**DIVISIBILITY BY 16 OF CLASS NUMBER OF QUADRATIC FIELDS WHOSE 2-CLASS GROUPS ARE CYCLIC**

YOSHIHIKO YAMAMOTO*

(Received August 5, 1982)

0. Introduction. Let $K=\mathbb{Q}(\sqrt{D})$ be the quadratic field with discriminant $D$, and $H(D)$ and $h(D)$ be the ideal class group of $K$ and its class number respectively. The ideal class group of $K$ in the narrow sense and its class number are denoted by $H^+(D)$ and $h^+(D)$ respectively. We have $h^+(D)=2h(D)$ if $D>0$ and the fundamental unit $\varepsilon_D (>1)$ has the norm 1, and $h^+(D)=h(D)$, otherwise. We assume, throughout the paper, that $|D|$ has just two distinct prime divisors, written $p$ and $q$, so that the 2-class group of $K$ (i.e. the Sylow 2-subgroup of $H^+(D)$ because we mean in the narrow sense) is cyclic. Then the discriminant $D$ can be written uniquely as a product of two prime discriminants $d_1$ and $d_2$, $D=d_1d_2$, such that $p|d_1$ and $q|d_2$ (cf. [16], for example).

By Redei and Reichardt [13] (cf. proposition 1.2 below), $h^+(D)$ is divisible by 4 if and only if $D$ belongs to one of the following 6 types:

(R1) $D=pq$, $d_1=p$, $d_2=q$, $p\equiv q\equiv 1 \pmod{4}$, and $\left(\frac{p}{q}\right)=1$ (by reciprocity);

(R2) $D=8q$, $d_1=8 \pmod{p=2}$, $d_2=q$, and $q\equiv 1 \pmod{8}$;

(I1) $D=-pq$, $d_1=-p$, $d_2=q$, $p\equiv 3 \pmod{4}$, $q\equiv 1 \pmod{4}$, and $\left(\frac{-p}{q}\right)=1$

(= $\left(\frac{-1}{p}\right)$ by reciprocity);

(I2) $D=-8p$, $d_1=-p$, $d_2=8 \pmod{q=2}$, and $p\equiv 7 \pmod{8}$;

(I3) $D=-8q$, $d_1=-8 \pmod{p=2}$, $d_2=q$, and $q\equiv 1 \pmod{8}$;

(I4) $D=-4q$, $d_1=-4 \pmod{p=2}$, $d_2=q$, and $q\equiv 1 \pmod{8}$;

where $(-)$ is the Legendre-Jacobi-Kronecker symbol.

Conditions for $h^+(D)$ to be divisible by 8 have been given by several authors for each case or cases ([1, 2, 3, 5, 6, 7, 8, 9, 11, 12, 15]). Some of them are reformulated in section 3. The purpose of this paper is to give some conditions for the divisibility by 16 of $h^+(D)$ for each case (cf. theorems 5.4, 5.5, 5.6, 5.7, 5.8, and 6.7). The main ideas were announced in [18] and [19].

While in preparation of the manuscript P. Kaplan informed me that theorem 6.7 was proved also by K.S. Williams with a different method and furthermore he gave a congruence for $h(-4q)$ modulo 16 ([17]).

* Research supported partly by Grant-in-Aid for Scientific Research.
1. 2-class field; divisibility by 4. Let $2^r$ be the order of the 2-class group of $K$, so that $2^r|h^+(D) (\varepsilon \geq 1)$. Since the 2-class group of $H^+(D)$ is cyclic, we have the following chain of subgroups:

$$H^+(D) \supset H^+(D)^2 \supset \cdots \supset H^+(D)^{2^r}.$$  

Denote by $K_{2^r}$ the class field of $K$ corresponding to the subgroup $H^+(D)^{2^r}$. We have a tower of of class fields:

$$K \subset K_{2^1} \subset \cdots \subset K_{2^r}.$$  

$K_{2^r}$ is unramified at every finite prime in $K$ and $[K_{2^r}: K] = (H^+(D): H^+(D)^{2^r}) = 2^r (1 \leq k \leq l)$.

**Proposition 1.1** (Reichardt [14]). $K_{2^r}$ is normal over $\mathbb{Q}$. The Galois group $G(K_{2^r}/\mathbb{Q})$ is isomorphic to the dihedral group $D_{2^k}$ of order $2^{k+1}$.

In particular $G(K_{2}/K) \cong Z_2 \times Z_2$, where $Z_2$ denotes a cyclic group of order 2. It is well-known and easy to see that

$$K_2 = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = AB,$$

where $A = \mathbb{Q}(\sqrt{d_1})$ and $B = \mathbb{Q}(\sqrt{d_2})$.

We write $a \sim b$ (resp. $a \cong b$), if ideals $a$, $b$ of $K$ are in the same ideal class (resp. in the same narrow ideal class). As $p$ and $q$ are ramified in $K$, we have $(p) = \mathfrak{p}^2$, $(q) = \mathfrak{q}^2$, where $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of $K$. Denote the narrow ideal class containing $\mathfrak{p}$ (resp. $\mathfrak{q}$) by $C^+(\mathfrak{p})$ (resp. $C^+(\mathfrak{q})$). Then $C^+(\mathfrak{p})^2 = C^+(\mathfrak{q})^2 = 1$.

It is also well-known that the elementary 2-subgroup of $H^+(D)$, which is isomorphic to $Z_2$ in the present case, is generated by $C^+(\mathfrak{p})$ and $C^+(\mathfrak{q})$. So one of the three alternatives holds:

(i) $C^+(\mathfrak{p}) = 1$ and $C^+(\mathfrak{q}) \neq 1$,

(ii) $C^+(\mathfrak{p}) \neq 1$ and $C^+(\mathfrak{q}) = 1$,

(iii) $C^+(\mathfrak{p}) = C^+(\mathfrak{q}) = 1$.

In case $D > 0$ and $d_i = -4 \ (i = 1, 2)$ we see easily that the condition (iii) holds if and only if $N_{K_2/\mathbb{Q}} = -1$. By class field theory, we get the following proposition which is a special case of a theorem of Redei and Reichardt [13].

**Proposition 1.2.** The following assertions are equivalent:

(a) $4|h^+(D)$;

(b) both $C^+(\mathfrak{p})$ and $C^+(\mathfrak{q})$ belong to $H^+(D)^2$;

(c) both $\mathfrak{p}$ and $\mathfrak{q}$ split completely in $K_2$;

(d) $p$ and $q$ split completely in $B$ and $A$, respectively;

(e) $\left(\frac{d_1}{q}\right) = \left(\frac{d_2}{p}\right) = 1$. 


As a direct consequence of proposition 1.2 we have $4|h^+(D)$ if and only if $D$ belongs to one of the types (R1), (R2), (I1), (I2), (I3), (I4) in section 0.

2. Construction of $K_4$. In this section we assume $4|h^+(D)$, so that $D$ belongs to one of (R1), ..., (I4) in section 0. The class field $K_4$ is normal over $\mathbb{Q}$ and the Galois group $G(K_4/\mathbb{Q})$ is isomorphic to the dihedral group $D_4$ of order 8. The subfields of $K_4$ are given as follows:

$$
\begin{align*}
A &= \mathbb{Q}(\sqrt{d_1}) \\
B &= \mathbb{Q}(\sqrt{d_2}) \\
A_2 &= A(\sqrt{\alpha}) \\
A_2' &= A(\sqrt{\alpha'}) \\
B_2 &= B(\sqrt{\beta}) \\
B_2' &= B(\sqrt{\beta'})
\end{align*}
$$

where $\alpha \in A$, $\beta \in B$, $\alpha'$ (resp. $\beta'$) is the conjugate of $\alpha$ (resp. $\beta$) over $\mathbb{Q}$, and $\alpha\alpha' \equiv d_2 \pmod{(A')^2}$, $\beta\beta' \equiv d_1 \pmod{(B')^2}$.

From proposition 1.2 it follows that $q$ (resp. $p$) splits completely in $A$ (resp. $B$). Let $(p) = \mathfrak{p}_A^2$, $(q) = q_A q_A'$ (resp. $(q) = q_B^2$, $(p) = \mathfrak{p}_B \mathfrak{p}_B'$) be the prime decompositions in $A$ (resp. $B$) with prime ideals $\mathfrak{p}_A$, $q_A$, $q_A'$ in $A$ (resp. $q_B$, $\mathfrak{p}_B$, $\mathfrak{p}_B'$ in $B$).

