Yamamoto, Y.
Osaka J. Math.
21 (1984), 1-22

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

YOSHIHIKO YAMAMOTO*

(Received August 5, 1982)

0. Introduction. Let $K=\boldsymbol{Q}(\sqrt{D})$ 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 ε_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* $\left(\frac{p}{q}\right)=1$ $\left(=\left(\frac{q}{p}\right)\right.$ *by reciprocity*);

(R2) $D=8q$, $d_1=8$ $(p=2)$, $d_2=q$, *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* $\left(\frac{-p}{q}\right)=1$ $\left(=\left(\frac{q}{p}\right)\right.$ *by reciprocity*);

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

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

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

where $\left(\frac{}{}\right)$ 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]).

* Reseach supported partly by Grant-in-Aid for Scientific Research.

1. 2-class field; divisibility by 4. Let 2^e be the order of the 2-class group of K, so that $2^e \| h^+(D)$ $(e \geqq 1)$. Since the 2-class group of $H^+(D)$ is cyclic, we have the following chain of subgroups:

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

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

$$K \subset K_2 \subset \cdots \subset K_{2^e}.$$

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

Proposition 1.1 (Reichardt [14]). *K_{2^k} is normal over $\boldsymbol{Q}$. The Galois group $G(K_{2^k}/\boldsymbol{Q})$ 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

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

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

We write $\mathfrak{a} \sim \mathfrak{b}$ (resp. $\mathfrak{a} \approx \mathfrak{b}$), if ideals $\mathfrak{a}$, $\mathfrak{b}$ 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) $C^+(\mathfrak{p}) = C^+(\mathfrak{q}) \neq 1$.

In case $D > 0$ and $d_i \neq -4$ $(i = 1, 2)$ we see easily that the condition (iii) holds if and only if $N_K \varepsilon_D = -1$. 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) $4 \mid h^+(D)$;

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

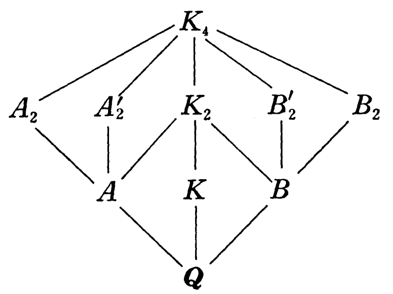
(c) *both $\mathfrak{p}$ and $\mathfrak{q}$ split completely in K_2*;

(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), $\cdots$, (I4) in section 0. The class field K_4 is normal over $\boldsymbol{Q}$ and the Galois group $G(K_4/\boldsymbol{Q})$ is isomorphic to the dihedral group D_4 of order 8. The subfields of K_4 are given as follows:



$$A=\boldsymbol{Q}(\sqrt{d_1})$$
$$B=\boldsymbol{Q}(\sqrt{d_2})$$
$$A_2=A(\sqrt{\alpha})$$
$$A_2'=A(\sqrt{\alpha'})$$
$$B_2=B(\sqrt{\beta})$$
$$B_2'=B(\sqrt{\beta'})$$

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

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

Let Q (resp. Q') be a prime divisor of $\mathfrak{q}_A$ (resp. $\mathfrak{q}_A'$) 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/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) $\mathfrak{q}_A$ *(resp.* $\mathfrak{q}_A'$*) is the only finite prime in A which ramifies in A_2 (resp. A_A').*

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

(2.2) $\mathfrak{p}_B$ *(resp.* $\mathfrak{p}_B'$*) is the only finite prime in B which ramifies in B_2 (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 ∞ of $\boldsymbol{Q}$ ramifies in A, $\infty=\infty_A^2$, and splits in B, $\infty=\infty_B\infty_B'$. By a suitable choice of ∞_B and ∞_B' we see that

(2.3) *if $D<0$, then both A_2 and A_2' are unramified at ∞_A, and B_2 (resp. B_2') is ramified at ∞_B (resp. ∞_B') and unramified at ∞_B' (resp. ∞_B).*

If $D>0$, both A and B are real, so that ∞ 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 $4\nmid h(D)$, then $2\|h(D)$ and $N_K\varepsilon_D=1$, so that K_4 is ramified at every infinite prime of K, which implies that K_2 is the inertia field of ∞ with respect to $K_4/\boldsymbol{Q}$, for K_2 is normal over $\boldsymbol{Q}$. Hence we have

(2.4) *if $D>0$ and $2\|h(D)$, 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 $4|h(D)$ then K_4 is unramified at every infinite prime over $\boldsymbol{Q}$. Hence we have

(2.5) *if $D>0$ and $4|h(D)$, 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 χ_A (resp. f_B and χ_B) be the conductor and the Hecke ideal character attached to the quadratic extension A_2/A (resp. B_2/B).

