SOME QUESTIONS ON THE IDEAL CLASS GROUP OF IMAGINARY ABELIAN FIELDS

TSUYOSHI ITOH

Abstract. Let \( k \) be an imaginary quadratic field. Assume that the class number of \( k \) is exactly an odd prime number \( p \), and \( p \) splits into two distinct primes in \( k \). Then it is known that a prime ideal lying above \( p \) is not principal. In the present paper, we shall consider a question whether a similar result holds when the class number of \( k \) is \( 2p \). We also consider an analogous question for the case that \( k \) is an imaginary quartic abelian field.

1. Questions

At first, we shall introduce the following:

**Theorem A.** Let \( k \) be an imaginary quadratic field. Assume that the class number of \( k \) is exactly an odd prime number \( p \) which splits into two distinct primes \( p \) and \( p' \) in \( k \). Then \( p \) is not principal.

This result is mentioned in the proof of [2, Proposition 2.4]. In the present paper, we try to generalize the above result. In particular, we shall consider the following two questions:

**Question 1.1.** Let \( k \) be an imaginary quadratic field. Assume that the class number of \( k \) is exactly \( 2p \) with an odd prime \( p \) which splits into two distinct primes \( p \) and \( p' \) in \( k \). Then is \( p^2 \) not principal?

**Question 1.2.** Let \( k \) be an imaginary quartic abelian field. Assume that both of the class number and the relative class number of \( k \) are exactly an odd prime number \( p \), and \( p \) splits completely in \( k \). Let \( p \) be a prime ideal of \( k \) lying above \( p \). Then is \( p \) not principal?

The assertion in the above questions (and Theorem A) implies that all classes in the Sylow \( p \)-subgroup of the ideal class group contain a power of \( p \). Of course, it is not satisfied in general (see Remark 2.9).

Question 1.1 has originally arisen from a question on Iwasawa theory. Under the assumption of Theorem A, it is known that both of the Iwasawa \( \lambda \)-...
and μ-invariants of the “p-ramified” $\mathbb{Z}_p$-extension of $k$ are zero ([2, Proposition 2.4]). If Question 1.1 has a positive answer, we can obtain a similar result (see section 4).

The author expects that at least Question 1.1 always has a positive answer.

We shall consider Question 1.1 in section 2. We will show that Question 1.1 has a positive answer for many imaginary quadratic fields. Especially, if the absolute value of the discriminant of $k$ is “small”, then Question 1.1 has a positive answer for $k$ (Corollary 2.5). Moreover, if a rational prime which is smaller than 1525 ramifies in $k$, then Question 1.1 has a positive answer for $k$ (Corollary 2.8).

In section 3, we shall consider Question 1.2. We will show that if $k$ is a bicyclic biquadratic field, then Question 1.2 has a positive answer for $k$ (Proposition 3.1). However, little is known in the case that $k$ is a cyclic quartic field.

In section 4, we will give an application to Iwasawa theory.

We will use the following notations throughout the present paper. We denote by $(\frac{-}{\mathcal{K}})$ the quadratic residue symbol. Let $k$ be an algebraic number field. We denote by $\text{Cl}(k)$ the ideal class group of $k$, $h(k)$ the class number of $k$, and $d(k)$ the absolute value of the discriminant of $k$. For a fractional ideal $\mathfrak{a}$ of $k$, we denote by $c(\mathfrak{a})$ the ideal class of $k$ which contains $\mathfrak{a}$. For a finite extension $k'/k$ of algebraic number fields, we denote by $N_{k'/k}$ the norm mapping from $k'$ to $k$. If $k$ is a CM-field, then we denote by $k^+$ the maximal real subfield of $k$ and $h^-(k) = h(k)/h(k^+)$ the relative class number.

2. Consideration for Question 1.1

First, we shall briefly recall the proof of Theorem A which is stated in [2]. Let $k$ be an imaginary quadratic field such that $h(k) = p$ with an odd prime $p$ which splits into two distinct primes $p$ and $p'$ in $k$. Since $h(k)$ is odd, we may write $k = \mathbb{Q}(\sqrt{-q})$ with an odd prime number $q$ which satisfies $q \equiv 3 \pmod{4}$. If $p$ is principal, then we have an inequality $p \geq q/4$ by taking the norm of a generator of $p$ to $\mathbb{Q}$. However, we can see $p = h(k) < q/4$ by using Dirichlet’s class number formula. It is a contradiction.