Let $Q$ (resp. $Q'$) be a prime divisor of $q_A$ (resp. $q_A'$) in $K_4$. Since the extension $K_4/K$ is unramified at every finite prime the inertia field of $Q$ with respect to $K_4/\mathbb{Q}$ is either $A_2$ or $A_2'$. We may choose $A_2'$ (resp. $A_2$) to be the inertia field of $Q$ (resp. $Q'$). Then we get easily that

$$(2.1) \quad q_A (\text{resp. } q_A') \text{ is the only finite prime in } A \text{ which ramifies in } A_2 (\text{resp. } A_2').$$

In the same way, by a suitable choice of $B_2$ and $B_2'$, we have

$$(2.2) \quad \mathfrak{p}_B (\text{resp. } \mathfrak{p}_B') \text{ is the only finite prime in } B \text{ which ramifies in } B_2 (\text{resp. } B_2').$$

As for the ramification of infinite primes, we can argue in the same way if $D<0$. Indeed when $D<0$ (types (I1), (I2), (I3), and (I4)), the infinite prime $\infty$ of $\mathbb{Q}$ ramifies in $A$, $\infty = \infty_A$, and splits in $B$, $\infty = \infty_B \infty_B'$. By a suitable choice of $\infty_B$ and $\infty_B'$ we see that

$$(2.3) \quad \text{if } D<0, \text{ then both } A_2 \text{ and } A_2' \text{ are unramified at } \infty_A, \text{ and } B_2 (\text{resp. } B_2') \text{ is ramified at } \infty_B (\text{resp. } \infty_B') \text{ and unramified at } \infty_B (\text{resp. } \infty_B).$$

If $D>0$, both $A$ and $B$ are real, so that $\infty$ splits in $A$ and $B$, $\infty = \infty_A \infty_A'$, $\infty = \infty_B \infty_B'$. To go further, we have to take the absolute class number $h(D)$ into account. If $4|h(D)$, then $2|h(D)$ and $N_K e_D = 1$, so that $K_4$ is ramified at
every infinite prime of $K$, which implies that $K_2$ is the inertia field of $\infty$ with respect to $K_2 \mid Q$, for $K_2$ is normal over $Q$. Hence we have

(2.4) if $D > 0$ and $2 \mid h(D)$, then every infinite prime of $A$ (resp. $B$) ramifies in $A_2$ and $A_2'$ (resp. $B_2$ and $B_2'$).

If $D > 0$ and $4 \mid h(D)$ then $K_4$ is unramified at every infinite prime over $Q$. Hence we have

(2.5) if $D > 0$ and $4 \mid h(D)$, then every infinite prime of $A$ (resp. $B$) does not ramify in $A_2$ and $A_2'$ (resp. $B_2$ and $B_2'$).

We denote by $O_F$ the ring of integers of a number field $F$. Let $f_A$ and $\chi_A$ (resp. $f_B$ and $\chi_B$) be the conductor and the Hecke ideal character attached to the quadratic extension $A_2 \mid A$ (resp. $B_2 \mid B$).

Proposition 2.6. Suppose $D$ belongs to type (R1). Then

(a) if $2 \mid h(D)$, we have

$$f_A = q_A \infty_A \infty_A, \quad \chi_A((\lambda)) = \left(\frac{\lambda}{q_A}\right) \text{sgn } N_A \lambda \quad (\lambda \in O_A - q_A);$$

$$f_B = \wp_B \infty_B \infty_B, \quad \chi_B((\mu)) = \left(\frac{\mu}{\wp_B}\right) \text{sgn } N_B \mu \quad (\mu \in O_B - \wp_B);$$

(b) if $4 \mid h(D)$, we have

$$\chi_A((\lambda)) = \left(\frac{\lambda}{q_A}\right) \text{sgn } N_A \lambda \quad (\lambda \in O_A - q_A);$$

$$\chi_B((\mu)) = \left(\frac{\mu}{\wp_B}\right) \text{sgn } N_B \mu \quad (\mu \in O_B - \wp_B);$$

where $\left(\frac{-}{q_A}\right)$ (resp. $\left(\frac{-}{\wp_B}\right)$) denotes the quadratic residue symbol modulo $q_A$ (resp. $\wp_B$).

Proof. If $2 \mid h(D)$ then $N_{F \mathcal{E}_D} = 1$. It follows from (2.1), (2.2), and (2.4) that the quadratic extension $A_2 \mid A$ (resp. $B_2 \mid B$) is ramified at $q_A$, $\infty_A$, $\infty_A'$ (resp. $\wp_B$, $\infty_B$, $\infty_B'$) and unramified outside them. Hence

$$\chi_A((\lambda)) = \left(\frac{\lambda}{q_A}\right) \left(\frac{\lambda, A_2/A}{\infty_A}\right) \left(\frac{\lambda, A_2/A}{\infty_A'}\right) \quad \text{(norm-residue symbol)}$$

$$= \left(\frac{\lambda}{q_A}\right) \left(\frac{\lambda}{\infty_A}\right) \left(\frac{\lambda}{\infty_A'}\right) \quad \text{(Hilbert symbol)}$$

$$= \left(\frac{\lambda}{q_A}\right) \text{sgn } N_A \lambda \quad (\lambda \in O_A - q_A),$$
which implies \( f_A = q_A \infty_A \infty_A^* \). We have \( \chi_B((\mu)) = \left( \frac{\mu}{p_B} \right) \text{sgn } N_B \mu \) and \( f_B = p_B \infty_B \infty_B^* \)

in the same way.

If \( 4 \mid h(D) \), then, from (2.1), (2.2), and (2.5), it follows that \( A_2/A \) (resp. \( B_2/B \)) is ramified only at \( q_A \) (resp. \( p_B \)). Hence the assertion (b) follows in the same way.

Q.E.D.

**Proposition 2.7.** Suppose \( D \) is of type (R2). Then

(a) if \( 2 \mid h(D) \), we have

\[
f_A = q_A \infty_A \infty_A^* , \quad \chi_A((\lambda)) = \left( \frac{\lambda}{q_A} \right) \text{sgn } N_A \lambda \quad (\lambda \in O_A - q_A);
\]

\[
f_B = p_B \infty_B \infty_B^* , \quad \chi_B((\mu)) = \left( \frac{\mu}{p_B} \right) \text{sgn } N_B \mu \quad (\mu \in O_B - p_B);
\]

(b) if \( 4 \mid h(D) \), we have

\[
f_A = q_A , \quad \chi_A((\lambda)) = \left( \frac{\lambda}{q_A} \right) \quad (\lambda \in O_A - q_A);
\]

\[
f_B = p_B , \quad \chi_B((\mu)) = \left( \frac{\mu}{p_B} \right) \quad (\mu \in O_B - p_B);
\]

where \( \left( \frac{\mu, 2}{p_B} \right) = \begin{cases} 1 & \text{if } \mu \equiv 1, 7 \pmod{p_B^3}, \\ -1 & \text{if } \mu \equiv 3, 5 \pmod{p_B^3}. \end{cases} \)

Proof. If \( 2 \mid h(D) \) then \( N_{K_D} = 1 \). It follows from (2.1), (2.2), and (2.4) that the quadratic extension \( A_2/A \) (resp. \( B_2/B \)) is ramified only at \( q_A, \infty_A, \infty_A^* \) (resp. \( p_B, \infty_B, \infty_B^* \)). We have \( \chi_A((\lambda)) = \left( \frac{\lambda}{q_A} \right) \text{sgn } N_A \lambda \) in the same way as in the proof of proposition 2.6, while \( \left( \frac{\mu, \beta}{p_B} \right) = \left( \frac{\mu}{p_B} \right) \left( \frac{\beta}{\infty_B} \right) \), which implies (a). Assertion (b) is proved similarly.

Q.E.D.

We obtain the corresponding results for the other types similarly.

