PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 101, Number 3, November 1987

ON THE QUADRATIC SUBFIELD OF A Z_2-EXTENSION OF AN IMAGINARY QUADRATIC NUMBER FIELD

AKIRA ENDÔ

(Communicated by William C. Waterhouse)

ABSTRACT. We determine explicitly the quadratic subfield of a noncyclotomic Z_2-extension of an imaginary quadratic number field and get a congruence property of the integer solution of a certain indeterminate equation.

1. Introduction. Let F be an imaginary quadratic number field and Z_2 the additive group of 2-adic rational integers. An infinite normal extension of F with Galois group isomorphic to Z_2 is called a Z_2-extension of F. It is known that F has two independent Z_2-extensions [**8**]. One is $F \subset F(\sqrt{2}) \subset F(\sqrt{2+\sqrt{2}}) \subset \cdots$, which is called a cyclotomic Z_2-extension. Carrol and Kisilevsky [**3, 4**] have shown that the quadratic subfield of a noncyclotomic Z_2-extension of F is related closely to the 2-primary subgroup $C_F(2)$ of the ideal class group of F. On the other hand, the structure of $C_F(2)$ has already been investigated in detail by Hasse [**5–7**], Bauer [**1, 2**] and others.

Let Q be the field of rational numbers. In this note we shall treat the case where $F = Q(\sqrt{-p})$, p an odd prime number, for which $C_F(2)$ is cyclic. We shall determine explicitly the quadratic subfield of a noncyclotomic Z_2-extension of F (Theorems 1 and 3), and show that this problem is also related to a congruence property modulo 8 of the integer solution of a certain indeterminate equation (Theorem 2).

2. Preliminaries. Let $F = Q(\sqrt{-p})$ be as in the Introduction. As is well known, $C_F(2) \neq 1$ if and only if $p \equiv 1 \pmod 4$, and $|C_F(2)| \geq 2^2$ if and only if $p \equiv 1 \pmod 8$ [**5**]. The following was shown or can be easily proved by [**3, 4**]:

PROPOSITION. *If $p \equiv 5 \pmod 8$, then $F(\sqrt{-1}) \subset F(\sqrt{2E}) \subset F(\sqrt[4]{2E})$ are subfields of a Z_2-extension of F, where E is the fundamental unit of $Q(\sqrt{p})$; if $p \equiv 3$ (mod) and $p = a^2 + 2b^2$, then $F(\sqrt{-2}) \subset F(\sqrt{2b - a\sqrt{-2}})$ are subfields of a Z_2-extension of F; and if $p \equiv 7 \pmod 8$ and $p = -a^2 + 2b^2$, then $F(\sqrt{a - \sqrt{-p}})$ is a subfield of a Z_2-extension of F.*

In what follows, we assume that $p \equiv 1 \pmod 8$ and $p = -a^2 + 2b^2$ with $a \equiv 1 \pmod 4$ and $b > 0$. (Since $\left(\frac{2}{p}\right) = 1$ and $Q(\sqrt{2})$ has a unit with negative norm, such a, b exist.) Then, (2) is ramified in F: $(2) = \mathfrak{z}^2$. There exists an ideal $\mathfrak{b}_1$ of F such that $\mathfrak{z}\mathfrak{b}_1^2 = (a - \sqrt{-p})$ ad $N\mathfrak{b}_1 = b$, where N means the norm [**5**]. The class of $\mathfrak{b}_1$ is in C_F^2, where C_F is the ideal class group of F, if and only if $b \equiv 1 \pmod 4$.

Received by the editors August 5, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12A25.
Key words and phrases. Imaginary quadratic number field, Z_2-extension.

Now, let L be the maximal abelian 2-ramified (i.e., unramified at all primes different from $\mathfrak{z}$) 2-extension of F with Galois group G. Then L contains the composite K of all Z_2-extensions of F and $G \cong Z_2 \times Z_2 \times T$, where T is the torsion subgroup of G corresponding to K. Let A denote the subgroup of all elements α of $F^* = F - \{0\}$ which are divisible by each prime different from $\mathfrak{z}$ to an even power. Then, in our case, A is generated by $-1, 2, a - \sqrt{-p}$, and F^{*2} [**3**]. For any $\alpha \in A$, $F(\sqrt{\alpha})$ is 2-ramified, i.e., $F(\sqrt{\alpha}) \subset L$, and further $F(\sqrt{\alpha})$ is contained in K if and only if it is fixed by T.