Let $k$ be an imaginary quadratic field such that $h(k) = 2p$ with an odd prime $p$ which splits into two distinct primes $p$ and $p'$ in $k$. We shall apply the above method for Question 1.1. Assume that $p^2$ is principal. Then $p^2 \geq d(k)/4$. Since $h(k) = 2p$, if $h(k) < \sqrt{d(k)}$ then Question 1.1 has a positive answer. However, the Brauer-Siegel theorem implies that

$$\frac{\log h(k)}{\log \sqrt{d(k)}} \to 1, \quad (d(k) \to \infty).$$
Hence it seems difficult to solve Question 1.1 by applying this method directly. If we remove the restriction on the class number, an imaginary quadratic field $k$ which satisfies $h(k) > \sqrt{d(k)}$ really exists.

We begin a more detailed consideration for Question 1.1. Since $h(k) = 2p$, we may assume that $k$ is one of the following:

(a) $k = \mathbb{Q}(\sqrt{-q})$ with an odd prime $q$ satisfying $q \equiv 5 \pmod{8}$,
(b) $k = \mathbb{Q}(\sqrt{-2q})$ with an odd prime $q$ satisfying $q \equiv 3, 5 \pmod{8}$, 
(c) $k = \mathbb{Q}(\sqrt{-lq})$ with odd primes $l, q$ satisfying $l \equiv 1, q \equiv 3 \pmod{4}$ and $(\frac{q}{l}) = -1$.

**Proposition 2.1.** Assume that $k$ is of the form (a) or (b), that is, the prime 2 ramifies in $k$. Then Question 1.1 has a positive answer for $k$.

**Proof.** We shall only show for the case that $k$ is of the form (b). The rest case can be proven similarly.

Let $p$ be a prime ideal in $k$ lying above $p$. Assume that $p^2$ is principal. We take a generator $a + b\sqrt{-2q}$ of $p^2$, where $a$ and $b$ are integers. Since $p$ splits in $k$, we see $ab \neq 0$. We may assume that $a > 0$. By taking the norm of $a + b\sqrt{-2q}$ to $\mathbb{Q}$, we see $p^2 = a^2 + 4b^2q$. Hence $(p - a)(p + a) = 4b^2q$. Note that the right hand side is positive and then $p > a$. Since $q$ is a prime number, $q$ divides $p + a$ or $p - a$. If $q$ divides $p - a$, then $p > p - a \geq q$. Otherwise, $2p > p + a \geq q$. Consequently we have the inequality $2p > q$.

On the other hand, by using a modified version of Dirichlet’s class number formula (see, e.g., [8, Theorem 9.7.7]), we can see

$$2p = h(k) = \sum_{i=0}^{2q} \chi_k(i),$$

where $\chi_k$ is the Dirichlet character corresponding to $k$. Since $\chi_k(i) = 0$ for even $i$, the right hand side is less than or equal to $q$. Hence we see that $2p \leq q$. It is a contradiction. \hfill $\square$

In the rest of this section, we assume that $k$ is of the form (c). In this case, Question 1.1 has not been solved yet. However, we can see that Question 1.1 has a positive answer for many cases.

**Proposition 2.2.** Assume that $k$ is of the form (c) and $h(k) = 2p$ with an odd prime $p$ which splits in $k$. If $(\frac{l}{p}) = 1$, then Question 1.1 has a positive answer for $k$.

**Proof.** Assume that $(\frac{l}{p}) = 1$. We note that $H := \mathbb{Q}(\sqrt{l}, \sqrt{-q})$ is the Hilbert 2-class field of $k$. By the assumption, the prime $p$ lying above $p$ splits in $H/k$. Hence, the order of the ideal class $c(p)$ containing $p$ is 1 or $p$. If the order
of $c(p)$ is 1, then we can see $p > lq/4$ by taking the norm of a generator of $p$ to $\mathbb{Q}$. Hence $h(k) = 2p > lq/2$. However, we can easily see that $h(k) < lq/2$ by using Dirichlet’s class number formula. It is a contradiction. Then the order of $c(p)$ is $p$, and this implies that $p^2$ is not principal. 

We will show that if $d(k)$ is “small” then Question 1.1 has a positive answer. First, we shall prove the following lemma.