**Proposition 2.8.** Suppose \( D \) is of type (I1), then

\[
f_A = q_A , \quad \chi_A((\lambda)) = \left( \frac{\lambda}{q_A} \right) \quad (\lambda \in O_A - q_A);
\]

\[
f_B = p_B \infty_B , \quad \chi_B((\mu)) = \left( \frac{\mu}{p_B} \right) \left( \frac{\beta}{\infty_B} \right) \quad (\mu \in O_B - p_B).
\]

**Proposition 2.9.** Suppose \( D \) is of type (I2), then

\[
f_A = q_A^3 , \quad \chi_A((\lambda)) = \left( \frac{\lambda, 2}{q_A} \right) \quad (\lambda \in O_A - q_A);
\]
\[ f_B = p_B \infty_B, \quad \chi_B((\mu)) = \left( \frac{\mu}{\infty_B} \right) \quad (\mu \in O_B - p_B). \]

**Proposition 2.10.** Suppose \( D \) is of type (13), then

\[ f_A = q_A, \quad \chi_A((\lambda)) = \left( \frac{\lambda}{q_A} \right) \quad (\lambda \in O_A - q_A); \]

\[ f_B = p_B^3 \infty_B, \quad \chi_B((\mu)) = \left( \frac{\mu, -2}{p_B} \right) \left( \frac{\mu, \beta}{\infty_B} \right) \quad (\mu \in O_B - p_B), \]

where \( \left( \frac{\mu, -2}{p_B} \right) = \begin{cases} 1 & \text{if } \mu \equiv 1, 3 \pmod{p_B^3}, \\ -1 & \text{if } \mu \equiv 5, 7 \pmod{p_B^3}. \end{cases} \)

**Proposition 2.11.** Suppose \( D \) is of type (14), then

\[ f_A = q_A, \quad \chi_A((\lambda)) = \left( \frac{\lambda}{q_A} \right) \quad (\lambda \in O_A - q_A); \]

\[ f_B = p_B^2 \infty_B, \quad \chi_B((\mu)) = \left( \frac{\mu, -1}{p_B} \right) \left( \frac{\mu, \beta}{\infty_B} \right) \quad (\mu \in O_B - p_B), \]

where \( \left( \frac{\mu, -1}{p_B} \right) = \begin{cases} 1 & \text{if } \mu \equiv 1 \pmod{p_B^2}, \\ -1 & \text{if } \mu \equiv -1 \pmod{p_B^2}. \end{cases} \)

In propositions 2.8 to 2.11 the infinite prime \( \infty_B \) is defined by \( \left( \frac{\beta, \beta}{\infty_B} \right) = -1, \) so that \( \left( \frac{\mu, \beta}{\infty_B} \right) \) is the sign of \( \mu \) with respect to \( \infty_B. \)

**Proposition 2.12.** For each \( D, \alpha \) and \( \beta \) can be taken so that they satisfy the following conditions:
(a) \( \alpha \in O_A, \beta \in O_B, (\alpha, \alpha') = 1, (\beta, \beta') = 1; \)
(b)

(R1): \[ \{ \alpha \alpha' = q^{k(\beta)}, \quad \beta \beta' = p^{k(\alpha)}, \]
\[ \alpha^3 \equiv 1 \pmod{4}, \quad \beta^3 \equiv 1 \pmod{4}; \]

(R2): \[ \{ \alpha \alpha' = q, \quad \beta \beta' = 2^{k(\alpha)}, \]
\[ \alpha \equiv 1 \text{ or } 3+2\sqrt{2} \pmod{4}, \quad \beta + \beta' \equiv 2^{k(\alpha)} + 1 \pmod{4}; \]

(I1): \[ \{ \alpha \alpha' = q^{k(-\beta)}, \quad \beta \beta' = -p^{k(\alpha)}, \]
\[ \alpha^3 \equiv 1 \pmod{4}, \quad \beta^3 \equiv 1 \pmod{4}; \]

(I2): \[ \{ \alpha \alpha' = 2^{k(-\beta)}, \quad \beta \beta' = -p, \]
\[ \alpha + \alpha' \equiv 2^{k(-\beta)} + 1 \pmod{4}, \quad \beta \equiv 1 \text{ or } 3+2\sqrt{2} \pmod{4}; \]

(I3): \[ \{ \alpha \equiv 1 \text{ or } 3+2\sqrt{2} \pmod{4}, \quad \beta + \beta' \equiv -2^{k(\alpha)} + 1 \pmod{4}; \]
DIVISIBILITY BY 16 OF CLASS NUMBER

Conversely, for each \( \alpha \) (resp. \( \beta \)) satisfying (a) and (b) the field \( A_2 \) (resp. \( B_2 \)) is the field \( A(\sqrt{\beta}) \) (resp. \( B(\sqrt{\alpha}) \)).

We remark that the condition \( \alpha^3 \equiv 1 \mod 4 \) (resp. \( \beta^3 \equiv 1 \mod 4 \)) is equivalent to \( \alpha \equiv 1 \mod 4 \) (resp. \( \beta \equiv 1 \mod 4 \)) if \( p \equiv 1 \mod 8 \) (resp. \( q \equiv 1 \mod 8 \)).

Proof. Since \( q_A \) is the unique finite prime which is ramified in \( A_2 = A(\sqrt{\alpha}) \) and \( \alpha \alpha' \equiv d_2 \mod (A^*)^2 \), we have \( \alpha = q_A \alpha^2 \) with an ideal \( \alpha \) in \( A \). It is well-known that the class number \( h(d_{\alpha}) \) is odd. Put \( \alpha = q^{\gamma} \). We may replace \( \alpha \) by \( \alpha^{h(d_{\beta})} \gamma^{-1} \), then \( \alpha \equiv O_A \), \( \alpha', = 1 \), and \( \alpha \alpha' = \pm N_A q^{\gamma \alpha'} = \pm q^{\gamma \alpha} \). The sign of the right hand side is determined by the multiplicative congruence \( \alpha \alpha' \equiv d_2 \mod (A^*)^2 \). Let \( \tau_A \) be a prime ideal in \( A \) such that \( \tau_A \parallel (2) \) and \( \tau_A \neq q_A \). The ideal \( \tau_A \) is unramified in \( A_2 \) if and only if there exists an integer \( S \in O_A \) such that \( \alpha = \delta^{\pm 1} \mod \tau_A \), where \( e \) is the index of ramification of \( \tau_A \) with respect to \( A/Q \), that is, \( \tau_A \parallel \ell \). Hence we have

\[
\begin{align*}
\alpha^3 &\equiv 1 \mod 4 \quad \text{if } p \equiv 2 \text{ and } q \equiv 2; \\
\alpha &\equiv \text{a square} \mod 4 \quad \text{if } p \equiv 2 \text{ and } q \equiv 2; \\
\alpha &\equiv 1 \mod q_A^2 \quad \text{if } p \equiv 2 \text{ and } q = 2.
\end{align*}
\]

In the last case \( \alpha \equiv 1 \mod 4 \), it follows from \( \alpha' \equiv 1 \mod (q_A^3) \) that \( \alpha = (\alpha - 1)(\alpha' - 1) = 2^{\gamma \alpha} \alpha - \alpha + 1 \equiv 0 \mod 4 \). We can argue similarly for \( \beta \) except in the case (I4), in which we may proceed as follows. Since \( \beta \beta' \equiv -4 \mod (B^*)^2 \), we have \( \beta \equiv O_B \) and \( \beta \beta' = -1 \), that is, \( \beta \) is a unit by a suitable choice of representative \( \beta \) modulo \( (B^*)^2 \). As \( B(\sqrt{\beta})/B \) is ramified at \( \mathfrak{p}_B \) and unramified at \( \mathfrak{p}_B' \), we have \( \beta \equiv -1 \mod \mathfrak{p}_B^2 \) and \( \beta \equiv 1 \mod \mathfrak{p}_B^5 \). Hence \( \beta - 1 \equiv 0 \mod \mathfrak{p}_B^2 \mathfrak{p}_B^5 \) and \( (\beta - 1)(\beta' - 1) = -\beta - \beta' = 0 \mod 8 \), which implies \( \beta + \beta' = 0 \mod 8 \). Conversely, if we take \( \alpha, \beta \) satisfying conditions (a) and (b) then it is easily seen that \( A(\sqrt{\alpha}, \sqrt{\beta'}) \) (resp. \( B(\sqrt{\beta}, \sqrt{\beta'}) \)) is a Galois extension of \( Q \) with Galois group isomorphic to \( D_4 \) and it is a cyclic extension of \( K \) unramified at every finite prime. Hence it must be \( K_4 \) by class field theory. So we have \( A_2 = A(\sqrt{\alpha}) \) and \( B_2 = B(\sqrt{\beta}) \).

We remark that in case (I4) we may take \( \beta = T + U \sqrt{q} = q \), the fundamental unit of \( B(T, U \in Z, T > 0, U > 0) \), in which case \( T \equiv 0 \mod 4 \) follows as a corollary.

