ACTA ARITHMETICA
107.4 (2003)

On the 3-class field tower of some biquadratic fields

by

EIJI YOSHIDA (Nagoya)

1. Introduction. Let K be an algebraic number field. For a prime number p, let $K^{(0)} = K$ and $K^{(i)}$ denote the Hilbert p-class field of $K^{(i-1)}$ for $i \geq 1$. Then we have the tower of fields

$$K = K^{(0)} \subseteq K^{(1)} \subseteq \ldots \subseteq K^{(\infty)} = \bigcup_{i=0}^{\infty} K^{(i)}.$$

We call this tower the *p-class field tower* of K. We say that K has a finite (resp. an infinite) p-class field tower if $|K^{(\infty)} : K| < \infty$ (resp. $|K^{(\infty)} : K| = \infty$). Golod and Shafarevich (cf. [3]) proved that there exist algebraic number fields which possess infinite class field towers. In particular, if K is a real quadratic field, they have shown that K has an infinite 2-class field tower if the 2-rank of the ideal class group of K is greater than 5. In this paper, we shall consider a number field with abelian p-class field towers (i.e. $K^{(1)} = K^{(2)}$). Hajir [5] has given all imaginary quadratic fields with abelian class field towers and Benjamin, Lemmermeyer and Snyder [1] have determined all real quadratic number fields with abelian 2-class field towers. Here we shall give a necessary and sufficient condition for the 3-class field tower of K to terminate at $K^{(1)}$, when K is a biquadratic field which contains $\sqrt{-3}$.

1.1. *Notation.* Throughout this paper, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}$ will be used in the usual sense. If L is an algebraic number field, let $L^{(1)}$ and Cl_L be the Hilbert 3-class field over L and the 3-class group (the 3-primary part of the ideal class group) of L, and h_L be the order of Cl_L. Let E_L, O_L be the group of units and the ring of integers of L respectively. If L is a Galois extension of an algebraic number field F, then $\mathrm{Gal}(L/F)$ is the Galois group for L/F. Let $K/\mathbb{Q}$ be a complex biquadratic extension and k_i be the three quadratic subfields of K. If two quadratic subfields have cyclic 3-class groups and the third one has

2000 *Mathematics Subject Classification*: 11R16, 11R37.

Key words and phrases: class field tower, biquadratic field, cubic field, ideal class group/3-class group.

trivial 3-class group, we denote these fields by k_1, k_2 and k_3 respectively. (When $k_3 = \mathbb{Q}(\sqrt{-3})$, we denote the complex subfield of K by k_1 and the real subfield of K by k_2.) In general, if L/k_i $(i = 1, 2, 3)$ is an unramified abelian extension, then $L/\mathbb{Q}$ is a Galois extension. In particular, if L/k_i is a cyclic extension with odd degree, then $\mathrm{Gal}(L/\mathbb{Q})$ is a dihedral group. Therefore if $k_i^{(1)}/k_i$ is a cyclic extension, then there exist three intermediate fields of $k_i^{(1)}/\mathbb{Q}$ which are cubic extensions over $\mathbb{Q}$ and these fields are conjugate over $\mathbb{Q}$. We denote one of the three fields by F_i if two quadratic subfields have cyclic 3-class groups and the third one has trivial 3-class group. In the case $k_3 = \mathbb{Q}(\sqrt{-3})$, we choose j $(j = 1, 2)$ for which the discriminant of k_j is divisible by 3 and denote the fundamental units of F_1 and F_2 by $\{\varepsilon_0\}$, $\{\varepsilon_1, \varepsilon_2\}$ respectively.

The purpose of this paper is the following.

Theorem 1. *Assume that $k_3 = \mathbb{Q}(\sqrt{-3})$ and set $A_1 = \{\varepsilon_0\}$, $A_2 = \{\varepsilon_1, \varepsilon_2, \varepsilon_1\varepsilon_2, \varepsilon_1\varepsilon_2^2\}$. Assume that $h_K \neq 1$. Then the 3-class field tower of K terminates at $K^{(1)}$ if and only if Cl_{k_1} is a cyclic group, and either*

- *Cl_{k_2} is trivial, or*
- *Cl_{k_2} is cyclic, and there are no $\varepsilon \in A_j$ which satisfy*

$$\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{L_j(\sqrt{-3})}}.$$

2. Proof of Theorem 1. When L is a finite extension of an algebraic number field F, we denote the map induced by extension of ideals by $\lambda_{L/F} : Cl_F \to Cl_L$. The following lemma exhibits a close relation between Cl_K and Cl_{k_i}.