Proposition 2.6. *Suppose D belongs to type* (R1). *Then*
(a) *if $2\|h(d)$, we have*

$$f_A=\mathfrak{q}_A\infty_A\infty_A',\quad \chi_A((\lambda))=\left(\frac{\lambda}{\mathfrak{q}_A}\right)\mathit{sgn}\,N_A\lambda\qquad(\lambda\in O_A-\mathfrak{q}_A);$$

$$f_B=\mathfrak{p}_B\infty_B\infty_B',\quad \chi_B((\mu))=\left(\frac{\mu}{\mathfrak{p}_B}\right)\mathit{sgn}\,N_B\mu\qquad(\mu\in O_B-\mathfrak{p}_B);$$

(b) *if $4|h(D)$, we have*

$$f_A=\mathfrak{q}_A,\quad \chi_A((\lambda))=\left(\frac{\lambda}{\mathfrak{q}_A}\right)\qquad(\lambda\in O_A-\mathfrak{q}_A);$$

$$f_B=\mathfrak{p}_B,\quad \chi_B((\mu))=\left(\frac{\mu}{\mathfrak{p}_B}\right)\qquad(\mu\in O_B-\mathfrak{p}_B);$$

where $\left(\frac{\ }{\mathfrak{q}_A}\right)$ (resp. $\left(\frac{\ }{\mathfrak{p}_B}\right)$) denotes the quadratic residue symbol modulo $\mathfrak{q}_A$ (resp. $\mathfrak{p}_B$).

Proof. If $2\|h(D)$ then $N_K\varepsilon_D=1$. It follows from (2.1), (2.2), and (2.4) that the quadratic extension A_2/A (resp. B_2/B) is ramified at $\mathfrak{q}_A$, ∞_A, ∞_A' (resp. $\mathfrak{p}_B$, ∞_B, ∞_B') and unramified outside them. Hence

$$\begin{aligned}\chi_A((\lambda))&=\left(\frac{\lambda,\,A_2/A}{\mathfrak{q}_A}\right)\left(\frac{\lambda,\,A_2/A}{\infty_A}\right)\left(\frac{\lambda,\,A_2/A}{\infty_A'}\right)\qquad\text{(norm-residue symbol)}\\&=\left(\frac{\lambda,\,\alpha}{\mathfrak{q}_A}\right)\left(\frac{\lambda,\,\alpha}{\infty_A}\right)\left(\frac{\lambda,\,\alpha}{\infty_A'}\right)\qquad\text{(Hilbert symbol)}\\&=\left(\frac{\lambda}{\mathfrak{q}_A}\right)(\mathit{sgn}\,\lambda)(\mathit{sgn}\,\lambda')\\&=\left(\frac{\lambda}{\mathfrak{q}_A}\right)\mathit{sgn}\,N_A\lambda\qquad(\lambda\in O_A-\mathfrak{q}_A),\end{aligned}$$

which implies $f_A=\mathfrak{q}_A\infty_A\infty'_A$. We have $\chi_B((\mu))=\left(\frac{\mu}{\mathfrak{p}_B}\right) sgn\, N_B\mu$ and $f_B=\mathfrak{p}_B\infty_B\infty'_B$ in the same way.

If $4|h(D)$, then, from (2.1), (2.2), and (2.5), it follows that A_2/A (resp. B_2/B) is ramified only at $\mathfrak{q}_A$ (resp. $\mathfrak{p}_B$). Hence the assertion (b) follows in the same way. Q.E.D.

Proposition 2.7. *Suppose D is of type* (R2). *Then*
(a) *if* $2||h(D)$, *we have*

$$f_A=\mathfrak{q}_A\infty_A\infty'_A\,,\quad \chi_A((\lambda))=\left(\frac{\lambda}{\mathfrak{q}_A}\right) sgn\, N_A\lambda \qquad (\lambda\in O_A-\mathfrak{q}_A);$$

$$f_B=\mathfrak{p}_B^3\infty_B\infty'_B\,,\quad \chi_B((\mu))=\left(\frac{\mu}{\mathfrak{p}_B}\right) sgn\, N_B\mu \qquad (\mu\in O_B-\mathfrak{p}_B);$$

(b) *if* $4|h(D)$, *we have*

$$f_A=\mathfrak{q}_A\,,\quad \chi_A((\lambda))=\left(\frac{\lambda}{\mathfrak{q}_A}\right) \qquad (\lambda\in O_A-\mathfrak{q}_A);$$

$$f_B=\mathfrak{p}_B^3\,,\quad \chi_B((\mu))=\left(\frac{\mu,\,2}{\mathfrak{p}_B}\right) \qquad (\mu\in O_B-\mathfrak{p}_B);$$

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

Proof. If $2||h(D)$ then $N_K\varepsilon_D=1$. 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 $\mathfrak{q}_A$, ∞_A, ∞'_A (resp. $\mathfrak{p}_B$, ∞_B, ∞'_B). We have $\chi_A((\lambda))=\left(\frac{\lambda}{\mathfrak{q}_A}\right) sgn\, N_A\lambda$ in the same way as in the proof of proposition 2.6, while $\left(\frac{\mu,\,\beta}{\mathfrak{p}_B}\right)=\left(\frac{\mu,\,2}{\mathfrak{p}_B}\right)$, 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*

$$f_A=\mathfrak{q}_A\,,\qquad \chi_A((\lambda))=\left(\frac{\lambda}{\mathfrak{q}_A}\right) \qquad (\lambda\in O_A-\mathfrak{q}_A);$$

$$f_B=\mathfrak{p}_B\infty_B\,,\quad \chi_B((\mu))=\left(\frac{\mu}{\mathfrak{p}_B}\right)\left(\frac{\mu,\,\beta}{\infty_B}\right) \qquad (\mu\in O_B-\mathfrak{p}_B)\,.$$

