TOKYO J. MATH.
VOL. 27, NO. 2, 2004

On the Sylow p-Subgroups of the Ideal Class Groups of Some Imaginary Cyclic Fields of Degree $p-1$

Yasuhiro KISHI

Tokyo Metropolitan University

(Communicated by Y. Ohnita)

Introduction

In this paper, we investigate how to construct imaginary cyclic fields of degree $p-1$ whose Sylow p-subgroups of the ideal class groups are not cyclic. This paper supplements our previous paper [6].

For a given integer n, Yamamoto [10] proved that there exist infinitely many imaginary quadratic fields whose ideal class groups contain $(\mathbf{Z}/n\mathbf{Z})^2$ as a subgroup. Moreover, Nakano [7] proved that there exist infinitely many algebraic number fields K of fixed degree $m = r_1 + 2r_2$ whose ideal class groups contain $(\mathbf{Z}/n\mathbf{Z})^{r_2+1}$ as a subgroup, where r_1 and r_2 denote the number of real and imaginary embeddings of K into $\mathbf{C}$, respectively. (Other related papers are those by Ishida [5] and Azuhata and Ichimura [1].) In the present paper, we give another way to construct imaginary cyclic fields of degree $p-1$ whose ideal class groups contain $(\mathbf{Z}/p\mathbf{Z})^2$ as a subgroup for a given prime p with $p \equiv 1 \pmod 4$.

Let p be a fixed odd prime. Let ζ be a primitive p-th root of unity and put $\omega := \zeta + \zeta^{-1}$. In Section 1, we give a sufficient condition for an imaginary cyclic field of degree $p-1$ containing $\mathbf{Q}(\omega)$ to have class number divisible by p (Theorem 1.1). We can easily verify whether our condition holds for given imaginary cyclic fields of degree $p-1$ or not (see Proposition 3.2). The condition which was given in our previous paper [6] is included in the present one, as we will see in (2) of Remark 1.2. In Section 2, there are two goals. The first is to prove Theorem 1.1. The second is to give infinitely many imaginary quadratic fields of degree $p-1$ containing $\mathbf{Q}(\omega)$ whose class numbers are divisible by p. This gives another proof of [6, Theorem 2]. In Section 3, we construct imaginary cyclic fields of degree $p-1$ which have ideal class groups of p-ranks greater than one in the case of $p \equiv 1 \pmod 4$. Moreover we give a parametric family of such fields (Example 3.5). Unfortunately, the author has not yet determined whether this family is infinite.

Received July 15, 2003
The author was supported by JSPS Research Fellowships for Young Scientists.

1. The main theorem

Let p be a fixed odd prime. Let ζ be a primitive p-th root of unity and put $\omega := \zeta + \zeta^{-1}$. Let $M(\neq \mathbf{Q}(\zeta))$ be an imaginary cyclic field of degree $p-1$ which contains $\mathbf{Q}(\omega)$. Assume that p satisfies $p \equiv 1 \pmod 4$. Then $M(\zeta)$ has exactly two real quadratic subfields which are not contained in M. We denote them by k_1 and k_2. Assume, on the contrary, that p satisfies $p \equiv 3 \pmod 4$. Then there is only one real quadratic subfield of $M(\zeta)$ which is not contained in M. We denote it by k_3. (See Figure 1.)

Conversely, for a real quadratic field k with $\mathbf{Q}(\zeta) \cap k = \mathbf{Q}$, the imaginary cyclic subfield M of degree $p-1$ in $k(\zeta)$ is uniquely determined; then we can express $M = \mathbf{Q}(\sqrt{d}(\zeta - \zeta^{-1}))$, where d is the discriminant of k.

