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 noncyclo-
tomic $Z_2$-extension of an imaginary quadratic number field and get a congru-
ence 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 $F(\sqrt{-1}) \subset F(\sqrt{2E}) \subset F(\sqrt{2E})$ are
subfields of a $Z_2$-extension of $F$, where $E$ is the fundamental unit of $Q(\sqrt{p})$; if
$p \equiv 3 \pmod{4}$ 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) = $3^2$. There exists an ideal $b_1$ of $F$
such that $3b_1^2 = (a - \sqrt{-p})$ ad $Nb_1 = b$, where $N$ means the norm [5]. The class of
$b_1$ is in $C_F^2$, where $C_F$ is the ideal class group of $F$, if and only if $b \equiv 1 \pmod{4}$.
Now, let $L$ be the maximal abelian 2-ramified (i.e., unramified at all primes different from 3) 2-extension of $F$ with Galois group $G$. Then $L$ contains the composite $K$ of all $\mathbb{Z}_2$-extensions of $F$ and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{T}$, where $T$ is the torsion subgroup of $G$ corresponding to $K$. Let $A$ denote the subgroup of all elements $\alpha$ of $F^* = F - \{0\}$ which are divisible by each prime different from 3 to an even power. Then, in our case, $A$ is generated by $-1, 2, \alpha = \sqrt{-p}$, 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 $p$ of $F$, let $U_p$ denote the unit group of the completion $F_p$ of $F$ of $p$. Put $J^{(2)} = \{1\} \times \prod_{p \neq 3} U_p$, 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 $J/F^* \rightarrow C_F$ induces an exact sequence

$$1 \rightarrow H \rightarrow T \rightarrow C_F(2),$$

where $H = (U_j/U)(2)$. $T/T^2$ 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

$$(\alpha, (x_p)) = \prod_p (\alpha, x_p)_p = 1$$

for all $(x_p) \in T = (J/J^{(2)}F^*)(2)$, where $(\ , \ )_p$ is the Hilbert 2-symbol in $F_p$.

Carroll [3] calculated $(\alpha, (x_p))$ for $\alpha \in A, (x_p) \in T$ in the case where $|T^2| \leq 2$.

Now, denote by

$$(\ldots, x_{p_1}, \ldots)$$

an idele of $F$ having $x_{p_1}$ at $p_1$-components and 1 elsewhere. In our case $T$ is cyclic and $H$ is its subgroup of order 2 [3]. We here note that $F_j = Q_2(\sqrt{-1}), Q_2$ being the field of 2-adic rational integers. It is seen that $H$ is generated by

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

Let

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

Then

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

3. Theorems. As stated above, $A/F^{*2}$ is generated by $-1, 2, \alpha = \sqrt{-p}$. $F(\sqrt{2})$ is contained in the cyclotomic $\mathbb{Z}_2$-extension of $F$. We assume that $\sqrt{-p} \equiv \sqrt{-1} \pmod{4}$ and so $\sqrt{-p} \equiv 1 \pmod{4}$ in $Q_2$. We now calculate $(-1, z_0)$ and $(\alpha - \sqrt{-p}, z_0)$. For a rational prime $q$, $(\ , \ )_q$ denotes the Hilbert 2-symbol at the field of $q$-adic rational numbers.

$$(\alpha - \sqrt{-p}, z_0) = (\alpha - \sqrt{-p}, 1 - \sqrt{-1})_3 = (\sqrt{p}(1 - \sqrt{-1}), 1 - \sqrt{-1})_3
= (\sqrt{p}, 1 - \sqrt{-1})_3 = (\sqrt{p}, 2)_2 = (-1)^{(p-1)/8}.$$
Thus, if \( p \equiv 9 \pmod{16} \), then \( F(\sqrt{-1}) \subset K \), \( T = (z_0) \) 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 \( \sqrt{\alpha} \equiv 1 \pmod{8} \). Each prime \( q_1 | b \) splits in \( F \): \( (q_1) = q_1 \overline{q}_1 \). We may assume that \( q_1 | (a - \sqrt{-p}) \) and hence \( q_1 | b_1 \). Let \( \mu_1 = (a - \sqrt{-p})/(1 - \sqrt{-1}) \in F_3 = Q_2(\sqrt{-1}) \); then \( \mu_1 \equiv 1 \pmod{3^5} \) and hence \( \sqrt{\mu_1} \equiv 1 \pmod{3^5} \) exists in \( F_3 \). Define