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

$$f_A=\mathfrak{q}_A^3\,,\qquad \chi_A((\lambda))=\left(\frac{\lambda,\,2}{\mathfrak{q}_A}\right) \qquad (\lambda\in O_A-\mathfrak{q}_A);$$

$$f_B = \mathfrak{p}_B \infty_B\,,\quad \chi_B((\mu)) = \left(\frac{\mu}{\mathfrak{p}_B}\right)\left(\frac{\mu,\,\beta}{\infty_B}\right) \qquad (\mu \in O_B - \mathfrak{p}_B)\,.$$

Proposition 2.10. *Suppose D is of type* (I3), *then*

$$f_A = \mathfrak{q}_A\,,\qquad \chi_A((\lambda)) = \left(\frac{\lambda}{\mathfrak{q}_A}\right) \qquad (\lambda \in O_A - \mathfrak{q}_A);$$

$$f_B = \mathfrak{p}_B^3 \infty_B\,,\quad \chi_B((\mu)) = \left(\frac{\mu,\,-2}{\mathfrak{p}_B}\right)\left(\frac{\mu,\,\beta}{\infty_B}\right) \qquad (\mu \in O_B - \mathfrak{p}_B)\,,$$

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

Proposition 2.11. *Suppose D is of type* (I4), *then*

$$f_A = \mathfrak{q}_A\,,\qquad \chi_A((\lambda)) = \left(\frac{\lambda}{\mathfrak{q}_A}\right) \qquad (\lambda \in O_A - \mathfrak{q}_A);$$

$$f_B = \mathfrak{p}_B^2 \infty_B\,,\quad \chi_B((\mu)) = \left(\frac{\mu,\,-1}{\mathfrak{p}_B}\right)\left(\frac{\mu,\,\beta}{\infty_B}\right) \qquad (\mu \in O_B - \mathfrak{p}_B)\,,$$

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

In propositions 2.8 to 2.11 the infinite prime ∞_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 μ with respect to ∞_B.

Proposition 2.12. *For each D, α and β 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)

$$\text{(R1):} \begin{cases} \alpha\alpha' = q^{h(p)}\,, \\ \alpha^3 \equiv 1 \pmod 4\,, \end{cases} \qquad \begin{matrix} \beta\beta' = p^{h(q)}\,, \\ \beta^3 \equiv 1 \pmod 4; \end{matrix}$$

$$\text{(R2):} \begin{cases} \alpha\alpha' = q\,, \\ \alpha \equiv 1 \text{ or } 3+2\sqrt{2} \pmod 4\,, \end{cases} \qquad \begin{matrix} \beta\beta' = 2^{h(q)}\,, \\ \beta+\beta' \equiv 2^{h(q)}+1 \pmod 4; \end{matrix}$$

$$\text{(I1):} \begin{cases} \alpha\alpha' = q^{h(-p)}\,, \\ \alpha^3 \equiv 1 \pmod 4\,, \end{cases} \qquad \begin{matrix} \beta\beta' = -p^{h(q)}\,, \\ \beta^3 \equiv 1 \pmod 4; \end{matrix}$$

$$\text{(I2):} \begin{cases} \alpha\alpha' = 2^{h(-p)}\,, \\ \alpha+\alpha' \equiv 2^{h(-p)}+1 \pmod 4\,, \end{cases} \qquad \begin{matrix} \beta\beta' = -p\,, \\ \beta \equiv 1 \text{ or } 3+2\sqrt{2} \pmod 4; \end{matrix}$$

$$\text{(I3):} \begin{cases} \alpha\alpha' = q\,, \\ \alpha \equiv 1 \text{ or } 3+2\sqrt{-2} \pmod 4\,, \end{cases} \qquad \begin{matrix} \beta\beta' = -2^{h(q)}\,, \\ \beta+\beta' \equiv -2^{h(q)}+1 \pmod 4; \end{matrix}$$

$$(\mathrm{I4}):\begin{cases}\alpha\alpha'=q\,, & \beta\beta'=-1\,,\\ \alpha\equiv\pm1\ (\mathrm{mod}\ 4)\,, & \beta+\beta'\equiv 0\ (\mathrm{mod}\ 4)\,.\end{cases}$$