Let U and J be the unit group and the idele group of F, respectively. For a prime $\mathfrak{p}$ of F, let $U_{\mathfrak{p}}$ denote the unit group of the completion $F_{\mathfrak{p}}$ of F of $\mathfrak{p}$. Put $J^{(2)} = \{1\}_{\mathfrak{z}} \times \prod_{\mathfrak{p} \neq \mathfrak{z}} U_{\mathfrak{p}}$, a subgroup of J. For an abelian group X, let $X(2)$ denote the 2-primary torsion subgroup of X. By class field theory, T is identified with $(J/J^{(2)}F^*)(2)$. Then the canonical mapping $J/F^* \to C_F$ induces an exact sequence

$$1 \to H \to T \xrightarrow{\phi} C_F(2),$$

where $H = (U_{\mathfrak{z}}/U)(2)$. T/T^2 is considered as a subgroup of G/G^2 and G/G^2 is identified with $J/J^{(2)}F^*J^2$. $F(\sqrt{\alpha})$, $\alpha \in A$, is contained in K if and only if

$$(\alpha, (x_{\mathfrak{p}})) = \prod_{\mathfrak{p}} (\alpha, x_{\mathfrak{p}})_{\mathfrak{p}} = 1$$

for all $(x_{\mathfrak{p}}) \in T = (J/J^{(2)}F^*)(2)$, where $(\ \ ,\ \ )_{\mathfrak{p}}$ is the Hilbert 2-symbol in $F_{\mathfrak{p}}$. Carroll [**3**] calculated $(\alpha, (x_{\mathfrak{p}}))$ for $\alpha \in A$, $(x_{\mathfrak{p}}) \in T$ in the case where $|T^2| \leq 2$.

Now, denote by

$$(\ldots, \underset{\mathfrak{p}_i}{x_{\mathfrak{p}_i}}, \ldots)$$

an idele of F having $x_{\mathfrak{p}_i}$ at $\mathfrak{p}_i$-components and 1 elsewhere. In our case T is cyclic and H is its subgroup of order 2 [**3**]. We here note that $F_{\mathfrak{z}} = Q_2(\sqrt{-1})$, Q_2 being the field of 2-adic rational integers. It is seen that H is generated by

$$(\underset{\mathfrak{z}}{\sqrt{-1}}, \ldots).$$

Let

$$z_0 = (\underset{\mathfrak{z}}{1 - \sqrt{-1}}, \ldots) \in J.$$

Then

$$z_0^2 \equiv (\underset{\mathfrak{z}}{\sqrt{-1}}, \ldots) \pmod{J^{(2)}F^*}.$$

3. Theorems. As stated above, A/F^{*2} is generated by $-1, 2$, and $a - \sqrt{-p}$. $F(\sqrt{2})$ is contained in the cyclotomic Z_2-extension of F. We assume that $\sqrt{-p} \equiv \sqrt{-1} \pmod{\mathfrak{z}^4}$ and so $\sqrt{p} \equiv 1 \pmod 4$ in Q_2. We now calculate $(-1, z_0)$ and $(a - \sqrt{-p}, z_0)$. For a rational prime q, $(\ \ ,\ \ )_q$ denotes the Hilbert 2-symbol at the field of q-adic rational numbers.

$$(-1, z_0) = (-1, 1 - \sqrt{-1})_{\mathfrak{z}} = (\sqrt{-1}, 1 - \sqrt{-1})_{\mathfrak{z}}^2 = 1,$$

$$\begin{aligned}(a - \sqrt{-p}, z_0) &= (a - \sqrt{-p}, 1 - \sqrt{-1})_{\mathfrak{z}} = (\sqrt{p}(1 - \sqrt{-1}), 1 - \sqrt{-1})_{\mathfrak{z}} \\ &= (\sqrt{p}, 1 - \sqrt{-1})_{\mathfrak{z}} = (\sqrt{p}, 2)_2 = (-1)^{(p-1)/8}.\end{aligned}$$

Thus, if $p \equiv 9 \pmod{16}$, then $F(\sqrt{-1}) \subset K$, $T = \langle z_0 \rangle$ and $\phi(T) \neq C_F(2)$. If $p \equiv 1 \pmod{16}$, then it remains to determine whether $F(\sqrt{-1}) \subset K$ or $F(\sqrt{\pm a - \sqrt{-p}}) \subset K$.