Lemma 1 ([10]). *Let L be a biquadratic field of $\mathbb{Q}$. Let L_i $(i = 1, 2, 3)$ denote the three intermediate fields of L. Then the map $\lambda : Cl_{L_1} \oplus Cl_{L_2} \oplus Cl_{L_3} \to Cl_L$ given by $(\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3) \mapsto \lambda_{L/L_1}\mathfrak{A}_1 \cdot \lambda_{L/L_2}\mathfrak{A}_2 \cdot \lambda_{L/L_3}\mathfrak{A}_3$ $(\mathfrak{A}_i \in Cl_{L_i})$ is an isomorphism.*

From Lemma 1, $\lambda_{K/k_i} : Cl_{k_i} \to Cl_K$ $(i = 1, 2, 3)$ are injective and so each Cl_{k_i} can be identified with a subgroup of Cl_K. The following result will simplify our work.

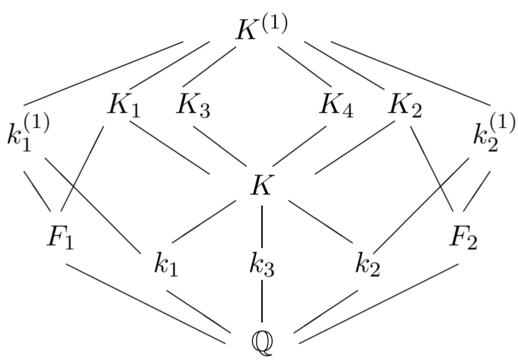
Lemma 2 ([1]). *Let L be an algebraic number field, and let r denote the p-rank of E_L/E_L^p. If the p-class field tower of L is abelian, then the rank of the p-class group of L is not greater than $(1 + \sqrt{1 + 8r})/2$.*

When K is a complex biquadratic extension of $\mathbb{Q}$ and $p = 3$, Lemma 2 implies that if $K^{(1)} = K^{(2)}$, then the rank of Cl_K is less than 3. If K has a cyclic 3-class group, then $K^{(1)} = K^{(2)}$. Hence we consider the case where $Cl_K \cong (3^s, 3^t)$ for $s, t \in \mathbb{N} - \{0\}$. (Here $(3^s, 3^t)$ means the direct product of cyclic groups of orders $3^s, 3^t$.)

LEMMA 3. *Let $K/\mathbb{Q}$ be a complex biquadratic extension with noncyclic 3-class group. If the 3-class field tower of K terminates at $K^{(1)}$, then the three quadratic subfields k_i of K can be ordered in such a way that Cl_{k_1} and Cl_{k_2} are cyclic and Cl_{k_3} is trivial.*

Proof. By Lemma 2, the 3-rank of Cl_K is 2. By Lemma 1, there are two possibilities: either two quadratic subfields have cyclic 3-class groups and the third one has trivial 3-class group, or one has 3-rank 2 and the 3-class groups of the other two are trivial. In the last case, let k denote the field with 3-rank 2. When k is a complex quadratic field, by Lemma 2, its 3-class field tower does not terminate with $k^{(1)}$. When k is a real quadratic field, by [11], its 3-class field tower does not terminate with $k^{(1)}$. Hence the same holds for K. ∎

By Lemma 3, in the case $Cl_K \cong (3^s, 3^t)$, we have the following diagram where $K_1 = KF_1$, $K_2 = KF_2$, and K_i/K are unramified cyclic cubic extensions.



From the following lemma, we see that K_i/k_3 $(i = 1, 2, 3, 4)$ are Galois extensions.

LEMMA 4 ([8]). *Let F be an algebraic number field and L be a quadratic extension of F. Suppose that the class number of F is prime to an odd prime number p and the class number of L is divisible by p. Let L' be an unramified extension of degree p over L. Then L'/F is a Galois extension and $\mathrm{Gal}(L'/F)$ is a dihedral group of order $2p$.*

Since $\mathrm{Gal}(K_i/k_3) \cong S_3$ (S_3 denotes the symmetric group of degree 3), there exist three distinct intermediate fields of K_i/k_3 which are non-Galois cubic extensions of k_3. We denote one of the three fields by L_i $(i = 1, 2, 3, 4)$. In the case $k_3 = \mathbb{Q}(\sqrt{-3})$, we can set L_i $(i = 1, 2)$ to be $F_i(\sqrt{-3})$.