\[
z_1 = (\sqrt{\mu_1}, \ldots, b_1, \ldots) \in J,
\]

where \( b_1 = b \). \( \phi(z_1) \) is the class of \( b_1 \) and

\[
z_1^2 = (\mu_1, \ldots, b_1^2, \ldots) \equiv \frac{1}{a - \sqrt{-p}}(\mu_1, \ldots, b_1^2, \ldots) \equiv z_0^{-1} \pmod{J^{(2)}F^*}.
\]

It is easy to see that

\[
\sqrt{\mu_1} \equiv 1 + \frac{a - \sqrt{-p}}{4}(1 - \sqrt{-1}) + \frac{\sqrt{\mu_1} - 1}{2} \pmod{3^5}
\]

\[
\equiv \begin{cases} 
1, & a \equiv 9 \pmod{16}, \\
5, & a \equiv 1 \pmod{16},
\end{cases}
\]

Then,

\[
(-1, z_1) = (-1, \sqrt{\mu_1})_3 \prod_{q_1 | b_1} (-1, b)_{q_1}
\]

\[
= \prod_{q_1 | b} (-1, b)_{q_1} = (-1, b)_2 = (-1)^{(b-1)/2},
\]

\[
(a - \sqrt{-p}, z_1) = (a - \sqrt{-p}, \sqrt{\mu_1})_3 \prod_{q_1 | b_1} (a - \sqrt{-p}, b)_{q_1}
\]

\[
= (1 - \sqrt{-1}, \sqrt{\mu_1})_3 \prod_{q_1 | b_1} (2(a + \sqrt{-p}), b)_{q_1}
\]

\[
= (-1)^{(a-1)/8} \prod_{q_1 | b_1} (4a, b)_{q_1}
\]

\[
= (-1)^{(a-1)/8} \prod_{q_1 | b} (a, b)_{q_1} = (-1)^{(a-1)/8} \left(\frac{a}{b}\right).
\]

Herein we have used that \( (1 - \sqrt{-1}, 5)_3 = (2, 5)_2 = -1 \), \( (1 - \sqrt{-1}, -1 - 2\sqrt{-1})_3 = (1 - \sqrt{-1}, 1 - (1 + \sqrt{-1})^2(1 - \sqrt{-1}))_3 = 1 \) and \( (1 - \sqrt{-1}, -1 + 2\sqrt{-1})_3 = (1 - \sqrt{-1}, 5(1 - 2\sqrt{-1}))_3 = -1 \). 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 \( (\frac{b}{p}) = -(1)^{(a-1)/8} \), then \( F(\sqrt{-1}) \) is a subfield of a \( \mathbb{Z}_2 \)-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 \( \mathbb{Z}_2 \)-extension of \( F \) according as \( (\frac{b}{p}) = (1)^{(a-1)/8} \) or \( (1)^{(a-1)/8} \), and \( \phi(T) = C_F(2) \). In these cases, \( T = (z_1) \).
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

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

Let $c = \prod' l^{v_l(b')}$ and $d = \prod'' l^{v_l(gt)}$, 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 $b_2$ of $F$ such that

$$b_1b_2^2 = ((cg^2/d^2)(r-s\sqrt{-p})), \quad Nb_2 = cgt/d^2.$$

Put $b_2 = cgt/d^2$. The class of $b_2$ 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 $F$: $(q_2) = q_2$. We assume that $q_2 | r + s\sqrt{-p}$ and hence $q_2 | b_1 b_2$. Note that for a prime $q_1 | b$, if $q_1 | b_2$ and $q_1 \nmid t$, then $q_1 | b_2$. 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