Putting, for each \( D \), respectively:

\[
\alpha = \frac{x + y \sqrt{p}}{2}, \quad \beta = \frac{x - y \sqrt{q}}{2};
\]

Q.E.D.
\[
\alpha = x + y\sqrt{2}, \quad \beta = \frac{z + w\sqrt{q}}{2};
\]

(R2)*: 
\[
\alpha = x + y\sqrt{-p}, \quad \beta = \frac{z + w\sqrt{q}}{2};
\]

(I1)*: 
\[
\alpha = x + y\sqrt{-p}, \quad \beta = z + w\sqrt{2};
\]

(I2)*: 
\[
\alpha = x + y\sqrt{-2}, \quad \beta = \frac{z + w\sqrt{q}}{2};
\]

(I3)*: 
\[
\alpha = x + y\sqrt{-1}, \quad \beta = z + w\sqrt{q};
\]

(x, y, z, w \in \mathbb{Z}), it is easy to see

**Proposition 2.13.** The conditions (a), (b) of proposition 2.12 is equivalent to the following conditions:

(c) \(x, y, z, w \in \mathbb{Z}\) and \(q \not\mid (x, y), p \not\mid (z, w);\)

(d) 
\[
\begin{aligned}
&\left\{ \begin{array}{l}
x^2 - py^2 = 4q^h(p), \\
x + \frac{y\sqrt{p}}{2} \equiv 1 \pmod{4}, \\
\end{array} \right. & \quad & z^2 - qw^2 = 4p^h(q), \\
&\left\{ \begin{array}{l}
x^2 - 2y^2 = q, \\
(x, y) \equiv (1, 0) \text{ or } (3, 2) \pmod{4}, \\
\end{array} \right. & \quad & z^2 - qw^2 = 2^h(q) + 1 \pmod{4};
\end{aligned}
\]

(R2)**: 
\[
\begin{aligned}
&\left\{ \begin{array}{l}
x^2 - 2y^2 = q, \\
(x, y) \equiv (1, 0) \text{ or } (3, 2) \pmod{4}, \\
\end{array} \right. & \quad & z^2 - qw^2 = 2^h(q) + 1 \pmod{4};
\end{aligned}
\]

(R1)**: 
\[
\begin{aligned}
&\left\{ \begin{array}{l}
x^2 - py^2 = 4q^h(p), \\
\frac{x + y\sqrt{p}}{2} \equiv 1 \pmod{4}, \\
\end{array} \right. & \quad & \left(\frac{z + w\sqrt{q}}{2}\right)^3 \equiv 1 \pmod{4};
\end{aligned}
\]

(I2)**: 
\[
\begin{aligned}
&\left\{ \begin{array}{l}
x^2 + py^2 = 4q^h(-p), \\
x \equiv 2^h(-p) + 1 \pmod{4}, \\
\end{array} \right. & \quad & z^2 - 2w^2 = -p,
\end{aligned}
\]

(I3)**: 
\[
\begin{aligned}
&\left\{ \begin{array}{l}
x^2 + 2y^2 = q, \\
(x, y) \equiv (1, 0) \text{ or } (3, 2) \pmod{4}, \\
\end{array} \right. & \quad & z^2 - qw^2 = -2^h(q) + 1 \pmod{4};
\end{aligned}
\]

(I4)**: 
\[
\begin{aligned}
&\left\{ \begin{array}{l}
x^2 + y^2 = q, \\
y \equiv 0 \pmod{4}, \\
\end{array} \right. & \quad & z^2 - qw^2 = -1, \\
&\left\{ \begin{array}{l}
x^2 + y^2 = q, \\
y \equiv 0 \pmod{4}, \\
\end{array} \right. & \quad & z \equiv 0 \pmod{4}.
\end{aligned}
\]

We remark that \(\left(\frac{x + y\sqrt{d}}{2}\right)^3 \equiv 1 \pmod{4}\) if and only if

\[(x, y) \equiv (2, 0) \text{ or } (6, 4) \pmod{8}\]
if \(d \equiv 1 \pmod{8},\)
\[(x, y) \equiv (2, 0), (6, 4), (3, 1), (3, 7), (7, 3), \text{ or } (7, 5) \pmod{8}\]
if \(d \equiv 5 \pmod{16},\)
\[(x, y) \equiv (2, 0), (6, 4), (3, 3), (3, 5), (7, 1), \text{ or } (7, 7) \pmod{8}\]
if \(d \equiv 13 \pmod{16}.\)
3. Divisibility by 8. Assume $4|h^+(D)$, then, in the same way as in section 1, we have the following criterion for the class number $h^+(D)$ to be divisible by 8:

**Proposition 3.1.** The following conditions are equivalent:

(a) $8|h^+(D)$;
(b) both $C^+(p)$ and $C^+(q)$ belong to $H^+(D)^*$;
(c) both $p$ and $q$ split completely in $K$.

Using the notation of section 2, we obtain easily:

**Lemma 3.2.** The following conditions are equivalent:

(a) $C^+(p)\in H^+(D)^*$ (resp. $C^+(q)\in H^+(D)^*$);
(b) $p$ (resp. $q$) splits completely in $K|K$;
(c) $p_A$ (resp. $q_A$) splits completely in $A_A|A$ (resp. $B_B|B$);
(d) $p_B$ (resp. $q_B$) splits completely in $B_B|B$ (resp. $A_A|A$);
(e) $\chi_A(p_A)=1$ (resp. $\chi_B(q_B)=1$);
(f) $\chi_B(p_B)=1$ (resp. $\chi_A(q_A)=1$).

**Proposition 3.3** (cf. [12] [3] [9]). Suppose $D$ is of type (R1). Then we have

(a) $2|h(d)$ if and only if $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=-1$;

if $\left(\frac{2}{q}\right)_4=-1$ and $\left(\frac{q}{2}\right)_4=1$ then $p=1$ and $q=1$;

if $\left(\frac{2}{q}\right)_4=1$ and $\left(\frac{q}{2}\right)_4=-1$ then $p=1$ and $q=1$;

(b) $4|h(d)$ and $N_{K^D}=-1$ if and only if $\left(\frac{p}{q}\right)_4=\left(\frac{q}{p}\right)_4=-1$;

(c) $8|h^+(D)$ if and only if $\left(\frac{p}{q}\right)_4=\left(\frac{q}{p}\right)_4=1$;

(d) $\left(\frac{p}{q}\right)_4=(-1)^{(d/2)}\left(\frac{x}{p}\right)_4$ and $\left(\frac{q}{p}\right)_4=(-1)^{(d/2)}\left(\frac{x}{q}\right)_4$,

where $x, z$ are rational integers satisfying the conditions (c), (d) (R1)** of proposition 2.13.

Proof. Assume $2|h(d)$. Since $N_{K^D}=1$ we have $p=1$ and $q=1$ or $p=1$ and $q=1$ alternatively. In the first case we have $C^+(p)\in H^+(D)^*$ and $C^+(q)\in H^+(D)^*$, hence, by proposition 2.6 (a) and lemma 3.2,

$$1 = \chi_A(p_A) = \chi_A((\sqrt{p})) = \left(\frac{\sqrt{p}}{q_A}\right) \text{sgn} N_A \sqrt{p} = -\left(\frac{p}{q}\right)_4,$$
\[-1 = \chi_B(q_B) = \chi_B(\sqrt{q}) = \left(\frac{\sqrt{q}}{\nu_B}\right) \text{sgn} N_B \sqrt{q} = -\left(\frac{q}{p}\right)_4.\]

In the same way we have \(\left(\frac{p}{q}\right)_4 = 1\) and \(\left(\frac{q}{p}\right)_4 = -1\) for the latter case.

Next, assume \(4|\varepsilon(D)\), then, by proposition 2.6 (b), we have \(\chi_A(p_A) = -\left(\frac{p}{q}\right)_4\) and \(\chi_B(q_B) = \left(\frac{\sqrt{q}}{\nu_B}\right) = \left(\frac{q}{p}\right)_4\). If \(8|h^+(D)\) then \(4|h(D)\) and \(N_K \varepsilon_B = -1\), hence \(p \approx q \mp 1\) and we see, by proposition 3.1 and lemma 3.2, \(C^+(b) = C^+(q) \in H^+(D)^4\) and \(\chi_A(p_A) = \chi_B(q_B) = -1\). If \(8|h^+(D)\), then we get \(\chi_A(p_A) = \chi_B(q_B) = 1\) in the same way. To sum up, we get the assertions (a), (b), (c), and that

\[\chi_A(p_A) = (-1)^{\varepsilon(D)q} \left(\frac{p}{q}\right)_4\] and \(\chi_B(q_B) = (-1)^{\varepsilon(D)q} \left(\frac{q}{p}\right)_4\).

On the other hand, since \(h(d_1)\) and \(h(d_2)\) are odd,

\[\chi_A(p_A) = \chi_B(p_B) \quad \text{(lemma 3.2)}\]
\[= \chi_B(p_B)^{h(d_2)} = \chi_B((\beta')) \quad \text{(proposition 2.6, proposition 2.12)}\]
\[= \left(\frac{\beta + \beta'}{\nu_B}\right) = \left(\frac{x}{p}\right) \quad \text{(by (R1)^*)}\]

and similarly \(\chi_B(q_B) = \left(\frac{x}{q}\right)\), which imply the assertion (d).