Proposition 1. *If the rank of Cl_K is 2, then*

$$h_{K_i} = \frac{h_K h_{L_i}^2}{3} \quad or \quad h_{K_i} = \frac{h_K h_{L_i}^2}{9} \quad (i = 1, 2, 3, 4).$$

In order to prove Proposition 1, we use the method of Callahan [2]. If H is a finite group, we denote by H', $Z(H)$ and $|H|$ the commutator subgroup, the center, and the number of elements of H respectively. If $x, y \in H$ and H_1 is a subgroup of H, we set $x^y = y^{-1}xy$ and $(H_1)_y = \{z \in H_1 \mid z^y = z\}$. We define $V_i = \mathrm{Gal}(K_i^{(1)}/k_3)$, $U_i = \mathrm{Gal}(K_i^{(1)}/K)$ and $A_i = \mathrm{Gal}(K_i^{(1)}/K_i)$ $(i = 1, 2, 3, 4)$. By Lemma 4, we have $\mathrm{Gal}(K_i/k_3) \cong S_3 \cong V_i/A_i$. Since $K^{(1)}$ is a maximal abelian extension of K contained in $K_i^{(1)}$, $\mathrm{Gal}(K_i^{(1)}/K^{(1)}) = U_i'$. We can pick $\sigma, \tau \in V_i - A_i$ so that

$$\sigma^2 = 1, \qquad (\sigma\tau)^2 \equiv \tau^3 \equiv 1 \pmod{A_i}, \qquad \tau \in U_i,\ \sigma \in \mathrm{Gal}(K_i^{(1)}/L_i).$$

There is an action of V_i/A_i on A_i given by

$$V_i/A_i \times A_i \to A_i, \qquad (xA_i, a) \mapsto a^x.$$

This action is well defined as A_i is an abelian normal subgroup of V_i. The two automorphisms $a \mapsto a^\sigma$ and $a \mapsto a^\tau$ define an action of S_3 on A_i. Since $\lambda_{K_i/L_i} : Cl_{L_i} \to Cl_{K_i}$ is injective and $\lambda_{K_i/L_i}(Cl_{L_i})$ is mapped onto $(A_i)_\sigma$ by the Artin map, we have $Cl_{L_i} \cong (A_i)_\sigma$. Thus we study the structure of A_i and $(A_i)_\sigma$ to prove Proposition 1. First we need two lemmas.

Lemma 5 ([4, Theorem 1.4, p. 336]). *Let G be any finite group of odd order and let $\sigma : G \to G$ be an automorphism of G of order 2. Suppose that $x^\sigma = x \Leftrightarrow x = 1$. Then G is abelian.*

Lemma 6. *Let B_i be the minimal normal subgroup of U_i which contains $(A_i)_\sigma$. Then $B_i = U_i'$.*

Proof. First we define

$$(A_i)_\sigma^\tau = \{a^\tau \mid a \in (A_i)_\sigma\},$$

and show $B_i = \langle (A_i)_\sigma, (A_i)_\sigma^\tau \rangle$, the group generated by $(A_i)_\sigma$ and $(A_i)_\sigma^\tau$. Let $N_\tau : A_i \to A_i$ be defined by $N_\tau a = aa^\tau a^{\tau^2}$ for each $a \in A_i$. Then for all $a \in (A_i)_\sigma$, $N_\tau a$ is fixed by σ, τ. Since the class number of k_3 is prime to 3, we have $N_\tau a = 1$ and thus $a^{\tau^2} \in \langle (A_i)_\sigma, (A_i)_\sigma^\tau \rangle$ for all $a \in (A_i)_\sigma$. This shows that $B_i = \langle (A_i)_\sigma, (A_i)_\sigma^\tau \rangle$.

Next we prove U_i/B_i is abelian. It is clear that the automorphism $a \mapsto a^\sigma$ induces an automorphism of U_i/B_i of order 2. Assume that there exists $u \pmod{B_i}$ such that $u^\sigma \equiv u \pmod{B_i}$. If $u = \tau^l a$ for $a \in A_i$ and $l = 1, 2$, then $u^\sigma = (\tau^l a)^\sigma = (\tau^l)^\sigma a^\sigma \equiv \tau^{-l} \pmod{A_i}$. Since $u^\sigma \equiv u \pmod{A_i}$, we get $\tau^{-l} \equiv \tau^l \pmod{A_i}$. This implies $\tau \in A_i$. Therefore $u \in A_i$. Since $aa^\sigma \in (A_i)_\sigma$ for $a \in A_i$, it follows that $u^\sigma \equiv u^{-1} \pmod{B_i}$. Hence $u^\sigma \equiv u^{-1} \equiv u \pmod{B_i}$ and $u \in B_i$. Thus by Lemma 5, U_i/B_i is abelian and $B_i \supseteq U_i'$. Conversely, since $U_i/U_i' \cong \mathrm{Gal}(K^{(1)}/K)$ and from Lemma 1, we have $x^\sigma \equiv x^{-1} \pmod{U_i'}$ for $x \in U_i$. Hence $(A_i)_\sigma \subset U_i'$ and $B_i = U_i'$. ∎