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

then

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

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

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

**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 $\left(\frac{q}{p}\right) = (-1)^{(a-1)/8}$ or $(-1)^{(a-1)/8+1}$. We may assume that $\phi(z_2)$ is the class of $b_2$. Therefore such $z_2$ is of the form

$$z_2 = (\sqrt{\mu_2}, \ldots, \frac{b_2}{q_1|b_1}, \ldots, b_2, \ldots).$$

Since

$$\left(\frac{2, \ldots}{3}\right) \equiv 1 \pmod {J(2)F^*},$$

we may assume that $\mu_2$ is prime to 3. There exists $M \in F$ such that

$$M(\mu_2, \ldots, \frac{b_2}{q_1|b_1}, \ldots, \frac{b_2}{q_2|b_2}, \ldots) \equiv (\sqrt{\mu_1}, \ldots, \frac{b_1}{q_1|b_1}, \ldots) \pmod {J(2)}.$$ 

Then $M/\mu_2 = \sqrt{\mu_1}$ and $(M)b_2^2 = b_1$, because $Nb_1 = b_1$ and $Nb_1 = b_2$. Since $b_1^{-1}b_2^2 = ((b_2/b'gt)(r+s\sqrt{-p}))$, $1/M = \mu_2/\sqrt{\mu_1} = \pm (b_2/b'gt)(r+s\sqrt{-p})$. Thus we have that, since

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

we have

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

and

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

we get

$$z_1 \equiv (\sqrt{-1}, \ldots) \pmod {J(2)F^*},$$

which is what we wanted to prove.
\[ \sqrt{-1}^j \mu_2 = \pm \sqrt{-1}^j \left( \frac{b_2}{b'g} t \right) \left( r + s \sqrt{-p} \right) \sqrt{\mu_1}, \quad j = 0 \text{ or } 1, \] is a square in \( Q_2(\sqrt{-1}) \), i.e., \( \equiv \pm 1 \pmod{35} \), if and only if \( \left( \frac{a}{b} \right) = (-1)^{(a-1)/8} \). Since

\[
\mu_2 \equiv \pm \frac{b_2}{b'g t} \left( r + s \sqrt{-1} \right) \sqrt{\mu_1} \equiv \pm \frac{c}{b} \left( r + s \sqrt{-1} \right) \sqrt{\mu_1} \pmod{35}
\]

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

\[
\pm c \left( r + s \sqrt{-1} \right) \pmod{35}, \quad p \equiv 2a - 1 \equiv 1 \pmod{32},
\]

\[
\pm 5c \left( r + s \sqrt{-1} \right) \pmod{35}, \quad p \equiv 2a - 17 \equiv 1 \pmod{32},
\]

\[
\pm 5\left(1 + 2\sqrt{-1} \right) c \left( r + s \sqrt{-1} \right) \pmod{35}, \quad p \equiv 2a - 17 \equiv 1 \pmod{32},
\]

\[
\pm 5\left(-1 + 2\sqrt{-1} \right) c \left( r + s \sqrt{-1} \right) \pmod{35}, \quad p \equiv 2a - 1 \equiv 1 \pmod{32},
\]

we normalize \( \mu_2 \) as follows:

\[
\mu_2 = \begin{cases} 
\frac{b_2}{b'g t} \left( r + s \sqrt{-1} \right) \sqrt{\mu_1}, & s \equiv 0 \pmod{2}, \\
\frac{b_2}{b'g t} \left( r + s \sqrt{-1} \right) \sqrt{\mu_1}, & r \equiv 0 \pmod{2}.
\end{cases}
\]

Then \( \mu_2 \equiv 1 \pmod{35} \) and hence \( \sqrt{\mu_2} \equiv 1 \pmod{35} \) exists in \( Q_2(\sqrt{-1}) \). Put

\[
z_2 = \left( \sqrt{\mu_2}, \ldots, \frac{b_2}{\sqrt{\mu_2}}, \ldots, \frac{b_2}{\sqrt{\mu_2}} \right) \in J;
\]