Q.E.D.

**Proposition 3.4 (cf. [12] [3] [9]).** Suppose \(D\) is of type (R2). Then we have

(a) \(2|h(D)\) if and only if \(\left(\frac{2}{q}\right)_4 = \left(\frac{q}{2}\right)_4 = -1\);

if \(\left(\frac{p}{q}\right)_4 = -1\) and \(\left(\frac{q}{p}\right)_4 = 1\) then \(p \approx 1\) and \(q \mp 1\);

if \(\left(\frac{p}{q}\right)_4 = 1\) and \(\left(\frac{q}{p}\right)_4 = -1\) then \(p \approx 1\) and \(q \approx 1\);

(b) \(4|h(D)\) and \(N_K \varepsilon_B = -1\) if and only if \(\left(\frac{2}{q}\right)_4 = \left(\frac{q}{2}\right)_4 = -1\);

(c) \(8|h^+(D)\) if and only if \(\left(\frac{2}{q}\right)_4 = \left(\frac{q}{2}\right)_4 = 1\);

(d) \(\left(\frac{2}{q}\right)_4 = \left(\frac{x - 2^{\varepsilon(d)}}{2}\right)\) and \(\left(\frac{q}{2}\right)_4 = \left(\frac{x}{q}\right)\),
where x, z are rational integers satisfying the conditions (c), (d) (R2)** of proposition 2.13 and

\[
\left( \frac{a}{2} \right)_4 = 1 \text{ if } a \equiv 1 \pmod{8}, \quad \left( \frac{a}{2} \right)_4 = -1 \text{ if } a \equiv 5 \pmod{8};
\]

\[
\left( \frac{a}{2} \right)_4 = 1 \text{ if } a \equiv 1 \pmod{16}, \quad \left( \frac{a}{2} \right)_4 = -1 \text{ if } a \equiv 9 \pmod{16}.
\]

Proof. Using the following:

\[
\left( \frac{\sqrt{q}}{p_B} \right) = \left( \frac{q}{2} \right)_4,
\]

\[
\left( \frac{\beta', 2}{p_B} \right) = \left( \frac{z - 2^{k(\alpha)}}{2} \right),
\]

we can argue in the same way as in the proof of proposition 3.3. The first equality of (3.5) is checked straightforwardly. Since \( \beta' \equiv 1 \pmod{p_B} \), we see \( \left( \frac{\beta', 2}{p_B} \right) = 1 \) if and only if \( \beta' \equiv 1 \pmod{p_B} \), that is, if and only if \( (\beta - 1)(\beta' - 1) \equiv 0 \pmod{p_B} \), for \( \beta \equiv 1 \pmod{p_B} \); on the other hand \( (\beta - 1)(\beta' - 1) = \beta \beta' - \beta - \beta' + 1 = 2^{k(\alpha)} - z + 1 \); so we get the latter equality of (3.5). Q.E.D.

**Proposition 3.5** (cf. [12] [9]). Suppose \( D \) is of type (II), then

\[
\left( \frac{-p}{q} \right)_4 = \left( \frac{x}{q} \right)_4 = \left( \frac{z}{p} \right)_4 = (-1)^{k(D)/4} \text{ and } \left( \frac{w}{p} \right)_4 = \text{sgn } w,
\]

where x, z, w are rational integers satisfying the conditions (c), (d) (II)** of proposition 2.13.

Proof. Since \( p q = (\sqrt{-pq}) \approx 1 \), we have \( p \approx q \pm 1 \). It follows from proposition 3.1 and lemma 3.2 that

\[
\chi_A(p_B) = \chi_B(q_B) = \chi_B(q_B) = (-1)^{k(D)/4}.
\]

By proposition 2.8 we have

\[
\chi_A(p_B) = \left( \frac{\sqrt{-p}}{q_A} \right)_4 = \left( \frac{-p}{q} \right)_4,
\]

\[
\chi_A(q_A) = \chi_A(q_A)^{(-p)} = \chi_A((\alpha')) = \left( \frac{\alpha'}{q_A} \right)_4 = \left( \frac{\alpha + \alpha'}{q_A} \right)_4 = \left( \frac{x}{q} \right)_4,
\]

\[
\chi_B(p_B) = \chi_B(p_B)^{k(\alpha')} = \chi_B((\beta')) = \left( \frac{\beta'}{p_B} \right)_4 = \left( \frac{z}{p} \right)_4,
\]

\[
\chi_B(q_B) = \chi_B((\sqrt{q})) = \left( \frac{\sqrt{q}}{p_B} \right)_4.
\]

It follows from \( \chi_B = -1 \) that \( \left( \frac{\sqrt{q}}{p_B} \right)_4 = \text{sgn } w \). Since \( \beta = \frac{z + w \sqrt{q}}{2} \),
$\equiv 0 \pmod{p_b}$, we have $\sqrt{q} \equiv -\frac{x}{w} \pmod{p_b}$, so that $\chi_B(q_b) = \left(\frac{-\frac{x}{w}}{p}\right)(-\text{sgn } w)$

$= \left(\frac{zw}{p}\right) \text{sgn } w$, which implies $\left(\frac{w}{p}\right) = \text{sgn } w.$ Q.E.D.

**Proposition 3.6** (cf. [9]). Suppose $D$ is of type (I2), then

$$\left(\frac{-p}{2}\right) = \left(\frac{x-2^{k(-p)}}{2}\right) = \left(\frac{x}{p}\right) = (-1)^{k(d)/4} \text{ and } \left(\frac{w}{p}\right) = \text{sgn } w,$$

where $x, z, w$ are rational integers satisfying the conditions (c), (d) (I2)** of proposition 2.13.

Proof. Since $pq = (\sqrt{-2p}) \approx 1$, we see that $p \equiv q \equiv 1$. By proposition 3.1 and lemma 3.2 we have $\chi_A(p_A) = \chi_B(q_b) = \chi_A(q_A') = \chi_B(p_B') = (-1)^{k(d)/4}$. By proposition 2.9 we have

$$\chi_A(p_A) = \chi_A(\sqrt{-p}) = \left(\frac{\sqrt{-p}, 2}{q_A}\right) = \left(\frac{-p}{2}\right),$$

$$\chi_A(q_A') = \chi_A(\sqrt{2}) = \left(\frac{x-2^{k(-p)}}{2}\right),$$

$$\chi_B(p_B') = \chi_B(-\beta') = \left(\frac{\beta'}{p_B}\right)(\frac{\beta'}{\infty_B}) = \left(\frac{x}{p}\right),$$

$$\chi_B(q_b) = \chi_B(\sqrt{2}) = \left(\frac{\sqrt{2}}{\infty_B}\right) = \left(\frac{zw}{p}\right) \text{sgn } w,$$

in the same way as in the proof of proposition 3.3, proposition 3.4, and proposition 3.5. Q.E.D.

**Proposition 3.7** (cf. [9]). Suppose $D$ is of type (I3), then

$$\left(\frac{-2}{q}\right) = \left(\frac{x}{q}\right) = \left(\frac{x+2^{k(t)}}{2}\right) = \left(\frac{x}{2}\right) = (-1)^{k(d)/4},$$

where $x, z, w$ are rational integers satisfying the conditions (c), (d) (I3)** with $z + w \equiv 0 \pmod{4}.$

Proof. Since $pq = (\sqrt{-2q}) \approx 1$, we have $p \equiv q \equiv 1$. By proposition 3.1 and lemma 3.2 we have

$$\chi_A(p_A) = \chi_B(q_b) = \chi_A(q_A') = \chi_B(p_B') = (-1)^{k(d)/4}.$$ By proposition 2.10, we have

$$\chi_A(p_A) = \chi_A(\sqrt{-2}) = \left(\frac{\sqrt{-2}}{q_A}\right) = \left(\frac{-2}{q}\right),$$
We may safely assume $\sqrt{q} \equiv 1 \pmod{p}$, by transposing $p_B$ and $p_B'$ if necessary, obtaining $\left(\frac{\sqrt{q}, -2}{p_B}\right) = \left(\frac{q}{2}\right)_4$ and $2\beta \equiv z + w\sqrt{q} \equiv z + w \pmod{p_B}$. Hence we have $z + w \equiv 0 \pmod{4}$, which determines the sign of $w$. It follows from $\beta < 0$ and $\beta' > 0$ with respect to $\infty_B$ that $w\sqrt{q} < 0$ with respect to $\infty_B$, which implies $\left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = -\text{sgn } w$.

Q.E.D.