For a number field K, let denote the norm map and the trace map of $K/\mathbf{Q}$ by N_K and Tr_K, respectively. For an element γ of $k = k_l$ ($l = 1$, 2, or 3) $\subset M(\zeta)$, we define a polynomial $f(X;\gamma)$ by

$$f(X;\gamma) := \sum_{i=0}^{(p-1)/2} (-N_k(\gamma))^i \frac{p}{p-2i}\binom{p-i-1}{i} X^{p-2i} - N_k(\gamma)^{(p-1)/2}\mathrm{Tr}_k(\gamma)\,.$$

We denote the minimal splitting field of $f(X;\gamma)$ over $\mathbf{Q}$ by K_γ. Then K_γ contains M if $f(X;\gamma)$ is irreducible over $\mathbf{Q}$ (cf. [4, Corollary 2.6]).

THEOREM 1.1. *Let the notation be as above. Assume that there exists a unit ε of $k = k_l$ ($l = 1$, 2, or 3) which satisfies the condition*

$$(1.1)\qquad \begin{cases} N_k(\varepsilon) = 1\,, \\ \mathrm{Tr}_k(\varepsilon) \equiv \pm 2 \pmod{p^3}\,, \\ \varepsilon \notin k^p\,. \end{cases}$$

Then K_ε is an unramified cyclic extension of M of degree p. Hence the class number of M is divisible by p.

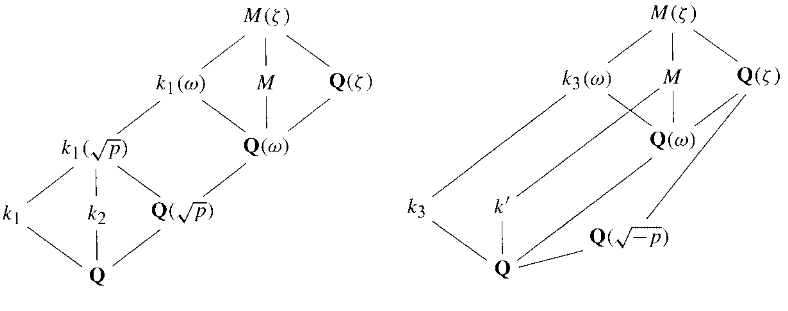

FIGURE 1

REMARK 1.2. (1) We may replace the condition (1.1) by

$$\begin{cases} \mathrm{Tr}_k(\varepsilon)^2 \equiv 4N_k(\varepsilon) \pmod{p^3}\,, \\ \varepsilon \notin k^p \end{cases} \tag{1.2}$$

in the statement of Theorem 1.1. Indeed, a unit satisfying (1.1) also satisfies (1.2), and the square of a unit satisfying (1.2) satisfies (1.1).

(2) In [6], we gave another sufficient condition

$$\begin{cases} \mathrm{Tr}_k(\varepsilon) \equiv 0 \pmod{p^2}\,, \\ \varepsilon \notin k^p \end{cases} \tag{1.3}$$

for p to divide the class number of M. This result is included in Theorem 1.1; indeed, if a unit ε satisfies (1.3), then the square ε^2 satisfies (1.1).

2. Proof of Theorem 1.1

Before proving Theorem 1.1, we prepare some propositions. First we extract a result from Sase [9, Proposition 2]. For a prime number p and an integer m, we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $v_p(m)$.

PROPOSITION 2.1 (Sase). *Let p be an odd prime number. Let θ be a root of the polynomial*

$$g(X) = X^p + \sum_{j=0}^{p-2} a_j X^j\,, \quad a_j \in \mathbf{Z}\,.$$

Suppose that $g(X)$ is irreducible over $\mathbf{Q}$ and the condition $v_p(a_j) < p - j$ holds for some j, $0 \le j \le p-2$. Then p is totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$ if and only if one of the following conditions (S-i), (S-ii) *holds*:

(S-i) $\quad 0 < \dfrac{v_p(a_0)}{p} \le \dfrac{v_p(a_j)}{p-j}$ *for every* j, $1 \le j \le p-2$;

(S-ii) (S-ii-1) $\quad v_p(a_0) = 0\,,$

(S-ii-2) $\quad v_p(a_j) > 0$ *for every* j, $1 \le j \le p-2\,,$

(S-ii-3) $\quad \dfrac{v_p(g(-a_0))}{p} \le \dfrac{v_p(g^{(j)}(-a_0))}{p-j}$ *for every* j, $1 \le j \le p-2$,

(S-ii-4) $\quad v_p(g^{(j)}(-a_0)) < p - j$ *for some* j, $0 \le j \le p-1\,,$

where $g^{(j)}(X)$ is the j-th differential of $g(X)$.