Proof of Proposition 1. If $x \in (A_i)_\sigma \cap (A_i)_\sigma^\tau$, then $x = y^\tau$ for some $y \in (A_i)_\sigma$ and

$$x = x^\sigma = y^{\tau\sigma} = y^{\sigma\tau^2} = y^{\tau^2} = x^\tau.$$

Hence $x \in Z(U_i)$. On the other hand, if $x \neq 1$, we see that U_i is nonabelian. Therefore $Z(U_i) \subset A_i$ and $Z(U_i) = \{a \in A_i \mid a^\tau = a\}$. Since $Z(U_i) \cong \{\Im \in Cl_{K_i} \mid \Im^\tau = \Im\} \subset Cl_{K_i}$, from the formula for the ambiguous ideal classes of K_i/K (see [3]), $|Z(U_i)| = h_K/3$. Moreover by [6], $|\mathrm{Ker}\,\lambda_{K_i/K}| = 3 \cdot |E_K : N_{K_i/K}E_{K_i}| = 3$ or 9, hence $|\lambda_{K_i/K}(Cl_K)| = h_K/9$ or $h_K/3$ and for all $x \in \lambda_{K_i/K}(Cl_K)$, $x^\sigma = x \Leftrightarrow x = 1$. We see that $|(A_i)_\sigma \cap (A_i)_\sigma^\tau| \le 3$. Thus

$$\begin{aligned} h_{K_i} &= |A_i| = |U_i|/3 = |U_i/U_i'| \cdot |U_i'|/3 \\ &= h_K \cdot |(A_i)_\sigma| \cdot |(A_i)_\sigma^\tau|/3 \cdot |(A_i)_\sigma \cap (A_i)_\sigma^\tau| \\ &= h_K h_{L_i}^2/3 \text{ or } h_K h_{L_i}^2/9. \ \blacksquare \end{aligned}$$

If H is a finite p-group for a prime $p \in \mathbb{N}$ and $H_1 \neq \{1\}$ is any normal subgroup of H, then $Z(H) \cap H_1 \neq \{1\}$ ([4, Theorem 6.4, p. 31]). Hence if F is an algebraic number field and $F^{(2)} \neq F^{(1)}$, then there exists a normal extension F' of F such that F' is a proper intermediate field of $F^{(2)}/F^{(1)}$ and $\mathrm{Gal}(F^{(2)}/F') \subset Z(\mathrm{Gal}(F^{(2)}/F))$. Since F' is a normal extension of F which contains $F^{(1)}$, we also have a normal extension F'' of F such that F'' is a proper intermediate field of $F'/F^{(1)}$ and $\mathrm{Gal}(F'/F'') \subset Z(\mathrm{Gal}(F'/F))$. By repeating this procedure, we can find a normal extension L of F such that $|L : F^{(1)}| = 3$ and $\mathrm{Gal}(L/F^{(1)}) \subset Z(\mathrm{Gal}(L/F))$. We set $G = \mathrm{Gal}(L/F)$ and $N = \mathrm{Gal}(L/L')$ where L' is an unramified cyclic cubic extension of F. For $\sigma, \tau \in G$, we denote $\sigma^{-1}\tau^{-1}\sigma\tau$ by $[\sigma, \tau]$. In order to prove Theorem 1, we have to show the following lemma.

LEMMA 7. *Let F be an algebraic number field and assume $Cl_F \cong (3^s, 3^t)$. Then $F^{(1)} = F^{(2)}$ if and only if there is an unramified cyclic cubic extension L' of F with $h_{L'} = h_F/3$.*

Proof. Suppose that there exists an unramified cyclic cubic extension L' of F with $h_{L'} = h_F/3$ and $F^{(1)} \neq F^{(2)}$. Then $L'^{(1)} = F^{(1)}$. Hence $G' = \mathrm{Gal}(L/F^{(1)}) = \mathrm{Gal}(L/L'^{(1)}) = N'$. On the other hand, since $G/G' \cong Cl_F \cong (3^s, 3^t)$, G is generated by two elements σ_1 and σ_2. Since $|G'| = 3$, we can pick σ_1, σ_2 so that $G' = \langle [\sigma_1, \sigma_2] \rangle$. Notice that N is the subgroup of G. Hence index 3 of N is one of the four subgroups $\langle \sigma_1, \sigma_2^3, G' \rangle$, $\langle \sigma_2, \sigma_1^3, G' \rangle$, $\langle \sigma_1\sigma_2, \sigma_2^3, G' \rangle$, and $\langle \sigma_1\sigma_2^2, \sigma_2^3, G' \rangle$. As $G' \subset Z(G)$ and $|G'| = 3$, we have $[\sigma_1^i, \sigma_2^{3j}] = [\sigma_1, \sigma_2]^{3ij} = 1$ $(i, j \in \mathbb{Z})$. This implies that $\langle \sigma_1, \sigma_2^3, G' \rangle' = \{1\}$. Similarly $\langle \sigma_2, \sigma_1^3, G' \rangle' = \langle \sigma_1\sigma_2, \sigma_2^3, G' \rangle' = \langle \sigma_1\sigma_2^2, \sigma_2^3, G' \rangle' = \{1\}$. Hence $N' =$

$\{1\}$. This contradicts $F^{(1)} = L'^{(1)}$. Conversely, if $F^{(1)} = F^{(2)}$, it is easy to see that $F^{(1)} = L'^{(1)}$, and hence $h_{L'} = h_F/3$. ∎

We shall consider whether $h_{L_i} = 1$ or not. If $k_3 = \mathbb{Q}(\sqrt{-3})$, then the following proposition holds.

