \Gamma(3^4, 9)$. Let C be the center of $\mathrm{Gal}(L_3/F)$. Since $\mathrm{Gal}(L_3/F) \cong \Gamma(3^4, 4)$ and $\mathrm{Gal}(L_2/F) \cong \mathrm{Gal}(L_3/F)/C \cong \Gamma(3^3, 2)$, then $\mathrm{Gal}(L_2/F') \cong \Gamma(3^3, 3)$. Thus L_2 is a solution of $P(F', \Gamma(3^3, 3), \Gamma(3^4, 9))$. By Theorem 6.3, any prime of F' which is ramified in $F'/\mathbb{Q}$ is completely decomposed in L_2/F'. Hence any prime of F which is ramified in $F/\mathbb{Q}$ is completely decomposed in L_2/F. L_2 is also a solution of the problem $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \Gamma(3^4, 9))$. By Theorem 6.1, the problem $P(F, \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \Gamma(3^5, 26))$ has a solution L_3'. Then L_3'/F is unramified abelian extension and the Galois group is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. □

Example 7.3. Let F_{pq} and F'_{pq} denote the two cyclic cubic fields of conductor pq, where $p \equiv q \equiv 1 \bmod 3$, and let $L = F_{pq}F'_{pq}$ be their composite. Denote by $(n_1, n_2, \ldots, n_r)$ the group $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$. The following table contains a few class groups computed with PARI:

p	q	$\mathrm{Cl}(F_{pq})$	$\mathrm{Cl}(F'_{pq})$	$\mathrm{Cl}(L)$
7	181	(6,6)	(3,3)	(6,2)
43	193	(3,3)	(3,3)	(3,3)
73	241	(9,3)	(63,3)	(21,3,3)
79	157	(9,3)	(9,3)	(9,3,3)
181	331	(9,3)	(9,3)	(3,3,3,3)
103	409	(9,9)	(27,9)	(9,9,3,3)

Corollary 7.4. *Let L, F, F' be as above.*

(1) *Assume that the class number of F is divisible by* 27*. Then the problem $P(F, \Gamma(3^4, 3), \Gamma(3^5, 3))$ has a solution. In particular the class number of the Hilbert* 3*-class field of F is divisible by* 3*.*

(2) *Assume that the class number of F is divisible by* 81*. Then the problem $P(F, \Gamma(3^5, 2), \Gamma(3^6, 40))$ has a solution.*

Proof. (1) Let L_1, L_2, L_2' be as in the proof of Proposition 7.1(2). By the proof of Proposition 7.1(2), $\mathrm{Gal}(L_2/\mathbb{Q})$ is not isomorphic to $\mathrm{Gal}(L_2'/\mathbb{Q})$. Then $L_2 \neq L_2'$. Let $\bar{L}$ be the composition field of L_2 and L_2'. Since $\mathrm{Gal}(\bar{L}/L_2)$ and $\mathrm{Gal}(\bar{L}/L_2')$ are contained in the center of $\mathrm{Gal}(\bar{L}/\mathbb{Q})$, then the center has a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. In addition, $\mathrm{Gal}(\bar{L}/\mathbb{Q})$ has order 243, has 3-rank 2, and is generated by elements of order 3. The group satisfying these conditions is isomorphic to $\Gamma(3^5, 3)$. $\Gamma(3^5, 3)$ has four maximal subgroups, two are isomorphic to $\Gamma(3^4, 3)$ and the others are isomorphic to $\Gamma(3^4, 12)$. We remark that $\Gamma(3^4, 3)$ is not generated by elements of order 3. Let F'' and F''' are cyclic cubic subfield of $\bar{L}$ not equal to F and F'. Then by Iwasawa [1956], the class number of F'' and F''' are both prime to 3. Since $\mathrm{Gal}(\bar{L}/F'')$ and $\mathrm{Gal}(\bar{L}/F''')$ are generated by elements of order 3, $\mathrm{Gal}(\bar{L}/F'')\cong\mathrm{Gal}(\bar{L}/F''')\cong\Gamma(3^4, 12)$. Hence $\mathrm{Gal}(\bar{L}/F)\cong\mathrm{Gal}(\bar{L}/F')\cong\Gamma(3^4, 3)$.