REMARK 2.2. In [9], Sase also determined the conditions for a general prime q with $q \ne \deg(g)$ to be totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$.

For an integer $n \geq 0$, we define two functions $T_n(x)$ and $U_n(x)$ by

$$T_n(x) := \cos n\theta\,, \quad U_n(x) := \frac{\sin(n+1)\theta}{\sin\theta}\,,$$

respectively, where $x = \cos\theta$. (The former is called *the Chebyshev polynomial* while the latter is called *the Chebyshev polynomial of second kind*.) Then we have

$$T_n(x) = \frac{(x+\sqrt{x^2-1})^n + (x-\sqrt{x^2-1})^n}{2}\,,$$

$$U_{n-1}(x) = \frac{(x+\sqrt{x^2-1})^n - (x-\sqrt{x^2-1})^n}{2\sqrt{x^2-1}}$$

(cf. [8, Chapter 1, pp. 5 and 10]). Then we have

$$T_p\left(\frac{\varepsilon+\bar{\varepsilon}}{2}\right) = \frac{\varepsilon^p+\bar{\varepsilon}^p}{2}\,, \quad U_{p-1}\left(\frac{\varepsilon+\bar{\varepsilon}}{2}\right) = \frac{\varepsilon^p-\bar{\varepsilon}^p}{\varepsilon-\bar{\varepsilon}}\,.$$

Moreover, each function has another expression:

$$2T_n\left(\frac{x}{2}\right) = \sum_{i=0}^{[n/2]}(-1)^i\frac{n}{n-2i}\binom{n-i-1}{i}x^{n-2i}\,,$$

$$U_n\left(\frac{x}{2}\right) = \sum_{i=0}^{[n/2]}(-1)^i\binom{n-i}{i}x^{n-2i}$$

(cf. [8, Chapter 1, p. 60]). By putting $x = (\varepsilon+\bar{\varepsilon})/2$, therefore, we obtain

LEMMA 2.3. *For a unit ε of k with $N_k(\varepsilon) = 1$ and for an odd integer p, the following equations holds*:

$$\frac{\varepsilon^p+\bar{\varepsilon}^p}{\varepsilon+\bar{\varepsilon}} = \sum_{i=0}^{(p-1)/2}(-1)^i\frac{p}{p-2i}\binom{p-i-1}{i}\mathrm{Tr}_k(\varepsilon)^{p-2i-1}\,, \tag{2.1}$$

$$\frac{\varepsilon^p-\bar{\varepsilon}^p}{\varepsilon-\bar{\varepsilon}} = \sum_{i=0}^{(p-1)/2}(-1)^i\binom{p-i-1}{i}\mathrm{Tr}_k(\varepsilon)^{p-2i-1}\,, \tag{2.2}$$

where $\bar{\varepsilon}$ is the conjugate of ε in k.

PROOF OF THEOREM 1.1. Assume that a real quadratic field k has a unit ε satisfying the condition (1.1). Then $f(X;\varepsilon)$ is irreducible over $\mathbf{Q}$ and K_ε is a cyclic extension of M of degree p (see [2, Chapter 5], [4, Proposition 1.10]). Moreover, K_ε is normal over $\mathbf{Q}$ and its Galois group $\mathrm{Gal}(K_\varepsilon/\mathbf{Q})$ is isomorphic to the Frobenius group of order $p(p-1)$ (see [4, Theorem 2.1]). Furthermore, K_ε/M is unramified outside p (see [6, Proof of Theorem 1]). By class field theory, therefore, it is sufficient to show that prime divisors of p in M is unramified in K_ε.