PROPOSITION 2. *Assume that* $Cl_K \cong (3^s, 3^t)$ *and* $k_3 = \mathbb{Q}(\sqrt{-3})$. *Then the class number of* L_j *is divisible by* 3 *if and only if there exists* $\varepsilon \in A_j$ *such that* $\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}}$.

Proof. We consider the decomposition of the prime ideals of F_j. The ideal of k_j lying above 3 is completely decomposed in $k_j^{(1)}$ because 3 is ramified in k_j. Hence the decomposition of 3 in F_j is

$$3 = \mathfrak{p}_1 \mathfrak{p}_2^2$$

where $\mathfrak{p}_i$ $(i = 1, 2)$ are ideals of F_j lying above 3. Suppose that $h_{L_j} \neq 1$. Let L' be an unramified cyclic cubic extension over L_j. Since Cl_{k_j} is cyclic, the class number of F_j is prime to 3. Hence L'/F_j is a normal extension from Lemma 4. Moreover, by Kummer theory, $L' = L_j(\sqrt[3]{\alpha})$ where $\alpha \in L_j^* - L_j^{*3}$ $(L_j^* = L_j - \{0\})$, α is prime to 3 and $(\alpha) = \mathfrak{A}^3$ ($\mathfrak{A}$ is an ideal of L_j). Let $\sigma' \in \mathrm{Gal}(L'/F_j)$ be an extension of the nontrivial automorphism of L_j over F_j. Then $\alpha^{\sigma'} \equiv \alpha \pmod{L_j^{*3}}$. Hence $L' = L_j(\sqrt[3]{\alpha}) = L_j(\sqrt[3]{N_{L_j/F_j}\alpha})$ where N_{L_j/F_j} is a norm from L_j to F_j. Furthermore, since the class number of F_j is prime to 3, we can put $\varepsilon \in A_j$ so that $L' = L_j(\sqrt[3]{\varepsilon})$.

The decompositions of $\mathfrak{p}_i$ $(i = 1, 2)$ in L_j are either

- $\mathfrak{p}_1 = \mathfrak{P}_1^2,\ \mathfrak{p}_2 = \mathfrak{P}_2\mathfrak{P}_3$ or
- $\mathfrak{p}_1 = \mathfrak{P}_1^2,\ \mathfrak{p}_2 = \mathfrak{P}_2,\ N_{L_j/F_j}\mathfrak{P}_2 = \mathfrak{p}_2^2$,

where $\mathfrak{P}_i$ $(i = 1, 2, 3)$ are prime ideals of L_j lying above 3. Since $L' = L_j(\sqrt[3]{\varepsilon})$ is unramified, the equation $X^3 \equiv \varepsilon \pmod{\mathfrak{P}_i^3}$ has a root in O_{L_j} for $i = 1, 2, 3$. Assume that $\mathfrak{p}_2 = \mathfrak{P}_2\mathfrak{P}_3$. Since $O_{L_j}/\mathfrak{P}_i^3 \cong O_{\mathbb{Q}(\sqrt{-3})}/(\sqrt{-3}^3)$, we have $\varepsilon \equiv \pm 1 \pmod{\mathfrak{P}_i^3}$ for $i = 1, 2, 3$. Hence $\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}}$.

Assume that $\mathfrak{p}_2 = \mathfrak{P}_2$ and $N_{L_j/F_j}\mathfrak{P}_2 = \mathfrak{p}_2^2$. Let $\alpha = \alpha_1 + \alpha_2\sqrt{-3} \in O_{L_j}$ $(\alpha_1, \alpha_2 \in F_j)$ satisfy $\alpha^3 \equiv \varepsilon \pmod{\mathfrak{P}_2^3}$. Since $2\alpha_1, 2\alpha_2\sqrt{-3} \in O_{L_j}$, we can make $\alpha_1, \alpha_2\sqrt{-3} \in O_{L_j}$ by replacing $\alpha_1, \alpha_2\sqrt{-3}$ with $-2\alpha_1, -2\alpha_2\sqrt{-3}$. Since $\mathfrak{p}_2 = \mathfrak{P}_2$, we see that $(\alpha_1 - \alpha_2\sqrt{-3})^3 \equiv \varepsilon \pmod{\mathfrak{P}_2^3}$. Hence

$$\begin{aligned} \alpha^3 - (\alpha_1 - \alpha_2\sqrt{-3})^3 &= (\alpha_1 + \alpha_2\sqrt{-3})^3 - (\alpha_1 - \alpha_2\sqrt{-3})^3 \pmod{\mathfrak{P}_2^3} \\ &= 2(3\alpha_1^2\alpha_2\sqrt{-3} - 3\alpha_2^3\sqrt{-3}) \equiv 0 \pmod{\mathfrak{P}_2^3}. \end{aligned}$$