Conversely, for each α (*resp.* β) *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 $\mathfrak{q}_A$ is the unique finite prime which is ramified in $A_2=A(\sqrt{\alpha})$ and $\alpha\alpha'\equiv d_2\,(\mathrm{mod}\,(A^\times)^2)$, we have $(\alpha)=\mathfrak{q}_A\mathfrak{a}^2$ with an ideal $\mathfrak{a}$ in A. It is well-known that the class number $h(d_1)$ is odd. Put $\mathfrak{a}^{h(d_1)}=(\gamma)$. We may replace α by $\alpha^{h(d_1)}\gamma^{-2}$, then $(\alpha)=\mathfrak{q}_A^{h(d_1)}$, so that $\alpha\in O_A$, $(\alpha,\alpha')=1$, and $\alpha\alpha'=\pm N_A\,\mathfrak{q}_A^{h(d_1)}=\pm q^{h(d_1)}$. The sign of the right hand side is determined by the multiplicative congruence $\alpha\alpha'\equiv d_2$ (mod $(A^\times)^2$). Let $\mathfrak{r}_A$ be a prime ideal in A such that $\mathfrak{r}_A\,|\,(2)$ and $\mathfrak{r}_A\neq\mathfrak{q}_A$. The ideal $\mathfrak{r}_A$ is unramified in A_2 if and only if there exists an integer $\delta\in O_A$ such that $\alpha\equiv\delta^2\,(\mathrm{mod}\,\mathfrak{r}_A^{2e})$, where e is the index of ramification of $\mathfrak{r}_A$ with respect to $A/\boldsymbol{Q}$, that is, $\mathfrak{r}_A^e\,||\,(2)$. Hence we have

$$\begin{array}{lll}\alpha^3\equiv 1\ (\mathrm{mod}\ 4) & & \text{if } p\neq 2 \text{ and } q\neq 2;\\ \alpha\ \equiv \text{a square}\ (\mathrm{mod}\ 4) & & \text{if } p=2 \text{ and } q\neq 2;\\ \alpha\ \equiv 1\ (\mathrm{mod}\ \mathfrak{q}_A'^2) & & \text{if } p\neq 2 \text{ and } q=2\,.\end{array}$$

In the last case ($p\neq 2$, $q=2$), it follows from $\alpha'\equiv 1\,(\mathrm{mod}\,\mathfrak{q}_A^2)$ that $(\alpha-1)(\alpha'-1)=2^{h(d_1)}-\alpha-\alpha'+1\equiv 0$ (mod 4). We can argue similarly for β except in the case (I4), in which we may proceed as follows. Since $\beta\beta'\equiv -4\,(\mathrm{mod}\,(B^\times)^2)$, we have $\beta\in O_B$ and $\beta\beta'=-1$, that is, β is a unit, by a suitable choice of representative β modulo $(B^\times)^2$. As $B(\sqrt{\beta})/B$ is ramified at $\mathfrak{p}_B$ and unramified at $\mathfrak{p}_B'$, we have $\beta\equiv -1\,(\mathrm{mod}\,\mathfrak{p}_B^2)$ and $\beta\equiv 1\,(\mathrm{mod}\,\mathfrak{p}_B'^2)$. Hence $\beta-1\equiv 0\,(\mathrm{mod}\,\mathfrak{p}_B\mathfrak{p}_B'^2)$ and $(\beta-1)(\beta'-1)=-\beta-\beta'\equiv 0$ (mod 8), which implies $\beta+\beta'\equiv 0$ (mod 8). Conversely, if we take α, β satisfying conditions (a) and (b) then it is easily seen that $A(\sqrt{\alpha},\sqrt{\alpha'})$ (resp. $B(\sqrt{\beta},\sqrt{\beta'})$) is a Galois extension of $\boldsymbol{Q}$ 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 $B_2=B(\sqrt{\beta})$. Q.E.D.

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

Putting, for each D, respectively:

$$(\mathrm{R1})^*:\qquad \alpha=\frac{x+y\sqrt{p}}{2}\,,\qquad \beta=\frac{z+w\sqrt{q}}{2}\,;$$

(R2)*: $\alpha=x+y\sqrt{2}$, $\beta=\dfrac{z+w\sqrt{q}}{2}$;

(I1)* : $\alpha=\dfrac{x+y\sqrt{-p}}{2}$, $\beta=\dfrac{z+w\sqrt{q}}{2}$;

(I2)* : $\alpha=\dfrac{x+y\sqrt{-p}}{2}$, $\beta=z+w\sqrt{2}$;

(I3)* : $\alpha=x+y\sqrt{-2}$, $\beta=\dfrac{z+w\sqrt{q}}{2}$;

(I4)* : $\alpha=x+y\sqrt{-1}$, $\beta=z+w\sqrt{q}$;

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

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

(c) $x, y, z, w\in\boldsymbol{Z}$ *and* $q\nmid(x, y)$, $p\nmid(z, w)$;

(d)

(R1)**: $\begin{cases} x^2-py^2=4q^{h(p)}, \\ \left(\dfrac{x+y\sqrt{p}}{2}\right)^3\equiv 1 \pmod 4, \end{cases}$ $\quad z^2-qw^2=4p^{h(q)}$, $\left(\dfrac{z+w\sqrt{q}}{2}\right)^3\equiv 1 \pmod 4$;