**Proposition 3.8** (cf. [11] [4] [10]). Suppose $D$ is of type (I4), then

$$\left(\frac{2}{q}\right)\left(\frac{q}{2}\right)_4 = (-1)^{x/4} = (-1)^{k_2/4},$$

$$\left(\frac{x}{q}\right) = 1, \text{ and } w \equiv 1 \pmod{4},$$

where $x, z, w$ are rational integers satisfying the conditions (c), (d) (I4)** of proposition 2.13.

Proof. Since $q = (\sqrt{-q}) \equiv 1$, we get $p \equiv 1$, so that, by proposition 3.1 and lemma 3.2, we have $\chi_A(p_A) = \chi_B(p_B') = (-1)^{k_2/4}$ and $\chi_A(q_A) = \chi_B(q_B) = 1$. By proposition 2.11, we have

$$\chi_A(p_A) = \chi_A(1 + \sqrt{-1}) = \left(\frac{1 + \sqrt{-1}}{q_A}\right) = \left(\frac{2\sqrt{-1}}{q_A}\right)_4.$$

Since $B_2 = B(\sqrt{\beta})$ and $\beta \equiv 1 \pmod{p_B}$, we have $\chi_B(p_B') = 1$ if and only if $\beta \equiv 1 \pmod{p_B}$. As $p_B||(\beta - 1)$, we have $\beta \equiv 1 \pmod{p_B}$ if and only if $(\beta - 1)(\beta' - 1) = -2z \equiv 0 \pmod{16}$. On the other hand,

$$\chi_A(q_A) = \chi_A((\alpha')) = \left(\frac{\alpha'}{q_A}\right) = \left(\frac{x}{q}\right) = 1,$$

$$\chi_B(q_B) = \chi_B((\sqrt{q})) = \left(\frac{\sqrt{q}, -1}{p_B}\right)\left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = \left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = 1.$$

Since $\sqrt{q} \equiv \pm 1 \pmod{p_B}$, we have $\left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = \pm 1$, which implies $w \equiv 0$,
while \( \beta' = z - w\sqrt{q} \equiv \mp w \equiv 1 \pmod{\wp_2^2} \). Hence \(|w| \equiv 1 \pmod{4}\). Q.E.D.

4. Construction of \( K_8 \). We assume \( 8|h^+(D) \) throughout the rest of this paper. By proposition 1.2, \( K_8 \) is a dihedral extension of \( \mathbb{Q} \) and both \( G(\mathbb{K}/A_2) \) and \( G(\mathbb{K}/B_2) \) are isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). The intermediate fields of \( \mathbb{K}/A_2 \) and \( \mathbb{K}/B_2 \) are given in the following diagram:

![Diagram](image)

where \( \alpha_2' \) (resp. \( \beta_2' \)) denotes the conjugate of \( \alpha_2 \) over \( A \) (resp. \( \beta_2 \) over \( B \)). By proposition 3.1, both \( \wp_A \) and \( q_A' \) (resp. both \( \wp_B \) and \( q_B' \)) split completely in \( A_2 \) (resp. in \( B_2 \)) and \( q_A \) (resp. \( \wp_B \)) ramifies in \( A_2 \) (resp. in \( B_2 \)). We put

\[
\begin{align*}
\wp_A &= P_A P_A', & q_A &= Q_A Q_A', \\
\wp_B &= \hat{P}_B, & q_B &= \hat{Q}_B Q_B' ,
\end{align*}
\]

with prime ideals \( P_A, P_A', \hat{Q}_A, Q_A, Q_A' \) in \( A_2 \) (resp. \( \hat{P}_B, P_B, P_B', Q_B, Q_B' \) in \( B_2 \)).

Since \( \mathbb{K}/K \) is unramified at every finite prime, \( Q_A \) (resp. \( P_B \)) ramifies in either \( A_4 \) or \( A_4' \) (resp. \( B_4 \) or \( B_4' \)). By a suitable choice, we may suppose that:

\[
\begin{align*}
(4.1) \quad Q_A \text{ (resp. } P_B) \text{ is the only finite prime of } A_2 \text{ (resp. } B_2) \text{, which is ramified in } A_4 \text{ (resp. } B_4). \\
(4.2) \quad \text{If } D < 0, \text{ then there is no (resp. only one (denoted by } V_B) \text{ infinite prime in } A_2 \text{ (resp. } B_2) \text{ which is ramified in } A_4 \text{ (resp. } B_4). \\
(4.3) \quad \text{If } D > 0, 4|h(D), \text{ and } N_{E_2} \equiv 1, \text{ then every infinite prime in } A_2 \text{ (resp. } B_2) \text{ is ramified in } A_4 \text{ (resp. } B_4). \\
(4.4) \quad \text{If } D > 0 \text{ and } 8|h(D), \text{ then every infinite prime in } A_2 \text{ (resp. } B_2) \text{ is unramified in } A_4 \text{ (resp. } B_4). 
\end{align*}
\]
DIVISIBILITY BY 16 OF CLASS NUMBER

Let $\psi_A$ (resp. $\psi_B$) be the Hecke character of $A_2$ (resp. $B_2$) which is attached to the quadratic extension $A_4/A_2$ (resp. $B_4/B_2$). By (4.1), (4.2), (4.3), and (4.4) we determine $\psi_A$ and $\psi_B$ as follows:

**Proposition 4.5.** Suppose $D$ is of type (R1) and $8| h^+(D)$. Then

(a) if $4|h(D)$, we have

$$
\psi_A(\lambda) = \left(\frac{\lambda}{Q_A}\right) \text{sgn } N_{A_2} \lambda \quad (\lambda \in O_{A_2} - Q_A);
$$

$$
\psi_B(\mu) = \left(\frac{\mu}{P_B}\right) \text{sgn } N_{B_2} \mu \quad (\mu \in O_{B_2} - P_B);
$$

(b) if $8|h(D)$, we have

$$
\psi_A(\lambda) = \left(\frac{\lambda}{Q_A}\right) \quad (\lambda \in O_{A_2} - Q_A);
$$

$$
\psi_B(\mu) = \left(\frac{\mu}{P_B}\right) \quad (\mu \in O_{B_2} - P_B).
$$

**Proof.** (a) By (4.3) the primes of $A_2$ which ramify in $A_4$ consist of $Q_A$ and all of the four infinite primes, so that

$$
\psi_A(\lambda) = \left(\frac{\lambda, A_4/A_2}{Q_A}\right) \prod_{\eta \in \omega} \left(\frac{\lambda, A_4/A_2}{v}\right).
$$

We have

$$
\left(\frac{\lambda, A_4/A_2}{Q_A}\right) = \left(\frac{\lambda, \alpha_2}{Q_A}\right) = \left(\frac{\lambda}{Q_A}\right)^{\text{ord}(\alpha_2)} = \left(\frac{\lambda}{Q_A}\right),
$$

where $\text{ord}(\alpha_2)$ is the order of $\alpha_2$ with respect to $Q_A$, and

$$
\prod_{\eta \in \omega} \left(\frac{\lambda, A_4/A_2}{v}\right) = \prod_{\eta \in \omega} \text{sgn } \lambda' = N_{A_2} \lambda.
$$

This complete the proof of the first part of (a). The second part is obtained in the same way.

(b) The only prime of $A_2$ which ramifies in $A_4$ in this case is $Q_A$. Hence we have $\psi_A(\lambda) = \left(\frac{\lambda, A_4/A_2}{Q_A}\right) = \left(\frac{\lambda}{Q_A}\right)$. We can calculate $\psi_B(\mu)$ similarly.

Q.E.D.

**Proposition 4.6.** Suppose $D$ is of type (R2) and $8| h^+(D)$. Then

(a) if $4|h(D)$, we have

$$
\psi_A(\lambda) = \left(\frac{\lambda}{Q_A}\right) \text{sgn } N_{A_2} \lambda \quad (\lambda \in O_{A_2} - Q_A);
$$

(b) if $8|h(D)$, we have

$$
\psi_A(\lambda) = \left(\frac{\lambda}{Q_A}\right) \quad (\lambda \in O_{A_2} - Q_A);
$$

$$
\psi_B(\mu) = \left(\frac{\mu}{P_B}\right) \quad (\mu \in O_{B_2} - P_B).
$$
\[ \psi_B((\mu)) = \left( \frac{\mu, 2}{P_B} \right) \text{sgn } N_{b_2}\mu \quad (\mu \in \mathcal{O}_{b_2} - P_B); \]

(b) if \( 8 \mid h(D) \), we have

\[ \psi_A((\lambda)) = \left( \frac{\lambda}{Q_A} \right) \quad (\lambda \in \mathcal{O}_{a_2} - Q_A); \]

\[ \psi_B((\mu)) = \left( \frac{\mu, 2}{P_B} \right) \quad (\mu \in \mathcal{O}_{b_2} - P_B). \]

Proof. Since \( B'_4 = B_4(\sqrt{B_2''}) \) is unramified at \( P_B \),

\[ \left( \frac{\mu, B_4}{P_B} \right) = \left( \frac{\mu, B_2}{P_B} \right) = \left( \frac{\mu, \beta}{P_B} \right) = \left( \frac{\mu, \beta'}{P_B} \right). \]

The rest of the proof is the same as that of proposition 4.5.