Since $3\alpha_1^2 \in \mathfrak{P}_2$, we have $-3\alpha_2^3\sqrt{-3} \in \mathfrak{P}_2$ and hence $\alpha_2\sqrt{-3} \in \mathfrak{P}_2$. Consequently,

$$\alpha^3 \equiv \alpha_1^3 + 3\alpha_1^2\alpha_2\sqrt{-3} - 9\alpha_1\alpha_2^2 - 3\alpha_2^3\sqrt{-3} \equiv \alpha_1^3 \pmod{\mathfrak{P}_2^3}.$$

We have $\varepsilon \equiv \pm 1 \pmod{\mathfrak{P}_i^3}$ for $i = 1, 2$. Thus $\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}}$.

Conversely, if there exists $\varepsilon \in A_j$ such that $\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}}$, then $\varepsilon \equiv \pm 1 \pmod{\mathfrak{P}_i^3}$ ($i = 1, 2, 3$ or $i = 1, 2$) and $L_j(\sqrt[3]{\varepsilon})$ is an unramified cyclic cubic extension over L_j. ■

The next result is well known.

LEMMA 8 ([12, Theorem 10.10, p. 190]). *Let $d > 1$ be square-free. Let r_1 (resp. r_2) be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$ (resp. $\mathbb{Q}(\sqrt{d})$). Then*

$$r_2 \le r_1 \le r_2 + 1.$$

Proof of Theorem 1. If $K^{(1)} = K^{(2)}$, we see that Cl_K is a nontrivial cyclic group or an abelian group of rank 2 from Lemma 2. If Cl_K is a nontrivial cyclic group, then Cl_{k_1} is a nontrivial cyclic group and Cl_{k_2} is trivial from Lemmas 1 and 8. If Cl_K is an abelian group of rank 2, then Cl_{k_1} and Cl_{k_2} are nontrivial cyclic groups. In this case $h_{K_i} = h_K/3$ for all $i = 1, 2, 3, 4$. By Propositions 1 and 2, F_j has no unit which satisfies the condition of Theorem 1. Conversely, if F_j has no such unit, then $h_{L_j} = 1$ and $h_{K_j} = h_K/3$ by Proposition 1. By Lemma 7, we have $K^{(1)} = K^{(2)}$. ■

3. Some examples. From the proof of Proposition 2, we see that

$$\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}} \ \Leftrightarrow\ \varepsilon^2 \equiv 1 \pmod{\mathfrak{p}_1^2\mathfrak{p}_2^3},$$

where $\mathfrak{p}_1$, $\mathfrak{p}_2$ are distinct prime ideals of O_{F_j} lying above 3 and $3 = \mathfrak{p}_1\mathfrak{p}_2^2$. Let

$$x^3 + ax^2 + bx - 1 \quad (a, b \in \mathbb{Z})$$

be the minimal polynomial of ε^2. Then the minimal polynomial of $\varepsilon^2 - 1$ is

$$x^3 + (a+3)x^2 + (2a+b+3)x + a + b.$$

Since $\varepsilon^2 - 1 \in \mathfrak{p}_1^2\mathfrak{p}_2^3$, we see that

$$\frac{\varepsilon^2 - 1}{3} \in O_{F_j}, \quad 27 \mid a+b, \quad 9 \mid 2a+b+3, \quad a+3 = 2a+b+3-(a+b).$$

Moreover, since

$$(\varepsilon^2-1)^3 \in \mathfrak{p}_2^9, \quad (a+3)(\varepsilon^2-1)^2 \in \mathfrak{p}_2^{10}, \quad (2a+b+3)(\varepsilon^2-1) \in \mathfrak{p}_2^7,$$

we have $81 \mid a+b$.

The minimal polynomial of $\varepsilon^2 + a/3$ is

$$x^3 - 3(a_0^2 - b_0)x + 2a_0^3 - 3a_0b_0 - 1,$$

where $a = 3a_0$, $b = 3b_0$, and we see that

$$3(a_0^2 - b_0) = \frac{(a+3)^2}{3} - (2a+b+3),$$

$$2a_0^3 - 3a_0b_0 - 1 = \frac{2(a+3)^3}{27} - \frac{(a+3)(2a+b+3)}{3} + a + b.$$

The next lemma concerns the decomposition of ideals of a cubic field.