Let θ be a root of $f(X;\varepsilon)$. Let q be a prime number in general. A prime divisor of q in M is ramified in K_ε if and only if q is totally ramified in $\mathbf{Q}(\theta)$ because $[K_\varepsilon : M]$ and $[M : \mathbf{Q}]$ are relatively prime. Hence we have only to verify whether the prime p is totally ramified in $\mathbf{Q}(\theta)$ or not.

Express $\varepsilon = (a + b\sqrt{d})/2$ $(a,\ b \in \mathbf{Z})$. Since ε satisfies (1.1), we have $p \mid b$ and $p \nmid a$. Then by

$$\varepsilon^p = \frac{1}{2^p}(a^p + pa^{p-1}b\sqrt{d} + \cdots + pab^{p-1}d^{\frac{p-1}{2}} + b^p d^{\frac{p-1}{2}}\sqrt{d}),$$
$$\bar{\varepsilon}^p = \frac{1}{2^p}(a^p - pa^{p-1}b\sqrt{d} + \cdots + pab^{p-1}d^{\frac{p-1}{2}} - b^p d^{\frac{p-1}{2}}\sqrt{d}),$$

we have

$$\varepsilon^p + \bar{\varepsilon}^p \equiv \frac{1}{2^{p-1}}a^p \pmod{p^3}.$$

Thus we get

$$\frac{\varepsilon^p + \bar{\varepsilon}^p}{\varepsilon + \bar{\varepsilon}} - 1 \equiv \left(\frac{a}{2}\right)^{p-1} - 1 \equiv \left(\frac{\pm 2}{2}\right)^{p-1} - 1 = 0 \pmod{p^3} \tag{2.3}$$

by using $\varepsilon + \bar{\varepsilon} = a$. On the other hand, we have

$$\varepsilon^p - \bar{\varepsilon}^p = \frac{1}{2^{p-1}}(pa^{p-1}b\sqrt{d} + p^2bt\sqrt{d})$$

for some $t \in \mathbf{Z}$ and

$$\varepsilon - \bar{\varepsilon} = b\sqrt{d}.$$

Then we have

$$\frac{\varepsilon^p - \bar{\varepsilon}^p}{\varepsilon - \bar{\varepsilon}} = \frac{1}{2^{p-1}}(pa^{p-1} + p^2t),$$

and hence

$$v_p\left(\frac{\varepsilon^p - \bar{\varepsilon}^p}{\varepsilon - \bar{\varepsilon}}\right) = 1. \tag{2.4}$$

Moreover we have

(2.5)

$$\begin{aligned} f(\mathrm{Tr}_k(\varepsilon);\varepsilon) &= \sum_{i=0}^{(p-1)/2} (-N_k(\varepsilon))^i \frac{p}{p-2i}\binom{p-i-1}{i}\mathrm{Tr}_k(\varepsilon)^{p-2i} - N_k(\varepsilon)^{(p-1)/2}\mathrm{Tr}_k(\varepsilon) \\ &= \mathrm{Tr}_k(\varepsilon)\left(\sum_{i=0}^{(p-1)/2} (-1)^i \frac{p}{p-2i}\binom{p-i-1}{i}\mathrm{Tr}_k(\varepsilon)^{p-2i-1} - 1\right) \end{aligned}$$

and

$$f'(\mathrm{Tr}_k(\varepsilon);\varepsilon) = p\left(\sum_{i=0}^{(p-1)/2}(-1)^i\binom{p-i-1}{i}\mathrm{Tr}_k(\varepsilon)^{p-2i-1}\right). \tag{2.6}$$