(R2)**: $\begin{cases} x^2-2y^2=q, \\ (x, y)\equiv(1, 0) \text{ or } (3, 2) \pmod 4, \end{cases}$ $\quad z^2-qw^2=2^{h(q)+2}$, $z\equiv 2^{h(q)}+1 \pmod 4$;

(I1)** : $\begin{cases} x^2+py^2=4q^{h(-p)}, \\ \left(\dfrac{x+y\sqrt{-p}}{2}\right)^3\equiv 1 \pmod 4, \end{cases}$ $\quad z^2-qw^2=-4p^{h(q)}$, $\left(\dfrac{z+w\sqrt{q}}{2}\right)^3\equiv 1 \pmod 4$;

(I2)** : $\begin{cases} x^2+py^2=4q^{h(-p)}, \\ x\equiv 2^{h(-p)}+1 \pmod 4, \end{cases}$ $\quad z^2-2w^2=-p$, $(z, w)\equiv (1, 0) \text{ or } (3, 2) \pmod 4$;

(I3)** : $\begin{cases} x^2+2y^2=q, \\ (x, y)\equiv(1, 0) \text{ or } (3, 2) \pmod 4, \end{cases}$ $\quad z^2-qw^2=-2^{h(q)+2}$, $z\equiv -2^{h(q)}+1 \pmod 4$;

(I4) **: $\begin{cases} x^2+y^2=q, \\ y\equiv 0 \pmod 4, \end{cases}$ $\quad z^2-qw^2=-1$, $z\equiv 0 \pmod 4$.

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

$(x, y)\equiv(2, 0)$ or $(6, 4) \pmod 8$ if $d\equiv 1 \pmod 8$,

$(x, y)\equiv(2, 0)$, $(6, 4)$, $(3, 1)$, $(3, 7)$, $(7, 3)$, or $(7, 5) \pmod 8$ if $d\equiv 5 \pmod{16}$,

$(x, y)\equiv(2, 0)$, $(6, 4)$, $(3, 3)$, $(3, 5)$, $(7, 1)$, 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* $C^+(\mathfrak{p})$ *and* $C^+(\mathfrak{q})$ *belong to* $H^+(D)^4$;
(c) *both* $\mathfrak{p}$ *and* $\mathfrak{q}$ *split completely in* K_4.

Using the notation of section 2, we obtain easily:

Lemma 3.2. *The following conditions are equivalent:*
(a) $C^+(\mathfrak{p})\in H^+(D)^4$ (*resp.* $C^+(\mathfrak{q})\in H^+(D)^4$);
(b) $\mathfrak{p}$ (*resp.* $\mathfrak{q}$) *splits completely in* K_4/K;
(c) $\mathfrak{p}_A$ (*resp.* $\mathfrak{q}_B$) *splits completely in* A_2/A (*resp.* B_2/B);
(d) $\mathfrak{p}'_B$ (*resp.* $\mathfrak{q}'_A$) *splits completely in* B_2/B (*resp.* A_2/A);
(e) $\chi_A(\mathfrak{p}_A)=1$ (*resp.* $\chi_B(\mathfrak{q}_B)=1$);
(f) $\chi_B(\mathfrak{p}'_B)=1$ (*resp.* $\chi_A(\mathfrak{q}'_A)=1$).

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* $\mathfrak{p}\approx 1$ *and* $\mathfrak{q}\not\approx 1$;

if $\left(\frac{2}{q}\right)_4=1$ *and* $\left(\frac{q}{2}\right)_4=-1$ *then* $\mathfrak{p}\not\approx 1$ *and* $\mathfrak{q}\approx 1$;

(b) $4\|h(D)$ *and* $N_K\varepsilon_D=-1$ *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) $\left(\frac{p}{q}\right)_4=(-1)^{h(D)/2}\left(\frac{z}{p}\right)$ *and* $\left(\frac{q}{p}\right)_4=(-1)^{h(D)/2}\left(\frac{x}{q}\right)$,
where x, z are rational integers satisfying the conditions (c), (d) (R1)** *of proposition* 2.13.

Proof. Assume $2\|h(D)$. Since $N_K\varepsilon_D=1$ we have $\mathfrak{p}\approx 1$ and $\mathfrak{q}\not\approx 1$ or $\mathfrak{p}\not\approx 1$ and $\mathfrak{q}\approx 1$ alternatively. In the first case we have $C^+(\mathfrak{p})\in H^+(D)^4$ and $C^+(\mathfrak{q})\notin H^+(D)^4$, hence, by proposition 2.6 (a) and lemma 3.2,

$$1=\chi_A(\mathfrak{p}_A)=\chi_A((\sqrt{p}))=\left(\frac{\sqrt{p}}{\mathfrak{q}_A}\right)sgn\,N_A\sqrt{p}=-\left(\frac{p}{q}\right)_4,$$

$$-1=\chi_B(\mathfrak{q}_B)=\chi_B((\sqrt{q}))=\left(\frac{\sqrt{q}}{\mathfrak{p}_B}\right) sgn\, N_B\sqrt{q}=-\left(\frac{q}{p}\right)_4.$$