**Lemma 2.3.** Assume that $k$ is of the form (c) and $h(k) = 2p$ with an odd prime $p$ which splits two distinct primes $p$ and $p'$ in $k$. Moreover, assume that $(\frac{k}{p}) = -1$. If $p^2$ is principal, then there are non-zero integers $b'$ and $c'$ such that

$$p = \frac{(b')^2l + (c')^2q}{4}$$

and $b' \equiv c' \pmod{2}$.

**Proof.** Under the assumptions, we can see that the order of $c(p)$ is exactly 2 by using the argument given in the proof of Proposition 2.2. By Hilbert 94 or Tannaka-Terada’s principal ideal theorem, we see that $p$ becomes principal in $\mathbb{Q}(\sqrt{l}, \sqrt{-q})$. We put $H = \mathbb{Q}(\sqrt{l}, \sqrt{-q})$ and denote by $O_H$ the ring of algebraic integers in $H$. Let $\alpha \in O_H$ be a generator of $pO_H$. We can write

$$\alpha = \frac{a + b\sqrt{l} + c\sqrt{-q} + d\sqrt{-lq}}{4}$$

with some integers $a, b, c, d$.

We note that $N_{H/\mathbb{Q}(\sqrt{l})}\alpha$ is a totally positive integer of $\mathbb{Q}(\sqrt{l})$. Since $N_{H/\mathbb{Q}(\sqrt{l})}\alpha$ generates the unique prime ideal of $\mathbb{Q}(\sqrt{l})$ lying above $p$, we can write $N_{H/\mathbb{Q}(\sqrt{l})}\alpha = p\epsilon$ with a totally positive unit $\epsilon$ of $\mathbb{Q}(\sqrt{l})$. We note that the norm of the fundamental unit of $\mathbb{Q}(\sqrt{l})$ to $\mathbb{Q}$ is $-1$. From this, we can take $\alpha$ which satisfies $N_{H/\mathbb{Q}(\sqrt{l})}\alpha = p$ by multiplying some power of the fundamental unit. Hence we have the equation

$$N_{H/\mathbb{Q}(\sqrt{l})}\alpha = \frac{(a^2 + b^2l + c^2q + d^2lq) + (2ab + 2cdq)\sqrt{l}}{16} = p.$$ 

This implies that $2ab + 2cdq = 0$, and then

$$p = \frac{a^2 + b^2l + c^2q + d^2lq}{16}.$$ 

Next, we shall take the norm of $\alpha$ to $\mathbb{Q}(\sqrt{-q})$. If $q > 3$, we see $N_{H/\mathbb{Q}(\sqrt{-q})}\alpha = \pm p$. If $q = 3$, we can take $\alpha$ which satisfies $N_{H/\mathbb{Q}(\sqrt{l})}\alpha = p$.
and $N_{H/Q(\sqrt{-q})} \alpha = \pm p$ by multiplying some third root of unity. Hence we have the equation

$$N_{H/Q(\sqrt{-q})} \alpha = \frac{(a^2 - b^2l - c^2q + d^2lq) + (2ac - 2bdl)\sqrt{-q}}{16} = \pm p.$$ 

This implies that $2ac - 2bdl = 0$, and then

$$\pm p = \frac{a^2 - b^2l - c^2q + d^2lq}{16}.$$ 

If $N_{H/Q(\sqrt{-q})} \alpha = p$, then $b = c = 0$. In this case, we can see that both of $a$ and $d$ are even by writing explicitly with the following integral basis:

$$(1, 1 + \sqrt{l}, 1 + \sqrt{-q}, 1 + \sqrt{l} + \sqrt{-q} + \sqrt{-lq})$$.

Hence we can write $\alpha = (a' + d'\sqrt{-lq})/2$ with integers $a' = a/2$ and $d' = d/2$. This implies that $p$ is already principal in $k$. However, it contradicts to the fact that the order of $c(p)$ is 2. Then we see $N_{H/Q(\sqrt{-q})} \alpha = -p$, and hence $a = d = 0$. We can see that both of $b$ and $c$ are even and $b \equiv c \pmod{4}$ by writing $\alpha$ explicitly with the above integral basis. Hence we can write $\alpha = (b'\sqrt{l} + c'\sqrt{-q})/2$ with integers $b' = b/2$ and $c' = c/2$ and they satisfy $b' \equiv c' \pmod{2}$.