From now on we assume $p \equiv 1 \pmod{16}$; then $\sqrt{p} \equiv 1 \pmod 8$. Each prime $q_1 | b$ splits in F: $(q_1) = \mathfrak{q}_1\overline{\mathfrak{q}_1}$. We may assume that $\mathfrak{q}_1 | (a - \sqrt{-p})$ and hence $\mathfrak{q}_1 | \mathfrak{b}_1$. Let $\mu_1 = (a - \sqrt{-p})/(1 - \sqrt{-1}) \in F_{\mathfrak{z}} = Q_2(\sqrt{-1})$; then $\mu_1 \equiv 1 \pmod{\mathfrak{z}^5}$ and hence $\sqrt{\mu_1} \equiv 1 \pmod{\mathfrak{z}^3}$ exists in $F_{\mathfrak{z}}$. Define

$$z_1 = (\underset{\mathfrak{z}}{\sqrt{\mu_1}}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1}{b_1}, \ldots) \in J,$$

where $b_1 = b$. $\phi(z_1)$ is the class of $\mathfrak{b}_1$ and

$$\begin{aligned} z_1^2 &= (\underset{\mathfrak{z}}{\mu_1}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1}{b_1^2}, \ldots) \\ &\equiv \frac{1}{a - \sqrt{-p}} (\underset{\mathfrak{z}}{\mu_1}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1}{b_1^2}, \ldots) \equiv z_0^{-1} \pmod{J^{(2)} F^*}. \end{aligned}$$

It is easy to see that

$$\begin{aligned} \sqrt{\mu_1} &\equiv 1 + \frac{a - \sqrt{p}}{4}(1 - \sqrt{-1}) + \frac{\sqrt{p} - 1}{2} \pmod{\mathfrak{z}^5} \\ &\equiv \begin{cases} 1, -1 - 2\sqrt{-1} \pmod{\mathfrak{z}^5}, & a \equiv 1 \pmod{16}, \\ 5, -1 + 2\sqrt{-1} \pmod{\mathfrak{z}^5}, & a \equiv 9 \pmod{16}. \end{cases} \end{aligned}$$

Then,

$$\begin{aligned} (-1, z_1) &= (-1, \sqrt{\mu_1})_{\mathfrak{z}} \prod_{\mathfrak{q}_1|\mathfrak{b}_1} (-1, b)_{\mathfrak{q}_1} \\ &= \prod_{q_1|b} (-1, b)_{q_1} = (-1, b)_2 = (-1)^{(b-1)/2}, \\ (a - \sqrt{-p}, z_1) &= (a - \sqrt{-p}, \sqrt{\mu_1})_{\mathfrak{z}} \prod_{\mathfrak{q}_1|\mathfrak{b}_1} (a - \sqrt{-p}, b)_{\mathfrak{q}_1} \\ &= (1 - \sqrt{-1}, \sqrt{\mu_1})_{\mathfrak{z}} \prod_{\mathfrak{q}_1|\mathfrak{b}_1} (2(a + \sqrt{-p}), b)_{\mathfrak{q}_1} \\ &= (-1)^{(a-1)/8} \prod_{\mathfrak{q}_1|\mathfrak{b}_1} (4a, b)_{\mathfrak{q}_1} \\ &= (-1)^{(a-1)/8} \prod_{q_1|b} (a, b)_{q_1} = (-1)^{(a-1)/8} \left(\frac{a}{b}\right). \end{aligned}$$

Herein we have used that $(1 - \sqrt{-1}, 5)_{\mathfrak{z}} = (2, 5)_2 = -1$, $(1 - \sqrt{-1}, -1 - 2\sqrt{-1})_{\mathfrak{z}} = (1 - \sqrt{-1}, 1 - (1 + \sqrt{-1})^2(1 - \sqrt{-1}))_{\mathfrak{z}} = 1$ and $(1 - \sqrt{-1}, -1 + 2\sqrt{-1})_{\mathfrak{z}} = (1 - \sqrt{-1}, 5(-1 - 2\sqrt{-1}))_{\mathfrak{z}} = -1$. Hence we have the following theorem.