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 $4|h(D)$, then, by proposition 2.6 (b), we have $\chi_A(\mathfrak{p}_A)=\left(\frac{\sqrt{p}}{\mathfrak{q}_A}\right)=\left(\frac{p}{q}\right)_4$ and $\chi_B(\mathfrak{q}_B)=\left(\frac{\sqrt{q}}{\mathfrak{p}_B}\right)=\left(\frac{q}{p}\right)_4$. If $8\nmid h^+(D)$ then $4\|h(D)$ and $N_K\varepsilon_D=-1$, hence $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$ and we see, by proposition 3.1 and lemma 3.2, $C^+(\mathfrak{p})=C^+(\mathfrak{q})\notin H^+(D)^4$ and $\chi_A(\mathfrak{p}_A)=\chi_B(\mathfrak{q}_B)=-1$. If $8|h^+(D)$, then we get $\chi_A(\mathfrak{p}_A)=\chi_B(\mathfrak{q}_B)=1$ in the same way. To sum up, we get the assertions (a), (b), (c), and that

$$\chi_A(\mathfrak{p}_A)=(-1)^{h(D)/2}\left(\frac{p}{q}\right)_4 \text{ and } \chi_B(\mathfrak{q}_B)=(-1)^{h(D)/2}\left(\frac{q}{p}\right)_4.$$

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

$$\begin{aligned}\chi_A(\mathfrak{p}_A)&=\chi_B(\mathfrak{p}'_B) &&\text{(lemma 3.2)}\\ &=\chi_B(\mathfrak{p}'_B)^{h(d_2)}=\chi_B((\beta'))\\ &=\left(\frac{\beta'}{\mathfrak{p}_B}\right) &&\text{(proposition 2.6, proposition 2.12)}\\ &=\left(\frac{\beta+\beta'}{\mathfrak{p}_B}\right)=\left(\frac{z}{p}\right) &&\text{(by (R1)*)}\end{aligned}$$

and similarly $\chi_B(\mathfrak{q}_B)=\left(\frac{x}{q}\right)$, 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* $\mathfrak{p}\approx 1$ *and* $\mathfrak{q}\not\approx 1$;

if $\left(\frac{p}{q}\right)_4=1$ *and* $\left(\frac{q}{p}\right)_4=-1$ *then* $\mathfrak{p}\not\approx 1$ *and* $\mathfrak{q}\approx 1$;

(b) $4\|h(D)$ *and* $N_K\varepsilon_D=-1$ *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) $\left(\frac{2}{q}\right)_4=\left(\frac{z-2^{h(q)}}{2}\right)$ *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*

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

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

Proof. Using the following:

$$\text{(3.5)}\qquad \begin{cases} \left(\dfrac{\sqrt{q},2}{\mathfrak{p}_B}\right)=\left(\dfrac{q}{2}\right)_4, \\ \left(\dfrac{\beta',2}{\mathfrak{p}_B}\right)=\left(\dfrac{z-2^{h(q)}}{2}\right), \end{cases}$$

we can argue in the same way as in the proof of proposition 3.3. The first equlity of (3.5) is checked straightforwardly. Since $\beta'\equiv 1 \pmod{\mathfrak{p}_B^2}$, we see $\left(\frac{\beta',2}{\mathfrak{p}_B}\right)=1$ if and only if $\beta'\equiv 1 \pmod{\mathfrak{p}_B^3}$, that is, if and only if $(\beta-1)(\beta'-1)\equiv 0 \pmod{\mathfrak{p}_B^3}$, for $\beta\not\equiv 1 \pmod{\mathfrak{p}_B}$; on the other hand $(\beta-1)(\beta'-1)=\beta\beta'-\beta-\beta'+1=2^{h(q)}-z+1$; so we get the latter equality of (3.5). Q.E.D.

Proposition 3.5 (cf. [12] [9]). *Suppose D is of type* (I1), *then*

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

where x, z, w are rational integers satisfying the conditions (c), (d) (I1)** *of proposition* 2.13.

Proof. Since $\mathfrak{p}\mathfrak{q}=(\sqrt{-pq})\approx 1$, we have $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$. It follows from proposition 3.1 and lemma 3.2 that $\chi_A(\mathfrak{p}_A)=\chi_B(\mathfrak{q}_B)=\chi_B(\mathfrak{p}'_B)=\chi_A(\mathfrak{q}'_A)=(-1)^{h^+(D)/4}$. By proposition 2.8 we have

$$\chi_A(\mathfrak{p}_A)=\left(\frac{\sqrt{-p}}{\mathfrak{q}_A}\right)=\left(\frac{-p}{\mathfrak{q}_A}\right)_4=\left(\frac{-p}{q}\right)_4,$$

$$\chi_A(\mathfrak{q}'_A)=\chi_A(\mathfrak{q}'_A)^{h(-p)}=\chi_A((\alpha'))=\left(\frac{\alpha'}{\mathfrak{q}_A}\right)=\left(\frac{\alpha+\alpha'}{\mathfrak{q}_A}\right)=\left(\frac{x}{q}\right),$$

$$\chi_B(\mathfrak{p}'_B)=\chi_B(\mathfrak{p}'_B)^{h(q)}=\chi_B((\beta'))=\left(\frac{\beta'}{\mathfrak{p}_B}\right)\left(\frac{\beta',\beta}{\infty_B}\right)=\left(\frac{z}{p}\right),$$

$$\chi_B(\mathfrak{q}_B)=\chi_B((\sqrt{q}))=\left(\frac{\sqrt{q}}{\mathfrak{p}_B}\right)\left(\frac{\sqrt{q},\beta}{\infty_B}\right).$$