Since $p$ is prime to $l$ and $q$, we see that $b'c' \neq 0$. The lemma follows. \qed

By using this, we can obtain the following:

**Proposition 2.4.** Assume that $k$ is of the form $(c)$ and $h(k) = 2p$ with an odd prime $p$ which splits in $k$. If $h(k) < (l + q)/2$, then Question 1.1 has a positive answer for $k$. Moreover, if $lq \equiv 7 \pmod{8}$ and $h(k) < \min\{2l + 8q, 8l + 2q\}$, then Question 1.1 has a positive answer for $k$.

**Proof.** Throughout the proof, we may suppose that $\left(\frac{l}{p}\right) = -1$ by Proposition 2.1.

Assume that $p^2$ is principal. Then by Lemma 2.3, we can write $p = ((b')^2l + (c')^2q)/4$ with some non-zero integers $b'$ and $c'$. Hence we see $p \geq (l + q)/4$. Since $h(k) = 2p$, the former part follows.

Assume that $lq \equiv 7 \pmod{8}$ and $p^2$ is principal. Similarly, we can write $4p = (b')^2l + (c')^2q$. Since $p$ is odd, we see $4p \equiv 4 \pmod{8}$. Recall that $b' \equiv c' \pmod{2}$. If both of $b'$ and $c'$ are odd, then

$$(b')^2l + (c')^2q \equiv l + q \equiv 0 \pmod{8}$$

from the assumption that $lq \equiv 7 \pmod{8}$. Hence both of $b'$ and $c'$ must be even, and $p = (b'')^2l + (c'')^2q$ with $b'' = b'/2$ and $c'' = c'/2$. Moreover,
either \( b'' \) or \( c'' \) must be even because \( p \) is odd. Hence we see that \( p \geq \min\{l + 4q, 4l + q\} \). The latter part follows.

Next, we shall quote the following:

**Theorem B** (Ramaré [13]). Let \( \chi \) be a primitive Dirichlet character of conductor \( f \). Assume that \( \chi(-1) = -1 \) and \( f \) is odd. Then

\[
\left| 1 - \frac{\chi(2)}{2} \right| L(1, \chi) \leq \frac{1}{4} \left( \log f + 5 - 2 \log \frac{3}{2} \right),
\]

where \( L(s, \chi) \) is the Dirichlet \( L \)-function.

Let \( k \) be an imaginary quadratic field which is of the form (c). From the above theorem, we obtain the following upper bound:

\[
h(k) \leq \frac{\sqrt{lq}}{2(2 - \chi_k(2))\pi} \left( \log lq + 5 - 2 \log \frac{3}{2} \right)
\]

by using the analytic class number formula, where \( \chi_k \) is the Dirichlet character corresponding to \( k \). We mentioned at the beginning of this section that if \( h(k) < \sqrt{lq} \) then Question 1.1 has a positive answer. Moreover, if \( lq \equiv 7 \pmod{8} \) and \( h(k) < 8\sqrt{lq} \) then Question 1.1 has a positive answer by Proposition 2.4. Connecting the above upper bound of \( h(k) \), we obtain the following:

**Corollary 2.5.** Assume that \( k \) is of the form (c) and \( h(k) = 2p \) with an odd prime \( p \) which splits in \( k \).

- If \( lq \equiv 3 \pmod{8} \) and
  \[
lq < \frac{9}{4} \exp(6\pi - 5) = 2327920965.965\ldots,
\]
  then Question 1.1 has a positive answer.
- If \( lq \equiv 7 \pmod{8} \) and
  \[
lq < \frac{9}{4} \exp(16\pi - 5) = 102501865638106235900.902\ldots,
\]
  then Question 1.1 has a positive answer.

**Remark 2.6.** By using the method which is given in the proof of Proposition 2.4, we can see that if \( lq \equiv 3 \pmod{8} \), \((l + q)/4\) is not a prime number, and \( h(k) < \min\{(l + 9q)/2, (9l + q)/2\} \), then Question 1.1 has a positive answer for \( k \). In particular, if \( lq \equiv 3 \pmod{8} \), \((l + q)/4\) is not a prime number, and

\[
lq < \frac{9}{4} \exp(18\pi - 5) = 54888893724926503841046.318\ldots,
\]

then Question 1.1 has a positive answer.
Next, we will show that if a “small” prime ramifies in \( k \), then Question 1.1 has a positive answer. In the following, we use slightly different notations.