(2) Let L_2, L_3, L_3' be as in the proof of Proposition 7.1(3). By that same proof we have $L_3 \neq L_3'$. Let $\bar{L}$ be the composite of L_3 and L_3'. Then $\mathrm{Gal}(\bar{L}/\mathbb{Q})$ has order 243 and 3-rank 2, it is generated by elements of order 3, and its center has a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The group satisfying these conditions is isomorphic to $\Gamma(3^6, 40)$. $\Gamma(3^6, 40)$ has four maximal subgroups, two are isomorphic to $\Gamma(3^5, 53)$ and the others are isomorphic to $\Gamma(3^5, 2)$ or $\Gamma(3^5, 15)$. We remark that $\Gamma(3^5, 2)$ and $\Gamma(3^5, 15)$ are not generated by elements of order 3. Then $\mathrm{Gal}(\bar{L}/F)$ is isomorphic to $\Gamma(3^5, 2)$ or $\Gamma(3^5, 15)$. Since $\Gamma(3^5, 15)$ has no subgroup H such that $\Gamma(3^5, 15)/H\cong\mathrm{Gal}(L_3/F)(\cong\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z})$, $\mathrm{Gal}(\bar{L}/F)$ is isomorphic to $\Gamma(3^5, 2)$. □

Acknowledgment

I am grateful to the referee for a careful reading, for advice, and for supplying Example 7.3.

References

[Boston and Leedham-Green 1999] N. Boston and C. Leedham-Green, "Counterexamples to a conjecture of Lemmermeyer", *Arch. Math.* (*Basel*) **72**:3 (1999), 177–179. MR 99m:11131 Zbl 0922.11095

[Cohn 1978] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer, New York, 1978. MR 80c:12001 Zbl 0395.12001

[Hoechsmann 1968] K. Hoechsmann, "Zum Einbettungsproblem", *J. Reine Angew. Math.* **229** (1968), 81–106. MR 39 #5507 Zbl 0185.11202

[Iwasawa 1956] K. Iwasawa, "A note on class numbers of algebraic number fields", *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258. MR 18,644d Zbl 0074.03002

[Lemmermeyer 1997] F. Lemmermeyer, "Unramified quaternion extensions of quadratic number fields", *J. Théor. Nombres Bordeaux* **9**:1 (1997), 51–68. MR 98j:11090 Zbl 0890.11031

[Naito 1987] H. Naito, "On ℓ^3-divisibility of class numbers of ℓ-cyclic extensions", pp. 87–92 in *Algebraic number theory* (Kyoto, 1986), Proc. Symp. RIMS (Kokyuroku) **603**, 1987. Zbl 0618.12007

[Neukirch 1973] J. Neukirch, "Über das Einbettungsproblem der algebraischen Zahlentheorie", *Invent. Math.* **21** (1973), 59–116. MR 49 #2663 Zbl 0267.12005

[Nomura 1991] A. Nomura, "On the existence of unramified p-extensions", *Osaka J. Math.* **28**:1 (1991), 55–62. MR 92e:11115 Zbl 0722.11055

[Nomura 1993] A. Nomura, "On the class numbers of certain Hilbert class fields", *Manuscripta Math.* **79**:3-4 (1993), 379–390. MR 94e:11116 Zbl 0806.11053

[Nomura 2002] A. Nomura, "Notes on the existence of certain unramified 2-extensions", *Illinois J. Math.* **46**:4 (2002), 1279–1286. MR 2004d:12008 Zbl 1024.12005

[Shafarevich 1964] I. R. Shafarevich, "Extensions with given points of ramification", *Publ. Math. IHES* **18** (1964), 295–319. In Russian; French summary, pp. 93–95; translated in *Amer. Math. Soc. Transl.* **59** (1966), 128–149. Zbl 0199.09707

Received August 7, 2005. Revised November 3, 2005.

AKITO NOMURA
DEPARTMENT OF MATHEMATICS
KANAZAWA UNIVERSITY
KANAZAWA 920-1192
JAPAN
anomura@t.kanazawa-u.ac.jp