Q.E.D.

In the same way we have:

**Proposition 4.7.** Suppose \( D \) is of type (I1) and \( 8 \mid h(D) \), then

\[ \psi_A((\lambda)) = \left( \frac{\lambda}{Q_A} \right) \quad (\lambda \in \mathcal{O}_{a_2} - Q_A); \]

\[ \psi_B((\mu)) = \left( \frac{\mu, 2}{P_B} \right) \left( \frac{\mu, \beta}{V_B} \right) \quad (\mu \in \mathcal{O}_{b_2} - P_B). \]

**Proposition 4.8.** Suppose \( D \) is of type (I2) and \( 8 \mid h(D) \), then

\[ \psi_A((\lambda)) = \left( \frac{\lambda, 2}{Q_A} \right) \quad (\lambda \in \mathcal{O}_{a_2} - Q_A); \]

\[ \psi_B((\mu)) = \left( \frac{\mu, 2}{P_B} \right) \left( \frac{\mu, \beta}{V_B} \right) \quad (\mu \in \mathcal{O}_{b_2} - P_B). \]

**Proposition 4.9.** Suppose \( D \) is of type (I3) and \( 8 \mid h(D) \), then

\[ \psi_A((\lambda)) = \left( \frac{\lambda}{Q_A} \right) \quad (\lambda \in \mathcal{O}_{a_2} - Q_A); \]

\[ \psi_B((\mu)) = \left( \frac{\mu, -2}{P_B} \right) \left( \frac{\mu, \beta}{V_B} \right) \quad (\mu \in \mathcal{O}_{b_2} - P_B). \]

**Proposition 4.10.** Suppose \( D \) is of type (I4) and \( 8 \mid h(D) \), then

\[ \psi_A((\lambda)) = \left( \frac{\lambda}{Q_A} \right) \quad (\lambda \in \mathcal{O}_{a_2} - Q_A); \]
5. Divisibility by 16. We assume $8|h^+(D)$ in this section and obtain a criterion for $h^+(D)$ to be divisible by 16 in the same way as in section 3:

**Proposition 5.1.** The following conditions are equivalent:

(a) $16|h^+(D)$;

(b) both $C^+(p)$ and $C^+(q)$ belong to $H^+(D)^g$;

(c) both $p$ and $q$ split completely in $K_s$.

Using the notation of previous sections, we obtain easily:

**Lemma 5.2.** The following conditions are equivalent:

(a) $C^+(p)\in H^+(D)^g$ (resp. $C^+(q)\in H^+(D)^g$);

(b) $p$ (resp. $q$) splits completely in $K_s$;

(c) $P_B$ (resp. $Q_A$) splits completely in $B$ (resp. $A$);

(d) $\psi_B(\hat{P}_B)=1$ (resp. $\psi_A(\hat{Q}_A)=1$).

If $d_1 = -4$, we can set

$$\alpha = \tilde{q}_A^{-h(d_1)} = \tilde{Q}_A^{2h(d_1)}$$

and

$$\beta = \tilde{p}_B^{-h(d_2)} = \tilde{P}_B^{2h(d_2)}.$$

Hence we have:

**Lemma 5.3.** If $d_1 = -4$, then

$$\tilde{Q}_A^{h(d_1)} = (\sqrt{\alpha}) \quad \text{and} \quad \tilde{P}_B^{h(d_2)} = (\sqrt{\beta}).$$

**Theorem 5.4.** Suppose $D$ is of type (R1) and $8|h^+(D)$. Then we have

(a) $4|h(D)$ if and only if $\left(\frac{x}{p}\right)_4 \left(\frac{x}{q}\right)_4 = -1$;

(b) $8|h(D)$ and $N_{K}\varepsilon_D = -1$ if and only if $\left(\frac{x}{p}\right)_4 = \left(\frac{x}{q}\right)_4 = -1$;

(c) $16|h^+(D)$ if and only if $\left(\frac{x}{p}\right)_4 = \left(\frac{x}{q}\right)_4 = 1$;

where $x, z$ are rational integers satisfying the conditions (c), (d) (R1)** of proposition 2.13.

**Proof.** Assume first that $4|h(D)$. Then, by proposition 4.5 and lemma 5.3, we have
\[ \psi_B(\hat{P}_B) = \psi_B((\sqrt{\beta})) = \left( \frac{\sqrt{\beta}}{P_B} \right)_4 \text{ sgn } N_{B_2} \sqrt{\beta}, \]
\[ \left( \frac{\sqrt{\beta}}{P_B} \right)_4 = \left( \frac{\beta}{P_B} \right)_4 = \left( \frac{\beta + \beta'}{P_B} \right)_4 = \left( \frac{x}{p} \right)_4, \]
\[ N_{B_2} \sqrt{\beta} = N_B (\beta \beta') = P^{h(q)} > 0. \]

Hence \( \psi_B(\hat{P}_B) = \left( \frac{x}{p} \right)_4 \). We obtain \( \psi_A(\hat{Q}_A) = \left( \frac{x}{q} \right)_4 \) similarly. On the other hand, as \( N_K \epsilon_D = 1 \), we have either \( p \equiv 1 \) and \( q \equiv 1 \) or \( p \equiv 1 \) and \( q \equiv 1 \). By lemma 5.2, we have \( \psi_B(\hat{P}_B) = 1 \) and \( \psi_A(\hat{Q}_A) = -1 \) in the first case and \( \psi_B(\hat{P}_B) = -1 \) and \( \psi_A(\hat{Q}_A) = 1 \) in the latter case.

Next, we assume that \( 8 \| h(D) \). By proposition 4.5 (b), we have
\[ \psi_B(\hat{P}_B) = \psi_B((\sqrt{\beta})) = \left( \frac{\sqrt{\beta}}{P_B} \right)_4 = \left( \frac{x}{p} \right)_4, \]
\[ \psi_A(\hat{Q}_A) = \psi_A((\sqrt{\alpha})) = \left( \frac{\alpha}{Q_A} \right)_4 = \left( \frac{x}{q} \right)_4. \]

If \( 8 \| h(D) \) and \( N_K \epsilon_D = -1 \), we have \( p \equiv q \equiv 1 \), hence \( \psi_B(\hat{P}_B) = \psi_A(\hat{Q}_A) = -1 \) by lemma 5.2. If \( 16 \| h^*(D) \), then, by proposition 5.1 and lemma 5.2, we have \( \psi_B(\hat{P}_B) = \psi_A(\hat{Q}_A) = 1 \).

**Theorem 5.5.** Suppose \( D \) is of type \((R2)\) and \( 8 \| h^*(D) \). Then we have

(a) \( 4 \| h(D) \) if and only if \( \left( \frac{x-2^{h(q)}}{2} \right)_4 = -1 \);
\[ \left( \frac{x-2^{h(q)}}{2} \right)_4 = 1 \text{ and } \left( \frac{x}{q} \right)_4 = -1 \text{ if and only if } p \equiv 1 \text{ and } q \equiv 1; \]
\[ \left( \frac{x-2^{h(q)}}{2} \right)_4 = -1 \text{ and } \left( \frac{x}{q} \right)_4 = 1 \text{ if and only if } p \equiv 1 \text{ and } q \equiv 1; \]

(b) \( 8 \| h(D) \) and \( N_K \epsilon_D = -1 \) if and only if \( \left( \frac{x-2^{h(q)}}{2} \right)_4 = \left( \frac{x}{q} \right)_4 = -1 \);

(c) \( 16 \| h^*(D) \) if and only if \( \left( \frac{x-2^{h(q)}}{2} \right)_4 = \left( \frac{x}{q} \right)_4 = 1 \);

where \( x, z \) are rational integers satisfying the conditions (c), (d) \((R2)** of proposition 2.13.