We put \( k = \mathbb{Q}(\sqrt{-rs}) \) with rational primes \( r, s \) which satisfy \( rs \equiv 3 \pmod{4} \) and \( \left( \frac{r}{s} \right) = -1 \). Fix an odd prime \( s \), and put

\[
fs(x) = \frac{x + s}{2} - \frac{\sqrt{xs}}{6\pi} \left( \log sx + 5 - 2\log\frac{3}{2} \right).
\]

Assume that \( h(k) = 2p \) with an odd prime \( p \) which splits in \( k \). By Proposition 2.4 and (1), if \( fs(r) > 0 \), then Question 1.1 has a positive answer for \( k \).

We put \( \kappa = (9/4)\exp(6\pi - 5) \). If \( r < \kappa/s \), then \( fs(r) > 0 \). Moreover, if \( fs'(\kappa/s) > 0 \), then we see that \( fs(r) > 0 \) for all \( r \). We note that if

\[
s < \frac{9\pi \exp\left(\frac{6\pi - 5}{2}\right)}{6\pi + 2} = 1379.394\ldots,
\]

then \( fs'(\kappa/s) > 0 \). This implies:

**Proposition 2.7.** We put \( k = \mathbb{Q}(\sqrt{-rs}) \) with rational primes \( r, s \) which satisfy \( rs \equiv 3 \pmod{4} \) and \( \left( \frac{r}{s} \right) = -1 \). Assume that \( h(k) = 2p \) with an odd prime \( p \) which splits in \( k \). If \( s \leq 1379 \), then Question 1.1 has a positive answer for \( k \).

Moreover, if we fix a prime \( s > 1379 \), then at most finitely many primes \( r \) satisfy \( fs(r) < 0 \). Hence we can check whether Question 1.1 has a positive answer for all \( r \). For example, we put \( s = 1523 \). There are only 23 primes \( r \) which satisfies \( rs \geq \kappa \), \( rs \equiv 3 \pmod{4} \), \( \left( \frac{r}{s} \right) = -1 \), and \( fs(r) < 0 \). These are 1609, 1621, 1637, 1693, 1733, 1741, 1777, 1801, 1861, 1913, 1933, 1973, 2053, 2069, 2089, 2113, 2153, 2161, 2237, 2269, 2281, 2297, 2309. All primes \( r \) in this list satisfy \( rs < 10^{20} \). Hence by Corollary 2.5 and Remark 2.6, if \( rs \equiv 7 \pmod{8} \) or \( (r+s)/4 \) is not a prime, then Question 1.1 has a positive answer.

From this, we see that the primes \( r \) for which we must check the class number of \( \mathbb{Q}(\sqrt{-rs}) \) are 1913 and 2153. We find that \( h(\mathbb{Q}(\sqrt{-1523 \times 1913})) = 310 \) and \( h(\mathbb{Q}(\sqrt{-1523 \times 2153})) = 350 \). Both fields do not satisfy the assumption of Question 1.1. Hence if \( s = 1523 \), then Question 1.1 has a positive answer for all \( r \). Similarly, we checked that Question 1.1 has a positive answer if \( 1379 < s < 1525 \). (We note that \( \sqrt{\kappa} = 1525.752\ldots \)) As a consequence, we have the following:

**Corollary 2.8.** Let \( k \) be an imaginary quadratic field. Assume that \( h(k) = 2p \) with an odd prime \( p \) which splits in \( k \). If a rational prime which is smaller than 1525 ramifies in \( k \), then Question 1.1 has a positive answer for \( k \).
Remark 2.9. We can also consider the following question: if \( h(k) = 3p \) and \( p \) splits in \( k \), then is the cube of a prime lying above \( p \) not principal? However, this question has a negative answer. We put \( k = \mathbb{Q}(\sqrt{-15391}) \). Then \( h(k) = 3 \times 31 \) and the rational prime 31 splits in \( k \). Let \( p \) be a prime in \( k \) lying above 31. Then \( p^3 \) is principal because \( 31^3 = (120 + \sqrt{-15391})(120 - \sqrt{-15391}) \).

3. Consideration for Question 1.2

In this section, let \( k \) be an imaginary quartic abelian field. In this case, \( k \) is a bicyclic biquadratic field or a cyclic quartic field. Assume that \( k \) satisfies \( h(k) = h^-(k) = p \) with an odd prime \( p \) which splits completely in \( k \).