Therefore, by (2.1), (2.3), (2.5) we have

$$v_p(f(\mathrm{Tr}_k(\varepsilon);\varepsilon)) \geq 3\,, \tag{2.7}$$

and by (2.2), (2.4), (2.6) we have

$$v_p(f'(\mathrm{Tr}_k(\varepsilon);\varepsilon)) = 2\,. \tag{2.8}$$

Now let us apply Proposition 2.1 to $f(X;\varepsilon)$. Since the constant term of $f(X;\varepsilon)$ is not divisible by p, the condition (S-i) does not hold. Moreover by (2.7) and (2.8), the condition (S-ii-3) does not hold for $j = 1$ when $p \geq 5$. In the case $p = 3$, the equation (2.8) assures that (S-ii-4) does not hold for $j = 1$. Therefore p is not totally ramified in $\mathbf{Q}(\theta)$. This completes the proof of Theorem 1.1. □

In the following example, we shall give an infinite family of quadratic fields which have units satisfying the condition (1.1).

EXAMPLE 2.4. Take a prime q so that we have

$$\begin{cases} q \equiv 4 \pmod{p^5}\,, \\ q \not\equiv 4 \pmod{p^6}\,. \end{cases} \tag{2.9}$$

Express

$$q = ap^5 + 4\,, \quad a = bc^2 \quad (b,\ c \in \mathbf{Z},\ b : \text{square-free})$$

and put $D := bpq$. Then it is clear that D is square-free. Since

$$D = bp(ap^5+4) = abp^6 + 4bp = (bcp^3)^2 + 4bp\,,$$

$\mathbf{Q}(\sqrt{D})$ is a real quadratic field of Richaud-Degert type. It is well-known that

$$\varepsilon_0 := \frac{bc^2p^5 + 2 + cp^2\sqrt{D}}{2}$$

is the fundamental unit of $\mathbf{Q}(\sqrt{D})$ (cf. [3], [11, Lemma 2]). Since

$$N_{\mathbf{Q}(\sqrt{D})}(\varepsilon_0) = \frac{(bc^2p^5+2)^2 - c^2p^4\{(bcp^3)^2+4bp\}}{4} = 1$$

and

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{D})}(\varepsilon_0)^2 = (bc^2p^5+2)^2 \equiv 4 \pmod{p^3}\,,$$

the unit ε_0 satisfies (1.1).

For each prime p, the existence of infinitely many primes q satisfying the above condition (2.9) is assured by Dirichlet's Theorem on primes in arithmetic progressions.

3. Imaginary cyclic fields of degree $p-1$ with p-ranks ≥ 2

In this section, we study a way to construct imaginary cyclic fields of degree $p-1$ which have ideal class groups of p-ranks greater than one in the case of $p \equiv 1 \pmod 4$.

From now on, we assume that $p \equiv 1 \pmod 4$. As we have seen in Section 1, for an imaginary cyclic field $M(\neq \mathbf{Q}(\zeta))$ of degree $p-1$ which contains $\mathbf{Q}(\omega)$, there are two real quadratic subfields k_1 and k_2 of $M(\zeta)$ which are not contained in M. Then, as is observed in [4, Remarks 2.4 (2)], we have

PROPOSITION 3.1. *For $\gamma_1 \in k_1 \setminus k_1^p$ and $\gamma_2 \in k_2 \setminus k_2^p$, we have $K_{\gamma_1} \neq K_{\gamma_2}$.*

By this Proposition, if k_1 and k_2 have units ε_1 and ε_2, respectively, both of which satisfy the condition (1.1), then there exist two unramified cyclic extensions K_{ε_1} and K_{ε_2} of M of degree p; hence the p-rank of M is greater than one.

Now we give a criterion for a real quadratic field to have a unit satisfying (1.1).

PROPOSITION 3.2. *Let d be a square-free positive integer and put $k = \mathbf{Q}(\sqrt{d})$. Let ε_0 be the fundamental unit of k.*

(1) *When $p \mid d$, there exists a unit of k which satisfies the condition* (1.1) *if and only if ε_0 satisfies the condition* (1.2).