It follows from $\left(\frac{\beta,\beta}{\infty_B}\right)=-1$ that $\left(\frac{\sqrt{q},\beta}{\infty_B}\right)=-sgn\, w$. Since $\beta=\frac{z+w\sqrt{q}}{2}$

$\equiv 0 \pmod{\mathfrak{p}_B}$, we have $\sqrt{q} \equiv -\frac{z}{w} \pmod{\mathfrak{p}_B}$, so that $\chi_B(\mathfrak{q}_B)=\left(\frac{-z/w}{p}\right)(-sgn\, w)$ $=\left(\frac{zw}{p}\right) sgn\, w$, which implies $\left(\frac{w}{p}\right)=sgn\, w$. Q.E.D.

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

$$\left(\frac{-p}{2}\right)_4 = \left(\frac{x-2^{h(-p)}}{2}\right) = \left(\frac{z}{p}\right) = (-1)^{h(D)/4} \text{ and } \left(\frac{w}{p}\right) = sgn\, w\,,$$

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

Proof. Since $\mathfrak{p}\mathfrak{q}=(\sqrt{-2p})\approx 1$, we see that $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$. By proposition 3.1 and lemma 3.2 we have $\chi_A(\mathfrak{p}_A)=\chi_B(\mathfrak{q}_B)=\chi_A(\mathfrak{q}'_A)=\chi_B(\mathfrak{p}'_B)=(-1)^{h(D)/4}$. By proposition 2.9 we have

$$\chi_A(\mathfrak{p}_A) = \chi_A((\sqrt{-p})) = \left(\frac{\sqrt{-p},\, 2}{\mathfrak{q}_A}\right) = \left(\frac{-p}{2}\right)_4,$$

$$\chi_A(\mathfrak{q}'_A) = \chi_A((\alpha')) = \left(\frac{\alpha',\, 2}{\mathfrak{q}_A}\right) = \left(\frac{x-2^{h(-p)}}{2}\right),$$

$$\chi_B(\mathfrak{p}'_B) = \chi_B((\beta')) = \left(\frac{\beta'}{\mathfrak{p}_B}\right)\left(\frac{\beta',\, \beta}{\infty_B}\right) = \left(\frac{z}{p}\right),$$

$$\chi_B(\mathfrak{q}_B) = \chi_B((\sqrt{2})) = \left(\frac{\sqrt{2}}{\mathfrak{p}_B}\right)\left(\frac{\sqrt{2},\, \beta}{\infty_B}\right) = \left(\frac{zw}{p}\right) sgn\, w\,,$$

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*

$$\left(\frac{-2}{q}\right)_4 = \left(\frac{x}{q}\right) = \left(\frac{z+2^{h(q)}}{2}\right) = \left(\frac{q}{2}\right)_4(-sgn\, w) = (-1)^{h(D)/4},$$

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

Proof. Since $\mathfrak{p}\mathfrak{q}=(\sqrt{-2q})\approx 1$, we have $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$. By proposition 3.1 and lemma 3.2 we have

$$\chi_A(\mathfrak{p}_A) = \chi_B(\mathfrak{q}_B) = \chi_A(\mathfrak{q}'_A) = \chi_B(\mathfrak{p}'_B) = (-1)^{h(D)/4}\,.$$

By proposition 2.10, we have

$$\chi_A(\mathfrak{p}_A) = \chi_A((\sqrt{-2}) = \left(\frac{\sqrt{-2}}{\mathfrak{q}_A}\right)_4 = \left(\frac{-2}{q}\right)_4,$$

$$\chi_A(\mathfrak{q}_A') = ((\alpha')) = \left(\frac{\alpha'}{\mathfrak{q}_A}\right) = \left(\frac{x}{q}\right),$$
$$\chi_B(\mathfrak{p}_B') = \chi_B((\beta')) = \left(\frac{\beta', -2}{\mathfrak{p}_B}\right)\left(\frac{\beta', \beta}{\infty_B}\right) = \left(\frac{\beta', -2}{\mathfrak{p}_B}\right) = \left(\frac{z+2^{h(q)}}{2}\right),$$
$$\chi_B(\mathfrak{q}_B) = \chi_B((\sqrt{q})) = \left(\frac{\sqrt{q}, -2}{\mathfrak{p}_B}\right)\left(\frac{\sqrt{q}, \beta}{\infty_B}\right).$$

We may safely assume $\sqrt{q} \equiv 1 \pmod{\mathfrak{p}_B^2}$, by transposing $\mathfrak{p}_B$ and $\mathfrak{p}_B'$ if necessary, obtaining $\left(\frac{\sqrt{q}, -2}{\mathfrak{p}_B}\right) = \left(\frac{q}{2}\right)_4$ and $2\beta \equiv z + w\sqrt{q} \equiv z+w \pmod{\mathfrak{p}_B^2}$. 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 ∞_B that $w\sqrt{q} < 0$ with respect to ∞_B, which implies $\left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = -sgn\ w$. Q.E.D.