THEOREM 1. *Suppose that $p \equiv 1 \pmod{16}$ and $p = -a^2 + 2b^2$ with $a \equiv 1 \pmod 8$ and $b > 0$. If $b \equiv 1 \pmod 4$ and $\left(\frac{a}{b}\right) = -(-1)^{(a-1)/8}$, then $F(\sqrt{-1})$ is a subfield of a Z_2-extension of F and $\phi(T) \neq C_F(2)$; and if $b \equiv -1 \pmod 4$, then $F(\sqrt{a - \sqrt{-p}})$ or $F(\sqrt{-a - \sqrt{-p}})$ is a subfield of a Z_2-extension of F according as $\left(\frac{a}{b}\right) = (-1)^{(a-1)/8}$ or $(-1)^{(a-1)/8}$, and $\phi(T) = C_F(2)$. In these cases, $T = \langle z_1 \rangle$.*

Let b' be the square-free part of b and put $b = b'g^2$ with $g > 0$. If $b \equiv b' \equiv 1 \pmod 4$, then there exist rational integers r, s, t which satisfy

$$r^2 + ps^2 - b't^2 = 0, \qquad (r, s, t) = 1,\ t > 0.$$

Let $c = \prod_l' l^{v_l(b')}$ and $d = \prod_l'' l^{v_l(g,t)}$, where the $'$ (resp. $''$) indicates that l runs through rational primes dividing $(a-\sqrt{-1})(r-s\sqrt{-p})$ (resp. $(a-\sqrt{-p})(r+s\sqrt{-p})$) and $l^{v_l(x)}$ means the exact power of l dividing x. Bauer [**1**] showed that there exists a primitive ideal $\mathfrak{b}_2$ of F such that

$$\mathfrak{b}_1\overline{\mathfrak{b}_2}^2 = ((cg^2/d^2)(r - s\sqrt{-p})), \qquad N\mathfrak{b}_2 = cgt/d^2.$$

Put $b_2 = cgt/d^2$. The class of $\mathfrak{b}_2$ is in C_F^2 if and only if $b_2 \equiv 1 \pmod 4$. We here note that $c = (r + as, b')$ and $d = (r - as, g, t)$.

Each prime $q_2|t$ splits in F: $(q_2) = \mathfrak{q}_2\overline{\mathfrak{q}_2}$. We assume that $\mathfrak{q}_2|r+s\sqrt{-p}$ and hence $\mathfrak{q}_2|\overline{\mathfrak{b}_1}\mathfrak{b}_2$. Note that for a prime $q_1|b$, if $q_1|b_2$ and $q_1 \nmid t$, then $\mathfrak{q}_1|\mathfrak{b}_2$. It is easy to see that r and s are of mixed parity (i.e., one odd and one even) and that $4|rs$ if and only if $p \equiv 2a - 1 \pmod{32}$.

THEOREM 2. *Suppose that* $p = -a^2 + 2b^2 \equiv 1 \pmod{16}$, $a \equiv 1 \pmod 8$, $b > 0$ *and* $b \equiv 1 \pmod 4$, *and let* b' *be the square-free part of* b. *If rational integers* r, s, t *satisfy* $r^2 + ps^2 = b't^2$, $(r, s, t) = 1$, $t > 0$, *then*

$$r + s \equiv \begin{cases} \pm c + 4\varsigma \pmod 8, & \left(\frac{a}{b}\right) = (-1)^{(a-1)/8}, \\ \pm 5c + 4\varsigma \pmod 8, & \left(\frac{a}{b}\right) = (-1)^{(a-1)/8+1}, \end{cases}$$

where $c = (r + as, b')$ *and* $\varsigma = 0$ *or* 1 *such that*

$$\varsigma \equiv \begin{cases} \frac{1}{16}(p-1) \pmod 2, & s \equiv 0 \pmod 4 \text{ or } r \equiv 0 \pmod 2, \\ \frac{1}{16}(p-1) + 1 \pmod 2, & s \equiv 2 \pmod 4. \end{cases}$$