**Proof.** If \( 4 \| h(D) \), then, by proposition 4.6 (a), we have
\[ \psi_B(\hat{P}_B) = \psi_B((\sqrt{\beta})) = \left( \frac{\sqrt{\beta}}{P_B} \right)_4 \text{ sgn } N_{B_2} \sqrt{\beta} \]
\[ = \left( \frac{\sqrt{\beta}}{P_B} \right)_4 = \left( \frac{\beta}{P_B} \right)_4, \]
where \( \left( \frac{\beta}{p_b} \right)_4 = 1 \) if \( \beta \equiv 1 \) (mod \( p_b^4 \)) and \( \left( \frac{\beta}{p_b} \right)_4 = -1 \) if \( \beta \equiv 9 \) (mod \( p_b^4 \)). Since \( \beta \equiv 1 \) (mod \( p_b^4 \)) and \( \beta' \equiv 1 \) (mod \( p_b^4 \)), we see that \( \beta \equiv 1 \) (mod \( p_b^4 \)) if and only if \( (\beta - 1)(\beta' - 1) = 2^k(h) - s + 1 \equiv 0 \) (mod 16), so that \( \psi_p(\tilde{p}_b) = \left( \frac{x - 2^k(h)}{2} \right)_4 \). The rest of the proof can be done in the same way as in theorem 5.4. Q.E.D.

**Theorem 5.6.** Suppose \( D \) is of type (11) and \( 8 \mid h(D) \), then

\[
\frac{x}{q} = (-1)^{h(D)/8},
\]

where \( x \) is a rational integer satisfying the conditions (c), (d) (11)** of proposition 2.13.

**Proof.** Since \( p \equiv q \equiv 1 \), it follows from proposition 5.1 and lemma 5.2 that \( \psi_p(\tilde{p}_b) = \psi_p(\tilde{q}_A) = (-1)^{h(D)/8} \). By proposition 4.7 and lemma 5.3, \( \psi_A(\tilde{q}_A) = \psi_A((\sqrt{\alpha})) = \left( \frac{\sqrt{\alpha}}{q_A} \right)_4 = \left( \frac{x}{q} \right)_4 \). Q.E.D.

**Theorem 5.7.** Suppose \( D \) is of type (12) and \( 8 \mid h(D) \), then

\[
\frac{x - 2^k(h - p)}{2} = (-1)^{h(D)/8},
\]

where \( x \) is a rational integer satisfying the conditions (c), (d) (12)** of proposition 2.13.

**Proof.** Since \( p \equiv q \equiv 1 \), it follows from proposition 5.1 and lemma 5.2 that \( \psi_p(\tilde{p}_b) = \psi_p(\tilde{q}_A) = (-1)^{h(D)/8} \). By proposition 4.8 and lemma 5.3, we have \( \psi_A(\tilde{q}_A) = \psi_A((\sqrt{\alpha})) = \frac{\sqrt{\alpha}}{Q_A} \), and we deduce that \( \left( \frac{\sqrt{\alpha}}{Q_A} \right)_4 = \left( \frac{x - 2^k(h - p)}{2} \right)_4 \) as in the proof of theorem 5.5. Q.E.D.

**Theorem 5.8.** Suppose \( D \) is of type (13) and \( 8 \mid h(D) \), then

\[
\left( \frac{2x}{q} \right)_4 = (-1)^{h(D)/8},
\]

where \( x \) is a rational integer satisfying the conditions (c), (d) (13)** of proposition 2.13.

**Proof.** Since \( p \equiv q \equiv 1 \), we have \( \psi_p(\tilde{p}_b) = \psi_p(\tilde{q}_A) = (-1)^{h(D)/8} \). By proposition 4.9, we have \( \psi_A(\tilde{q}_A) = \psi_A((\sqrt{\alpha})) = \frac{\sqrt{\alpha}}{Q_A} = \left( \frac{2x}{q} \right)_4 \). Q.E.D.

For discriminants of type (14), the above argument does not work well.
An alternative method is therefore given in the next section.

6. D of type (I4). We assume that D is of type (I4) and 8|h(D) in this section. It is easy to see that

\[ K_4 = K_2(\sqrt{e_s}) = \mathbb{Q}(\sqrt{-1}, \sqrt{e_s}), \]

where \( e_s = T + U\sqrt{-q} > 1 \) is the fundamental unit of B. The field \( K_s \) has been explicitly constructed by H. Cohn and G. Cooke [4] (cf. also [10]):

**Lemma 6.1 (Cohn-Cooke).**

\[ K_s = K_4(\sqrt{(f+\sqrt{-q})(1+\sqrt{-1})\sqrt{e_s}}), \]

where \( e \) and \( f \) are rational integral solutions of

\[ -q = f^2 - 2e^2; e > 0, f \equiv -1 \pmod{4}. \]

We let \( \lambda = (f+\sqrt{-q})(1+\sqrt{-1})\sqrt{e_s} \), so that \( K_s = K_4(\sqrt{\lambda}) \). As \( P_B \) is ramified in \( K_4 \), we have \( P_B = \mathfrak{P}^2 \) where \( \mathfrak{P} \) is a prime ideal of \( K_4 \). It is easy to see that the completion of \( K_4 \) at \( \mathfrak{P} \) is isomorphic to \( \mathbb{Q}_2(\sqrt{-1}) \) and we may fix the isomorphism by taking

\[ \sqrt{q} \equiv \frac{q+1}{2} \pmod{p_B^2} \quad \text{and} \quad \sqrt{e_s} \equiv \frac{e_s+1}{2} \pmod{P_B^3}. \]

We remark that \( \mathfrak{P}^2 | P_B | p_B^3(2) \). Denote by \( O_{\mathfrak{P}} \) the ring of \( \mathfrak{P} \)-adic integers, then \( \pi = 1 - \sqrt{-1} \) is a prime element of \( O_{\mathfrak{P}} \) and its maximal ideal is \( \pi O_{\mathfrak{P}} \), which is also denoted by \( \mathfrak{P} \). Since the ramification index of \( \mathfrak{P} \) is 2, we obtain easily:

**Lemma 6.4.** Let the \( \mathfrak{P} \)-adic units be denoted by \( O_{\mathfrak{P}}^\times \). Then

\[ \mu \in O_{\mathfrak{P}}^\times \text{ if and only if } \mu \equiv \pm 1 \pmod{\mathfrak{P}^3}. \]

As \( \lambda/\pi^2 \in O_{\mathfrak{P}}^\times \), we have

**Lemma 6.5.** The following conditions are equivalent:

(a) \( 16|h(D) \);

(b) \( \mathfrak{P} \) splits completely in \( K_s \);

(c) \( \lambda/\pi^2 \equiv \pm 1 \pmod{\mathfrak{P}^3} \).

By simple calculations we have:

**Lemma 6.6.** (a) \( f \equiv -q+1 \pmod{8} \);

(b) \[ \frac{f+\sqrt{-q}}{\pi} \equiv -q+1 \pmod{\mathfrak{P}^3}. \]
Theorem 6.7 (Williams [17]). Suppose $D$ is of type (14) and $8|h(D)$. Then $16|h(D)$ if and only if $T \equiv q-1 \pmod{16}$, equivalently, $(-1)^{\tau/8} \left( \frac{q}{2} \right) = (-1)^{h(D)/8}$, where $\varepsilon_q = T + U\sqrt{q} > 1$ is the fundamental unit of $\mathbb{Q}\sqrt{(q)}$.

Proof. By (6.3) and lemma 6.6, we have

$$\frac{\varepsilon_q+1}{2} \equiv \frac{q+1}{2} \pmod{\varphi^8},$$

and so $\lambda/\pi^2 \equiv \pm 1 \pmod{\varphi^8}$ if and only if

$$(6.8) \quad \frac{\varepsilon_q+1}{2} \equiv \frac{q+1}{2} \pmod{\varphi^8}.$$

As $q \equiv 1 \pmod{8}$ and $\varepsilon_q \equiv 1 \pmod{\varphi^8}$, that is, $q \equiv \varepsilon_q \equiv 1 \pmod{\varphi^8}$, we obtain (6.8) if and only if $\varepsilon_q \equiv q \pmod{\varphi^7}$, that is, if and only if $\varepsilon_q \equiv q \pmod{\varphi^7}$. It follows from lemma 6.5 that $16|h(D)$ if and only if $\varepsilon_q \equiv q \pmod{\varphi^8}$. Since $\varepsilon_q \equiv 1 \pmod{\varphi^8}$ and $\varepsilon_q \equiv -1 \pmod{\varphi^8}$, we have $\varepsilon_q \equiv 1 \pmod{\varphi^8}$ if and only if $(\varepsilon_q-1)(\varepsilon_q'-1)=2T \equiv 0 \pmod{32}$. Hence we deduce $\varepsilon_q-1 \equiv T \pmod{\varphi^8}$.

Q.E.D.

References


[2] E. Brown: The class number of $\mathbb{Q}(\sqrt{-p})$, for $p \equiv 1 \pmod{8}$ a prime, Proc. Amer. Math. Soc. 31 (1972), 381–383.


Department of Mathematics
Osaka University
Toyonaka, Osaka 560, Japan