Lemma 9 ([7]). *Let L be a cubic field over $\mathbb{Q}$ and let α be a primitive element of L whose minimal polynomial is $x^3 - ax + b$ where $a, b \in \mathbb{Z}$, $a, b \neq 0$. Define $v_3(m) = \max\{s \mid 3^s \mid m\}$. Then $3 = \mathfrak{p}_1\mathfrak{p}_2^2$ if and only if either*

- $v_3(a) = 2t + 1$, $v_3(b) \geq 3t + 2$, *or*
- $v_3(a) \geq 2t + 1$, $v_3(b) = 3t$, *and either*
  - — $a/3^{2t} \equiv 3 \pmod 9$, $(b/3^{3t})^2 \equiv a/3^{2t} + 1 \pmod{27}$ *and* $v_3(4a^3 - 27b^2)$ *is odd, or*
  - — $a/3^{2t} \equiv 6, 0 \pmod 9$, $(b/3^{3t})^2 \equiv a/3^{2t} + 1 \pmod 9$.

By the above lemma and since $9 \mid a + 3, 2a + b + 3$, we see that

$$27 \left| \frac{(a+3)^2}{3} - (2a + b + 3), \qquad 27 \mid a + 3, 2a + b + 3.\right.$$

As $81 \mid a + b$, we have

$$3^5 \mid 2a_0^3 - 3a_0b_0 - 1, \qquad 3^5 \mid a + b.$$

Thus if $\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3}\cdot O_{F_j(\sqrt{-3})}}$, then $27 \mid a+3, 2a+b+3$ and $3^5 \mid a+b$. Conversely, it is easy to see that if $27 \mid a + 3, 2a + b + 3$ and $3^5 \mid a + b$, then $\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}}$. Thus

$$\varepsilon^2 \equiv 1 \pmod{3\sqrt{-3} \cdot O_{F_j(\sqrt{-3})}} \;\Leftrightarrow\; 27 \mid a + 3, 2a + b + 3,\; 3^5 \mid a + b.$$

By utilizing the above fact, one can find examples of $K^{(1)} = K^{(2)}$ and $K^{(1)} \neq K^{(2)}$.

An example of $K^{(1)} = K^{(2)}$. Let $F = \mathbb{Q}(\theta)$ be a cubic extension over $\mathbb{Q}$ with $\theta^3 - 9m\theta^2 - 1 = 0$ ($m \in \mathbb{N} - \{0\}$) and let $k = \mathbb{Q}(\sqrt{-3(4(3m)^3 + 1)})$. From [7], we see that kF/k is an unramified cyclic cubic extension. Furthermore by [9], the root of the equation $x^3 - 9mx^2 - 1 = 0$ is either a fundamental unit of F or its square. It is clear that θ does not satisfy the condition of Theorem 1 and since $(\theta^2)^3 - 81m^2(\theta^2)^2 + 18m(\theta^2) - 1 = 0$, neither does θ^2. Therefore the following holds.

Corollary 1. *Let $K = \mathbb{Q}(\sqrt{-3(4(3m)^3 + 1)}, \sqrt{-3})$ ($m \in \mathbb{N} - \{0\}$). Assume that $Cl_K \cong (3^s, 3^t)$. Then $K^{(1)} = K^{(2)}$.*

An example of $K^{(1)} \neq K^{(2)}$. Let $F = \mathbb{Q}(\theta)$ with $\theta^3 + 3\theta + a^3 = 0$ where $a \in \mathbb{N} - \{0\}$ and let $k = \mathbb{Q}(\sqrt{-3(a^6 + 4)})$. By [7], if $3 \mid a$, then Fk/k is an unramified cyclic cubic extension. The minimal polynomial of $1 - a^2 - a\theta$ is

$$x^3 + 3(a^2 - 1)x^2 + (3(a^2 - 1)^2 + 3a^2)x - 1.$$

Assume that $a \not\equiv 0 \pmod 7$. The discriminant of x^3+3x+a^3 is $-27(a^6+4) \equiv 5 \not\equiv 0 \pmod 7$. Moreover

$$\begin{aligned} &x^3+3x+a^3 \\ &\equiv \begin{cases} x^3+3x+1 \equiv (x+3)(x^2-3x+5) \pmod 7 & \text{if } a^3 \equiv 1 \pmod 7, \\ x^3+3x-1 \equiv (x-3)(x^2+3x+5) \pmod 7 & \text{if } a^3 \equiv -1 \pmod 7. \end{cases}\end{aligned}$$

Hence $\mathfrak{p} = (\theta+3, 7)$ ($a^3 \equiv 1 \pmod 7$) and $\mathfrak{p} = (\theta-3, 7)$ ($a^3 \equiv -1 \pmod 7$) are prime ideals of F lying above 7 whose relative degree is 1.