(2) *When $p \nmid d$, there exists a unit of k which satisfies the condition* (1.1) *if and only if ε_0^m satisfies the condition* (1.2) *for some integer m with $m \mid \varphi_k(p)$ and $p \nmid m$, where φ_k is the Euler function in k.*

To prove this proposition, we need the following lemma.

LEMMA 3.3. *Let ε be a fixed unit of $\mathbf{Q}(\sqrt{d})$. For a positive integer m, we put*

$$\varepsilon^m = a_m + b_m\sqrt{d}\,, \quad a_m,\ b_m \in \frac{1}{2}\mathbf{Z}\,.$$

For an integer i, moreover, we defined an integer n_i by

$$n_i := \min\{\, m(>0) \in \mathbf{Z} \mid b_m \equiv 0 \pmod{p^i}\,\}\,.$$

Then we have

$$b_n \equiv 0 \pmod{p^i} \Leftrightarrow n \equiv 0 \pmod{n_i}\,.$$

PROOF. The "$\Leftarrow$" part is easily verified.

Let us prove the "$\Rightarrow$" part. Assume that $b_n \equiv 0 \pmod{p^i}$ and put $n = n_i s + t$ ($s, t \in \mathbf{Z}$, $0 \leq t < n_i$). By the definition of n_i, we have

$$\varepsilon^{n_i} \equiv a_{n_i} \pmod{p^i}\,.$$

Then we have

$$\varepsilon^n = (\varepsilon^{n_i})^s \varepsilon^t \equiv a_{n_i}^s (a_t + b_t\sqrt{d}) \pmod{p^i}\,,$$

and hence

$$b_t \equiv 0 \pmod{p^i}\,.$$

By the minimality of n_i, therefore, we have $t = 0$. □

PROOF OF PROPOSITION 3.2. For a positive integer m, we put

$$\varepsilon_0^m = a_m + b_m\sqrt{d}\,, \quad a_m,\ b_m \in \frac{1}{2}\mathbf{Z}\,.$$

For an integer i, we defined an integer n_i by

$$n_i := \min\{\, m(>0) \in \mathbf{Z} \mid b_m \equiv 0 \pmod{p^i}\,\}\,.$$

(1) Assume that $p \mid d$. We note that

$$\varepsilon_0^m \text{ satisfies (1.1)} \Rightarrow \varepsilon_0^m \text{ satisfies (1.2)} \Leftrightarrow b_m \equiv 0 \pmod{p}\,. \tag{3.1}$$

We see that $b_p \equiv 0 \pmod{p}$. Then by applying Lemma 3.3 to $i = 1$, we have $p \equiv 0 \pmod{n_1}$, hence $n_1 = 1$ or p. Assume now that there exists a unit ε_0^m $(p \nmid m)$ satisfying (1.1). Then by (3.1), we have $b_m \equiv 0 \pmod{p}$. By Lemma 3.3, therefore, we have $m \equiv 0 \pmod{n_1}$. From this, together with $p \nmid m$, we have $p \nmid n_1$. Therefore, n_1 must be equal to 1. Then we have $b_1 \equiv 0 \pmod{p}$, and hence by (3.1) ε_0 satisfies the condition (1.2).

Conversely, if ε_0 satisfies (1.2), as we have stated in Remark 1.2 (1), ε_0^2 satisfies (1.1).

(2) Assume that $p \nmid d$. Then we have

$$\varepsilon_0^m \text{ satisfies (1.1)} \Rightarrow \varepsilon_0^m \text{ satisfies (1.2)} \Leftrightarrow b_m \equiv 0 \pmod{p^2}\,. \tag{3.2}$$

We see that $b_{pn_1} \equiv 0 \pmod{p^2}$. Then by applying Lemma 3.3 to $i = 2$, we have

$$pn_1 \equiv 0 \pmod{n_2}\,. \tag{3.3}$$

Now assume that there exists a unit satisfying (1.1). By a similar argument as in (1), we get $p \nmid n_2$. From this, together with (3.3) and the fact that $n_1 \le n_2$, we have $n_2 = n_1$. Furthermore, we have $n_1 \mid \varphi_k(p)$ because of $\varepsilon^{\varphi_k(p)} \equiv 1 \pmod{p}$. Therefore, we see that n_2 satisfies $n_2 \mid \varphi_k(p)$, $p \nmid n_2$, and $\varepsilon_0^{n_2}$ satisfies (1.2) by (3.2).