First, we shall show the following:

**Proposition 3.1.** If \( k \) is a bicyclic biquadratic field, then Question 1.2 has a positive answer.

**Proof.** Since \( h^-(k) = p \), there is a unique imaginary quadratic subfield \( k' \) of \( k \) which satisfies \( h(k') = p \) or \( h(k') = 2p \). Let \( A(k) \) (resp. \( A(k') \)) be the Sylow \( p \)-subgroup of \( \text{Cl}(k) \) (resp. \( \text{Cl}(k') \)). Let \( p \) be a prime of \( k' \) lying above \( p \). By Theorem A, Proposition 2.1, and Proposition 2.2, we can see that \( A(k') \) is generated by \( c(p) \). Let \( \mathfrak{p} \) be a prime of \( k \) lying above \( p \). Since \( p \) is not principal and \( p = N_{k/k'} \mathfrak{p} \), it follows that \( \mathfrak{p} \) is not principal. (We can also show this by using the following method. We denote by \( \sigma_{\mathfrak{p}} \) (resp. \( \sigma_p \)) the Frobenius element of \( \text{Gal}(H(k)/k) \) (resp. \( \text{Gal}(H(k')/k') \)) corresponding to \( \mathfrak{p} \) (resp. \( p \)), where \( H(k) \) (resp. \( H(k') \)) is the Hilbert class field of \( k \) (resp. \( k' \)). Since the restriction \( \sigma_{\mathfrak{p}}|_{H(k')} \) coincides with \( \sigma_p \) and the order of \( \sigma_p \) is divisible by \( p \), we see that the order of \( \sigma_{\mathfrak{p}} \) is exactly \( p \).) The proposition follows. \( \square \)

We assume that \( k \) is a cyclic quartic field. If \( h^-(k) \) is an odd prime, then we can see that the conductor of \( k \) is an odd prime \( q \) by [3, Theorem 3’]. Moreover, we see \( q \equiv 5 \pmod{8} \) because \( k \) is an imaginary cyclic quartic field. By specializing the method given in the proof of [9, Theorem D], we can obtain the following:

**Lemma 3.2.** Let \( q \) be an odd prime which satisfies \( q \equiv 5 \pmod{8} \), and \( k \) the imaginary cyclic quartic field of conductor \( q \). Let \( p \) be a rational prime which splits completely in \( k \), and \( \mathfrak{p} \) a prime of \( k \) lying above \( p \). If \( \mathfrak{p} \) is principal, then \( p > q/8 \).

**Proof.** Let \( \varepsilon \) be the fundamental unit of \( k^+ = \mathbb{Q}(\sqrt{q}) \). Since \( h(k^+) \) is odd, we can see that \( k/k^+ \) has a relative integral basis (see, e.g., [6]).
Assume that $\mathfrak{P}$ is principal. We claim that

$$\mathfrak{P} = \left( \frac{\alpha + \beta \sqrt{\varepsilon / q}}{2} \right)$$

with non-zero algebraic integers $\alpha, \beta$ in $k^+$. It is known that $k = \mathbb{Q}(\sqrt{-(q + b \sqrt{q})})$ with an even integer $b$ (see, e.g., [10]). Since $k/k^+$ has a relative integral basis, we can write $k = k^+(\sqrt{\varepsilon / q})$ by using [6, Lemma 2]. Moreover, we can apply Theorem 2 of [6]. From this theorem, every algebraic integer of $k$ is written in the form $\frac{\alpha + \beta \sqrt{\varepsilon / q}}{2}$ with algebraic integers $\alpha, \beta$ in $k^+$. Hence we can take a generator of $\mathfrak{P}$ written in the above form.

Since $p$ splits completely in $k$, both of $\alpha$ and $\beta$ must be non-zero. The claim follows.