If $a \not\equiv 0 \pmod 7$, the polynomial $x^3-(1-a^2-a\theta)$ is irreducible in $O_F/\mathfrak{p}$ because if $a \not\equiv 0 \pmod 7$, then $x^3-(1-a^2-a\theta) \equiv x^3 \pm 3 \pmod{\mathfrak{p}}$. Thus $1-a^2-a\theta \notin E_F^3$ since if $3 \mid a$, then $27 \mid 3a^2 = 3(a^2-1)+3$, $27 \mid 3a^2+3a^4$ and $3^5 \mid 3a^4 = 3(a^2-1)+3(a^2-1)^2+3a^2$. Therefore the class number of $L_j = F(\sqrt{-3})$ is divisible by 3. Suppose that Cl_K is cyclic where $K = \mathbb{Q}(\sqrt{-3(a^6+4)}, \sqrt{-3})$. Then $\mathrm{Gal}(K^{(1)}/\mathbb{Q}(\sqrt{-3}))$ is a dihedral group and so is $\mathrm{Gal}(K^{(1)}/F(\sqrt{-3}))$. Hence $F(\sqrt{-3})(\sqrt[3]{1-a^2-a\theta})$ is not contained in $K^{(1)}$. This is a contradiction. Hence the 3-rank of the ideal class group of $K = \mathbb{Q}(\sqrt{-3(a^6+4)}, \sqrt{-3})$ is greater than 2. Consequently, the following holds.

Corollary 2. *Let $K = \mathbb{Q}(\sqrt{-3(a^6+4)}, \sqrt{-3})$. Assume that $a \not\equiv 0 \pmod 7$ and $a \equiv 0 \pmod 3$. Then $K^{(1)} \neq K^{(2)}$.*

Example 1: $k_1 = \mathbb{Q}(\sqrt{-237})$, $k_2 = \mathbb{Q}(\sqrt{79})$, $k_3 = \mathbb{Q}(\sqrt{-3})$. Then for $K = \mathbb{Q}(\sqrt{-237}, \sqrt{-3})$ we have $Cl_K \cong (3,3)$ and $k_j = k_1 = \mathbb{Q}(\sqrt{-237})$, and a primitive element of F_1 is one of the roots of the polynomial

$$x^3-3x-160.$$

A fundamental unit of F_1 is the root of

$$x^3-149x^2+23357x-1.$$

The root of

$$x^3+24513x^2+545549151x-1$$

is the second power of the fundamental unit of F_1. Then 149 is prime to 3, and $27 \parallel 24513+3$, $27 \parallel 545549151+24513$. Therefore F_1 has no unit which satisfies the assumption of Theorem 1. Thus for $K = \mathbb{Q}(\sqrt{-237}, \sqrt{-3})$, $K^{(1)} = K^{(2)}$.

Example 2: $k_1 = \mathbb{Q}(\sqrt{-12540667})$, $k_2 = \mathbb{Q}(\sqrt{3 \cdot 12540667})$, $k_3 = \mathbb{Q}(\sqrt{-3})$. Then $3 \parallel h_{k_1} = 3$ and $3 \parallel h_{k_2} = 3$. (The class numbers of k_1 and k_2 are 609 and 3 respectively). As a unit of $F_j = F_2$ which satisfies the assumption of Theorem 1, we can take a root of

$$x^3-2190x^2+179337x-1.$$

Then $3^7 \parallel -2190+3,\ 3^{11} \parallel -2190+179337$ and this root is not the cube of any unit of F_2. The class number of L_2 is 27 and $K^{(1)} \neq K^{(2)}$.

We calculated these results by KASH.

References

[1] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower*, J. Number Theory 73 (1998), 182–194.

[2] T. Callahan, *The 3-class groups of non-Galois cubic fields, 1*, Mathematika 21 (1974), 72–89.

[3] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.

[4] D. Gorenstein, *Finite Groups*, Harper & Row, 1968.

[5] F. Hajir, *On the class numbers of Hilbert class fields*, Pacific J. Math. 1997, Olga Taussky-Todd memorial issue, 177–187.

[6] F.-P. Heider und B. Schmithals, *Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen*, J. Reine Angew. Math. 336 (1982), 1–25.

[7] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. 87 (1983), 579–585.

[8] D. J. Madden and W. Y. Vélez, *A note on the normality of unramified, abelian extensions of quadratic extensions*, Manuscripta Math. 30 (1980), 343–349.

[9] R. Morikawa, *On units of certain cubic number fields*, Abh. Math. Sem. Univ. Hamburg 39 (1973), 72–77.

[10] N. Nakagoshi, *On the class number relations of abelian extensions whose Galois groups are of type* (p,p), Math. Rep. Toyama Univ. 4 (1981), 91–106.

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

[12] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

Graduate School of Mathematics
Nagoya University
Chikusa-ku, Nagoya 464-8602, Japan
E-mail: m98111i@math.nagoya-u.ac.jp

Received on 18.1.2002
and in revised form on 6.5.2002 (4190)