Conversely, if ε_0^m satisfies (1.2) for some $m \in \mathbf{Z}$, then ε_0^{2m} satisfies (1.2). □

In the following Tables 1 and 2, for $p = 5,\ 13$, we list all of d's with

$$0 < d \le 2000\,, \quad 5 \nmid d\,, \quad d : \text{square-free} \quad \text{if} \quad p = 5\,,$$
$$0 < d \le 4000\,, \quad 13 \nmid d\,, \quad d : \text{square-free} \quad \text{if} \quad p = 13$$

for which both $k_1 = \mathbf{Q}(\sqrt{d})$ and $k_2 = \mathbf{Q}(\sqrt{pd})$ have units satisfying (1.1). Moreover, for each d, we list the minimal exponent m of the unit ε_0^m which satisfies the condition (1.2) and the structure of the ideal class group of M, where ε_0 is the fundamental unit of k_1. The cases where $N_{k_1}(\varepsilon_0) = -1$ are marked with an asterisk in these tables; then ε_0^{2m} satisfies (1.1) in these cases. We denote an abelian group $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$ by $[n_1,\ n_2, \cdots,\ n_r]$.

TABLE 1 $p = 5$ ($0 < d \leq 2000$)

d	exponent	structure of the ideal	d	exponent	structure of the ideal
	of ε (m)	class group of M		of ε (m)	class group of M
127	1	[10, 10]	1231	2	[50, 10, 2]
191	2	[10, 10, 2]	1238	1	[50, 10, 2]
*257	3	[10, 5]	1366	2	[30, 30]
*298	1	[20, 10, 2]	1389	2	[50, 10]
426	1	[10, 10, 2, 2]	1434	1	[20, 20, 2, 2]
427	3	[10, 10, 2, 2]	*1493	3	[50, 5]
*457	3	[10, 5]	1518	3	[20, 10, 2, 2, 2]
501	2	[10, 10]	1531	2	[50, 10, 2]
502	3	[20, 10, 2]	*1597	1	[50, 5]
509	2	[10, 10]	1631	1	[30, 30, 2]
574	2	[10, 10, 2, 2]	1738	3	[20, 10, 2, 2, 2]
581	2	[10, 10]	1758	3	[130, 10, 2]
587	3	[50, 10]	1829	1	[10, 10, 2, 2]
626	2	[50, 10]	1834	2	[20, 20, 2, 2]
629	2	[10, 10]	*1853	3	[20, 10, 2]
734	2	[50, 10]	1907	3	[170, 10]
753	3	[10, 10, 2]	*1913	3	[50, 5]
*881	1	[20, 10]	1914	2	[10, 10, 2, 2, 2, 2]
*922	1	[50, 10, 2]	1938	3	[20, 10, 2, 2, 2]
1113	3	[10, 10, 2]	1999	2	[40, 20, 2]
1137	3	[10, 10, 2]			

REMARK 3.4. We use computer manipulations with GP/PARI (Version 2.1.0) and KASH (Version 2.0). In the case $p = 13$, the author cannot compute the structure of the ideal class group of M except for $d = 489$ because of the computational complexity.

Finally, we give an example of a family of positive integers d for which both $k_1 = \mathbf{Q}(\sqrt{d})$ and $k_2 = \mathbf{Q}(\sqrt{pd})$ have units satisfying the condition (1.1).