PROOF. As shown above, if $b \equiv 1 \pmod 4$, then $z_1 \in T^2$ or not, in other words, z_1 is the square of some $z_2 \in J$ modulo $J^{(2)}F^*$ or not, according as $\left(\frac{a}{b}\right) = (-1)^{(a-1)/8}$ or $(-1)^{(a-1)/8+1}$. We may assume that $\phi(z_2)$ is the class of $\mathfrak{b}_2$. Therefore such z_2 is of the form

$$z_2 = (\underset{\mathfrak{z}}{\sqrt{\mu_2}}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1, \mathfrak{b}_2}{b_2}, \ldots, \underset{\substack{\mathfrak{q}_2 \nmid \mathfrak{b}_1 \\ \mathfrak{q}_2|\mathfrak{b}_2}}{b_2}, \ldots).$$

Since

$$(\underset{\mathfrak{z}}{2}, \ldots) \equiv 1 \pmod{J^{(2)}F^*},$$

we may assume that μ_2 is prime to $\mathfrak{z}$. There exists $M \in F$ such that

$$M(\underset{\mathfrak{z}}{\mu_2}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1, \mathfrak{b}_2}{b_2^2}, \ldots, \underset{\substack{\mathfrak{q}_2 \nmid \mathfrak{b}_1 \\ \mathfrak{q}_2|\mathfrak{b}_2}}{b_2^2}, \ldots) \equiv (\underset{\mathfrak{z}}{\sqrt{\mu_1}}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1}{b_1}, \ldots) \pmod{J^{(2)}}.$$

Then $M\mu_2 = \sqrt{\mu_1}$ and $(M)\mathfrak{b}_2^2 = \mathfrak{b}_1$, because $N\mathfrak{b}_1 = b_1$ and $N\mathfrak{b}_1 = b_2$. Since $\mathfrak{b}_1^{-1}\mathfrak{b}_2^2 = ((b_2/b'gt)(r + s\sqrt{-p}))$, $1/M = \mu_2/\sqrt{\mu_1} = \pm(b_2/b'gt)(r + s\sqrt{-p})$. Thus we have that, since

$$z_0^2 \equiv (\underset{\mathfrak{z}}{\sqrt{-1}}, \ldots)\ (\in H) \pmod{J^{(2)}F^*},$$

$\sqrt{-1}^j\mu_2 = \pm\sqrt{-1}^j(b_2/b'gt)(r+s\sqrt{-p})\sqrt{\mu_1}$, $j=0$ or 1, is a square in $Q_2(\sqrt{-1})$, i.e., $\equiv \pm 1 \pmod{\mathfrak{z}^5}$, if and only if $\left(\frac{a}{b}\right) = (-1)^{(a-1)/8}$. Since

$$\mu_2 \equiv \pm\frac{b_2}{b'gt}(r+s\sqrt{-1})\sqrt{\mu_1} \equiv \pm\frac{c}{b}(r+s\sqrt{-1})\sqrt{\mu_1} \pmod{\mathfrak{z}^5}$$
$$\equiv \begin{cases} \pm\, c(r+s\sqrt{-1}) \pmod{\mathfrak{z}^5}, & p\equiv 2a-1\equiv 1 \pmod{32},\\ \pm\, 5c(r+s\sqrt{-1}) \pmod{\mathfrak{z}^5}, & p\equiv 2a-1\equiv 17 \pmod{32},\\ \pm\, 5(-1+2\sqrt{-1})c(r+s\sqrt{-1}) \pmod{\mathfrak{z}^5}, & p\equiv 2a-17\equiv 1 \pmod{32},\\ \pm\, 5(-1-2\sqrt{-1})c(r+s\sqrt{-1}) \pmod{\mathfrak{z}^5}, & p\equiv 2a-17\equiv 17 \pmod{32},\end{cases}$$

the assertion of the theorem follows easily.