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

\[
\sqrt{\mu_2} \equiv 1 + 2\gamma(1 - \sqrt{-1}) + 4\delta \pmod{35}
\]

with

\[
\gamma = \begin{cases} 
\frac{1}{16} \left( a - \sqrt{p} + 4rs \right), & s \equiv 0 \pmod{2}, \\
\frac{1}{16} \left( a - \sqrt{p} - 4rs \right), & r \equiv 0 \pmod{2},
\end{cases}
\]

\[
\delta = \begin{cases} 
\frac{1}{16} \left( s^2 + 2rs - \left( \frac{b_2}{b'g t} \right)^2 r^2 \sqrt{p} + 1 \right), & s \equiv 0 \pmod{2}, \\
\frac{1}{16} \left( r^2 - 2rs - \left( \frac{b_2}{b'g t} \right)^2 ps^2 \sqrt{p} + 1 \right), & r \equiv 0 \pmod{2}.
\end{cases}
\]

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

\[
\rho = \begin{cases} 
-s^2 + 2rs + \left( \frac{b_2}{b'g t} \right)^2 ar^2 - 1 \pmod{32}, & s \equiv 0 \pmod{2}, \\
-r^2 - 2rs + \left( \frac{b_2}{b'g t} \right)^2 aps^2 - 1 \pmod{32}, & r \equiv 0 \pmod{2}.
\end{cases}
\]
Hence
\[
(-1, z_2) = (-1, \sqrt{\mu_2})_3 \prod_{q_1 | b_1, b_2} (-1, b_2)_{q_1} \prod_{q_2 | b_1, b_2} (-1, b_2)_{q_2}
\]
\[
= \prod_{q_1 | b_1, b_2} (-1, b_2)_{q_1} \prod_{q_2 | b_1, b_2} (-1, b_2)_{q_2}
\]
\[
= (-1, b_2)_2 = (-1)^{(b_2-1)/2},
\]
\[
(a - \sqrt{-p}, z_2) = (a\sqrt{-p}, \sqrt{\mu_2})_3 \prod_{q_1 | b_1, b_2} (a - \sqrt{-p}, b_2)_{q_1} \prod_{q_2 | b_1, b_2} (a - \sqrt{-p}, b_2)_{q_2}
\]
\[
= (1 - \sqrt{-1}, \sqrt{\mu_2})_3 \prod_{q_1 | b_1, b_2} (2(a + \sqrt{-p}), b_2)_{q_1} \prod_{q_2 | b_1, b_2} ((r + as)s, b_2)_{q_2}
\]
\[
= (-1)^{p/16} \prod_{q_1 | b_1, b_2} (a, b_2)_{q_1} \prod_{q_2 | b_1, b_2} ((r + as)s, b_2)_{q_2} = (-1)^{p/16} \chi
\]

with
\[
\chi = \prod_{q_1 | b_1} \left( \frac{a}{q_1} \right)^{v_1(b_2)} \prod_{q_2 | b_2} \left( \frac{(r + as)s}{q_2} \right)^{v_2(b_2)}
\]

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 \( b_2, \rho, \chi \) as above. If \( b_2 \equiv 1 \pmod{4} \) and \( \chi = (-1)^{p/16+1} \), then \( F(\sqrt{-1}) \) is a subfield of a \( \mathbb{Z}_2 \)-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 \( \mathbb{Z}_2 \)-extension of \( F \) according as \( \chi = (-1)^{p/16} \) or \( (-1)^{p/16+1} \), 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 \( \chi = (-1)^{p/16} \), \( T \) has a proper subgroup \( \langle z_2 \rangle \) and we can also determine the quadratic subfield of a noncyclotomic \( \mathbb{Z}_2 \)-extension of \( F \) after a finite number of procedures similar to the above, since \( C_F(2) \) is a finite group.

**References**


DEPARTMENT OF MATHEMATICS, KUMAMOTO UNIVERSITY, KUMAMOTO, JAPAN