By taking the norm of the above generator to $\mathbb{Q}$, we obtain the following:

$$p = \frac{1}{16} \left\{ (\alpha \sigma)^2 + (\beta \sigma)^2 q + \sqrt{q}((\alpha \sigma)^2 \beta^2 \varepsilon - \alpha^2 (\beta \sigma)^2 \varepsilon^\sigma) \right\} ,$$

where $\sigma$ is the nontrivial automorphism of Gal($k^+/\mathbb{Q}$). We note that $\sqrt{q}((\alpha \sigma)^2 \beta^2 \varepsilon - \alpha^2 (\beta \sigma)^2 \varepsilon^\sigma)$ is a positive rational integer and divisible by $q$. Hence we see $p > (q + q)/16 = q/8$. \(\square\)

As a conclusion of the above lemma, if $h^-(k) < q/8$ then Question 1.2 has a positive answer. By using Theorem B, if $q > 5$ then we have the following upper bound:

$$h^-(k) \leq \frac{q}{40 \pi^2} \left( \log q + 5 - 2 \log \frac{3}{2} \right)^2$$

(see also Corollary 11 of [11]). Unfortunately, the above lemma is not useful to deduce that Question 1.2 has a positive answer for all $k$. In fact, if we remove the restriction on the class number, there exist imaginary cyclic quartic fields $k$ of conductor $q$ which satisfy $h(k) > q/8$ (see [10]).

We note that if an odd prime $p$ divides $h(k)$ and $p$ does not divide $h(k^+)$, then the $p$-rank of the Sylow $p$-subgroup of $\text{Cl}(k)$ is greater than or equal to the order of $p$ in $(\mathbb{Z}/4\mathbb{Z})^\times$ (see, e.g., [14, Theorem 10.8]). Hence we see that if $h(k) = h^-(k) = p$, then $p \equiv 1 \pmod{4}$. On the other hand, we can obtain the following result. It is also considered as an analog of Theorem A.

**Proposition 3.3.** Let $q$ be an odd prime which satisfies $q \equiv 5 \pmod{8}$, and $k$ the imaginary cyclic quartic field of conductor $q$. Assume that $k$ satisfies $h(k) = h^-(k) = p^2$ with an odd prime $p \equiv 3 \pmod{4}$ which splits completely in $k$. Then $\text{Cl}(k)$ is generated by the classes containing a prime ideal lying above $p$. 
Proof. We may assume that \( q \geq 13 \). Let \( \mathfrak{p} \) be a prime of \( k \) lying above \( p \). By Lemma 3.2, we see that if \( h(k) < q^2/64 \), then \( \mathfrak{p} \) is not principal. We note that

\[
\frac{q}{40 \pi^2} \left( \log q + 5 - 2 \log \frac{3}{2} \right)^2 < \frac{q^2}{64}
\]
holds if \( q \geq 13 \). Hence \( \mathfrak{p} \) is not principal by (2).

Let \( D \) be the subgroup of \( \text{Cl}(k) \) generated by the classes containing a prime ideal lying above \( p \). Since \( \mathfrak{p} \) is not principal, \( D \) is a nontrivial \( p \)-group. We note that \( \text{Gal}(k=\mathbb{Q}) \) acts on \( D \). By using the same argument given in the proof of [14, Theorem 10.8], we can see that the \( p \)-rank of \( D \) is greater than or equal to 2. Since \( \text{Cl}(k) \cong (\mathbb{Z}/p\mathbb{Z})^2 \), the assertion follows. \( \square \)

4. Application to Iwasawa theory

Our questions relate to a question on the Iwasawa invariants of certain non-cyclotomic \( \mathbb{Z}_p \)-extensions. Let \( N \) be an algebraic number field and \( p \) a rational prime. For a \( \mathbb{Z}_p \)-extension \( M/N \), we denote by \( \lambda(M/N), \mu(M/N), \) and \( \nu(M/N) \) the Iwasawa \( \lambda \)-, \( \mu \)-, and \( \nu \)-invariants of \( M/N \), respectively.

4.1. Let \( k \) be an imaginary quadratic field and \( p \) an odd prime which splits into two distinct primes \( p \) and \( p' \) in \( k \). By class field theory, there exists a unique \( \mathbb{Z}_p \)-extension \( K/k \) which is unramified outside \( \mathfrak{p} \). As an analog of Greenberg’s conjecture, there is a question (cf. [2]): are the invariants \( \lambda(K/k) \) and \( \mu(K/k) \) always zero?