We next consider the case where $b\equiv 1 \pmod 4$ and $\left(\frac{a}{b}\right) = (-1)^{(a-1)/8}$. We may assume $r+s\equiv c \pmod 4$. Then, from the proof above

$$\frac{b_2}{b'gt}(r+s\sqrt{-p})\sqrt{\mu_1} \equiv \begin{cases} 1 \pmod{\mathfrak{z}^5}, & s\equiv 0 \pmod 2,\\ \sqrt{-1} \pmod{\mathfrak{z}^5}, & r\equiv 0 \pmod 2.\end{cases}$$

We normalize μ_2 as follows:

$$\mu_2 = \begin{cases} \dfrac{b_2}{b'gt}(r+s\sqrt{-p})\sqrt{\mu_1}, & s\equiv 0 \pmod 2,\\[2ex] \dfrac{b_2}{b'gt}(r+s\sqrt{-p})\dfrac{\sqrt{\mu_1}}{\sqrt{-1}}, & r\equiv 0 \pmod 2.\end{cases}$$

Then $\mu_2\equiv 1 \pmod{\mathfrak{z}^5}$ and hence $\sqrt{\mu_2}\equiv 1 \pmod{\mathfrak{z}^3}$ exists in $Q_2(\sqrt{-1})$. Put

$$z_2 = (\underset{\mathfrak{z}}{\sqrt{\mu_2}}, \ldots, \underset{\mathfrak{q}_1|\mathfrak{b}_1,\mathfrak{b}_2}{b_2}, \ldots, \underset{\substack{\mathfrak{q}_2\nmid \mathfrak{b}_1\\ \mathfrak{q}_2|\mathfrak{b}_2}}{b_2}, \ldots) \in J;$$

then $z_2^2\equiv z_1 \pmod{J^{(2)}F^*}$ if $2|s$ and $(z_2z_0^{-1})^2\equiv z_1 \pmod{J^{(2)}F^*}$ if $2|r$. It is easy to see that

$$\sqrt{\mu_2}\equiv 1+2\gamma(1-\sqrt{-1})+4\delta \pmod{\mathfrak{z}^5}$$

with

$$\gamma = \begin{cases} \dfrac{1}{16}(a-\sqrt{p}+4rs), & s\equiv 0 \pmod 2,\\[2ex] \dfrac{1}{16}(a-\sqrt{p}-4rs), & r\equiv 0 \pmod 2,\end{cases}$$
$$\delta = \begin{cases} \dfrac{1}{16}\left(s^2+2rs-\left(\dfrac{b_2}{b'gt}\right)^2 r^2\sqrt{p}+1\right), & s\equiv 0 \pmod 2,\\[2ex] \dfrac{1}{16}\left(r^2-2rs-\left(\dfrac{b_2}{b'gt}\right)^2 ps^2\sqrt{p}+1\right), & r\equiv 0 \pmod 2.\end{cases}$$

Put $\rho = 16(\gamma-\delta)$; then

$$\rho \equiv \begin{cases} -s^2+2rs+\left(\dfrac{b_2}{b'gt}\right)^2 ar^2-1 \pmod{32}, & s\equiv 0 \pmod 2,\\[2ex] -r^2-2rs+\left(\dfrac{b_2}{b'gt}\right)^2 aps^2-1 \pmod{32}, & r\equiv 0 \pmod 2.\end{cases}$$

Hence

$$\begin{aligned}(-1, z_2) &= (-1, \sqrt{\mu_2})_{\mathfrak{z}} \prod_{\mathfrak{q}_1 | \mathfrak{b}_1, \mathfrak{b}_2} (-1, b_2)_{\mathfrak{q}_1} \prod_{\substack{\mathfrak{q}_2 \nmid \mathfrak{b}_1 \\ \mathfrak{q}_2 | \mathfrak{b}_2}} (-1, b_2)_{\mathfrak{q}_2} \\ &= \prod_{q_1 | b_1, b_2} (-1, b_2)_{q_1} \prod_{\substack{q_2 \nmid b_1 \\ q_2 | b_2}} (-1, b_2)_{q_2} \\ &= (-1, b_2)_2 = (-1)^{(b_2-1)/2},\end{aligned}$$