EXAMPLE 3.5. For a pair $(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z}$ with

$$\begin{cases} \alpha^2 - p^3\beta^2 = 4\,, \\ \alpha + \beta \equiv 0 \pmod{p^2}\,, \end{cases}$$

we define an integer d by

$$d := (\alpha + \beta)^2 - 4\,.$$

Moreover, we put

$$\varepsilon_1 := \frac{\alpha + \beta + \sqrt{d}}{2} \in \mathbf{Q}(\sqrt{d})\,,$$

TABLE 2 $p = 13$ $(0 < d \leq 4000)$

d	exponent of ε (m)	structure of the ideal class group of M	d	exponent of ε (m)	structure of the ideal class group of M
489	7	[117650, 26, 2]	*3074	7	———
1381	6	———	3739	7	———
1615	6	———	3766	1	———
1639	3	———	3847	6	———
2003	6	———	3910	6	———
2038	6	———			

$$\varepsilon_2 := \frac{\alpha + p^3\beta + p\sqrt{pd}}{2} \in \mathbf{Q}(\sqrt{pd})\,.$$

Then we can easily verify that

$$N_{\mathbf{Q}(\sqrt{d})}(\varepsilon_1^2) = 1 = N_{\mathbf{Q}(\sqrt{pd})}(\varepsilon_2)\,,$$

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{d})}(\varepsilon_1^2) \equiv \pm 2 \equiv \mathrm{Tr}_{\mathbf{Q}(\sqrt{pd})}(\varepsilon_2) \pmod{p^3}\,.$$

Hence the p-rank of $\mathbf{Q}(\sqrt{d}(\zeta - \zeta^{-1}))$ is greater than one, if

$$\varepsilon_1^2 \notin \mathbf{Q}(\sqrt{d})^p \quad \text{and} \quad \varepsilon_2 \notin \mathbf{Q}(\sqrt{pd})^p\,. \tag{3.4}$$

REMARK 3.6. If d is square-free, then the condition (3.4) holds. However, the author has not yet verified when d is square-free, nor whether the condition (3.4) holds more generally.

ACKNOWLEDGEMENT. The author would like to thank the referee for his careful reading and various comments.

References

[1] T. AZUHATA and H. ICHIMURA, On the divisibility problem of the class numbers of algebraic number fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **30** (1984), 579–585.

[2] H. COHEN, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193** (2000) Springer.

[3] G. DEGERT, Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97.

[4] M. IMAOKA and Y. KISHI, On dihedral extensions and Frobenius extensions, *Galois theory and Modular forms*, Developments in Mathematics **11** (2003), Kluwer Acad. Publ. 195–220.

[5] M. ISHIDA, A note on class numbers of algebraic number fields, J. Number Theory **1** (1969), 65–69.

[6] Y. KISHI, Imaginary cyclic fields of degree $p - 1$ whose relative class numbers are divisible by p, Proc. Japan Acad. **77A** (2001), 55–58.

[7] S. NAKANO, On ideal class groups of algebraic number fields, J. Reine Angew. Math. **358** (1985), 61–75.

[8] T. J. RIVLIN, *Chebyshev polynomials. From approximation theory to algebra and number theory. Second edition*, Pure and Applied Mathematics (1990), John Wiley.

[9] M. SASE, On a family of quadratic fields whose class numbers are divisible by five, Proc. Japan Acad. **74A** (1998), 120–123.

[10] Y. YAMAMOTO, On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76.

[11] H. YOKOI, On real quadratic fields containing units with norm -1, Nagoya Math. J. **33** (1968), 139–152.

Address:
DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY,
MINAMI-OHSAWA, HACHIOJI-SHI, TOKYO, 192–0397 JAPAN.
e-mail: ykishi@comp.metro-u.ac.jp

Present Address:
DEPARTMENT OF MATHEMATICS, FUKUOKA UNIVRSITY OF EDUCATION,
BUNKYOUMACHI AKAMA, MUNAKATA-SHI, FUKUOKA, 811–4192 JAPAN.
e-mail: ykishi@fukuoka-edu.ac.jp