For example, if \( h(k) \) is not divisible by \( p \), then \( \lambda(K/k) = \mu(K/k) = 0 \). Moreover, it is known that if \( A(k) \) is generated by a power of \( c(p) \), then \( \lambda(K/k) = \mu(K/k) = 0 \) (see [12], [2]). Hence, if \( h(k) = p \), then \( \lambda(K/k) = \mu(K/k) = 0 \) by Theorem A ([2]). Similarly, if \( h(k) = 2p \) and Question 1.1 has a positive answer for \( k \), then \( \lambda(K/k) = \mu(K/k) = 0 \).

Moreover, if \( A(k) \) is generated by a power of \( c(p) \), then Greenberg’s generalized conjecture (GGC) also holds for \( k \) and \( p \) ([12]). (For the detail of GGC, see [5].)

4.2. Next, let \( k \) be an imaginary quartic abelian field and \( p \) an odd prime which splits completely in \( k \). Let \( \mathfrak{p}_1 \) and \( \mathfrak{p}_2 \) be the distinct primes in \( k^+ \) lying above \( p \), and \( \mathfrak{p}_1 \) (resp. \( \mathfrak{p}_2 \)) be a prime in \( k \) lying above \( \mathfrak{p}_1 \) (resp. \( \mathfrak{p}_2 \)). By class field theory, there exists a unique \( \mathbb{Z}_p \)-extension \( K/k \) which is unramified outside \( \mathfrak{p}_1, \mathfrak{p}_2 \) (see, e.g., [7, Lemma 2.2]). Let \( k^+ \) be the cyclotomic \( \mathbb{Z}_p \)-extension of \( k^+ \). In [7], it is shown that if \( h(k) \) is not divisible by \( p \) and \( \lambda(k^+/k^+) = \mu(k^+/k^+) = \nu(k^+/k^+) = 0 \), then \( \lambda(K/k) = \mu(K/k) = 0 \). Moreover, Goto [4] independently obtained the following (the statement is modified by using the argument given in [7]):
Theorem C (Goto [4]). If both of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are totally ramified, $A(k)$ is generated by a power of $c(\mathfrak{P}_1)$ and $c(\mathfrak{P}_2)$, and $\lambda(k^+_\infty/k^+) = \mu(k^+_\infty/k^+) = \nu(k^-_\infty/k^+) = 0$, then $\lambda(K/k) = \mu(K/k) = 0$.

By using this, we can see the following:

Proposition 4.1. Assume that $h(k) = p$ and Question 1.2 has a positive answer for $k$. If $\lambda(k^+_\infty/k^+) = \mu(k^+_\infty/k^+) = \nu(k^-_\infty/k^+) = 0$, then $\lambda(K/k) = \mu(K/k) = 0$.

Proof. For a positive integer $n$, let $k_n$ be the $n$-th layer of $K/k$. By using the argument given in the proof of [7, Proposition 3.2], we can see that both of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are totally ramified or unramified in $k_1/k$. If both of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are totally ramified, then the assertion follows from Theorem C. Otherwise, we can see that the order of $A(k_n)^{\text{Gal}(k_n/k)}$ is 1 for $n \geq 1$ by using the genus formula. Hence $A(k_n)$ is trivial for all $n \geq 1$.

Proposition 4.2. Assume that $k$ is a cyclic quartic field, $h(k) = h^-(k) = p^2$, and $p \equiv 3 \pmod{4}$. If both of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are totally ramified and $\lambda(k^+_\infty/k^+) = \mu(k^+_\infty/k^+) = \nu(k^-_\infty/k^+) = 0$, then $\lambda(K/k) = \mu(K/k) = 0$.

Proof. Let $D$ be the subgroup of $\text{Cl}(k)$ generated by the classes containing a prime ideal lying above $p$. By Proposition 3.3, we see that $\text{Cl}(k) = D$. Since $h(k^+) = 1$, $D$ is actually generated by $c(\mathfrak{P}_1)$ and $c(\mathfrak{P}_2)$. Hence we can apply Theorem C.

By using the argument given in [7] (with some modifications), we can see that if $k$ satisfies the assumption of Proposition 4.1 or Proposition 4.2, then GGC for $k$ and $p$ holds.

Acknowledgements

The author would like to express his thanks to the referee for his/her comments. The calculation of class numbers and all other computations are done by using KASH [1].

References


College of Science and Engineering, Ritsumeikan University, 1-1-1 Noji Higashi, Kusatsu, Shiga 525-8577, JAPAN

e-mail address: tsitoh@se.ritsumei.ac.jp

(Received July 10, 2006)
(Revised June 22, 2007)