$$\begin{aligned}(a - \sqrt{-p}, z_2) &= (a\sqrt{-p}, \sqrt{\mu_2})_{\mathfrak{z}} \prod_{\mathfrak{q}_1 | \mathfrak{b}_1, \mathfrak{b}_2} (a - \sqrt{-p}, b_2)_{\mathfrak{q}_1} \prod_{\substack{\mathfrak{q}_2 \nmid \mathfrak{b}_1 \\ \mathfrak{q}_2 | \mathfrak{b}_2}} (a - \sqrt{-p}, b_2)_{\mathfrak{q}_2} \\ &= (1 - \sqrt{-1}, \sqrt{\mu_2})_{\mathfrak{z}} \prod_{\mathfrak{q}_1 | \mathfrak{b}_1, \mathfrak{b}_2} (2(a + \sqrt{-p}), b_2)_{\mathfrak{q}_1} \prod_{\substack{\mathfrak{q}_2 \nmid \mathfrak{b}_1 \\ \mathfrak{q}_2 | \mathfrak{b}_2}} ((r + as)s, b_2)_{\mathfrak{q}_2} \\ &= (-1)^{\rho/16} \prod_{q_1 | b_1, b_2} (a, b_2)_{q_1} \prod_{\substack{q_2 \nmid b_1 \\ q_2 | b_2}} ((r + as)s, b_2)_{q_2} = (-1)^{\rho/16}\chi\end{aligned}$$

with

$$\chi = \prod_{q_1 | b_1} \left(\frac{a}{q_1}\right)^{v_{q_1}(b_2)} \prod_{\substack{q_2 \nmid b_1 \\ q_2 | b_2}} \left(\frac{(r + as)s}{q_2}\right)^{v_{q_2}(b_2)}.$$

Therefore the following theorem holds:

THEOREM 3. *Suppose that* $p = -a^2 + 2b^2 \equiv 1 \pmod{16}$, $a \equiv 1 \pmod 8$, $b > 0$, $b \equiv 1 \pmod 4$ *and* $\left(\frac{a}{b}\right) = (-1)^{(a-1)/8}$, *and let* $b = b'g^2$ *with square-free* b' *and* $g > 0$. *Take rational integers* r, s, t *such that* $r^2 + ps^2 = b't^2$, $(r, s, t) = 1$, $r+s \equiv (r+as, b') \pmod 4$, $t > 0$, *and define* b_2, ρ, χ *as above. If* $b_2 \equiv 1 \pmod 4$ *and* $\chi = (-1)^{\rho/16+1}$, *then* $F(\sqrt{-1})$ *is a subfield of a* Z_2*-extension of* F *and* $\phi(T) \neq C_F(2)$; *and if* $b_2 \equiv -1 \pmod 4$, *then* $F(\sqrt{a - \sqrt{-p}})$ *or* $F(\sqrt{-a - \sqrt{-p}})$ *is a subfield of a* Z_2*-extension of* F *according as* $\chi = (-1)^{\rho/16}$ *or* $(-1)^{\rho/16+1}$, *and* $\phi(T) = C_F(2)$. *In these cases,* $T = \langle z_2 \rangle$.

In the case where $b_2 \equiv 1 \pmod 4$ and $\chi = (-1)^{\rho/16}$, T has a proper subgroup $\langle z_2 \rangle$ and we can also determine the quadratic subfield of a noncyclotomic Z_2-extension of F after a finite number of procedures similar to the above, since $C_F(2)$ is a finite group.

REFERENCES

1. H. Bauer, *Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. Reine Angew. Math. **248** (1971), 42–46.
2. ——, *Die 2-Klassenzahlen specieller quadratischer Zahlkörper*, J. Reine Angew. Math. **252** (1972), 79–81.
3. J. E. Carroll, *On determining the quadratic subfields of* Z_2*-extensions of complex quadratic fields*, Compositio Math. **30** (1975), 259–271.
4. J. E. Carroll and H. Kisilevsky, *Initial layers of* Z_2*-extensions of complex quadratic fields*, Compositio Math. **3** (1976), 157–168.
5. H. Hasse, *Über die Klassenzahl des Körpers* $P(\sqrt{-p})$ *mit einer Primzahl* $p \equiv 1 \mod 2^3$, Aequationes Math. **3** (1969), 165–169.

6. ——, *Über die Teilbarkeit durch* 2^3 *der Klassenzahl imaginär-quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. Reine Angew. Math. **241** (1970), 1–6.
7. ——, *An algorithm for determining the structure of the* 2-*Sylow subgroup of the divisor class group of a quadratic number field*, Sympos. Math. **15** (1975), 341–352.
8. K. Iwasawa, *On* Z_l*-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 247–326.

DEPARTMENT OF MATHEMATICS, KUMAMOTO UNIVERSITY, KUMAMOTO, JAPAN