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

$$\left(\frac{2}{q}\right)_4 \left(\frac{q}{2}\right)_4 = (-1)^{z/4} = (-1)^{h(d)/4},$$
$$\left(\frac{x}{q}\right) = 1, \quad \textit{and} \quad w \equiv 1 \pmod 4),$$

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

Proof. Since $\mathfrak{q} = (\sqrt{-q}) \approx 1$, we get $\mathfrak{p} \not\approx 1$, so that, by proposition 3.1 and lemma 3.2, we have $\chi_A(\mathfrak{p}_A) = \chi_B(\mathfrak{p}_B') = (-1)^{h(D)/4}$ and $\chi_A(\mathfrak{q}_A') = \chi_B(\mathfrak{q}_B) = 1$. By proposition 2.11, we have

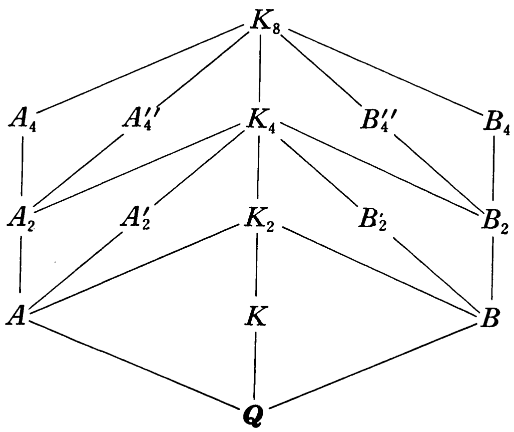
$$\chi_A(\mathfrak{p}_A) = \chi_A((1+\sqrt{-1})) = \left(\frac{1+\sqrt{-1}}{\mathfrak{q}_A}\right) = \left(\frac{2\sqrt{-1}}{\mathfrak{q}_A}\right)_4$$
$$= \left(\frac{2}{q}\right)_4 \left(\frac{q}{2}\right)_4.$$

Since $B_2 = B(\sqrt{\beta})$ and $\beta \equiv 1 \pmod{\mathfrak{p}_B'^2}$, we have $\chi_B(\mathfrak{p}_B') = 1$ if and only if $\beta \equiv 1 \pmod{\mathfrak{p}_B'^3}$. As $\mathfrak{p}_B \| (\beta - 1)$, we have $\beta \equiv 1 \pmod{\mathfrak{p}_B'^3}$ if and only if $(\beta-1)(\beta'-1) = -2z \equiv 0 \pmod{16}$. On the other hand,

$$\chi_A(\mathfrak{q}_A') = \chi_A((\alpha')) = \left(\frac{\alpha'}{\mathfrak{q}_A}\right) = \left(\frac{x}{q}\right) = 1,$$
$$\chi_B(\mathfrak{q}_B) = \chi_B((\sqrt{q})) = \left(\frac{\sqrt{q}, -1}{\mathfrak{p}_B}\right)\left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = 1.$$

Since $\sqrt{q} \equiv \pm 1 \pmod{\mathfrak{p}_B^2}$, we have $\left(\frac{\sqrt{q}, \beta}{\infty_B}\right) = \pm 1$, which implies $w \lessgtr 0$, while $\beta'=z-w\sqrt{q}\equiv\mp w\equiv 1 \pmod{\mathfrak{p}_B^2}$. 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 $\boldsymbol{Q}$ and both $G(K_8/A_2)$ and $G(K_2/B_2)$ are isomorphic to $Z_2\times Z_2$. The intermediate fields of K_8/A_2 and K_8/B_2 are given in the following diagram:



$$A_2=A_4(\sqrt{\alpha_2}),\quad \alpha_2\in A_2$$
$$A_4''=A_2(\sqrt{\alpha_2''}),$$
$$B_4=B_2(\sqrt{\beta_2}),\quad \beta_2\in B_2$$
$$B_4''=B_2(\sqrt{\beta_2''}),$$
$$\alpha_2\alpha_2''\equiv\alpha' \pmod{(A_2^\times)^2},$$
$$\beta_2\beta_2''\equiv\beta' \pmod{(B_2^\times)^2};$$

where α_2'' (resp. β_2'') denotes the conjugae of α_2 over A (resp. of β_2 over B). By proposition 3.1, both $\mathfrak{p}_A$ and $\mathfrak{q}_A'$ (resp. both $\mathfrak{p}_B'$ and $\mathfrak{q}_B$) split completely in A_2 (resp. in B_2) and $\mathfrak{q}_A$ (resp. $\mathfrak{p}_B$) is ramified in A_2 (resp. in B_2). We put

$$\mathfrak{p}_A=P_AP_A'',\quad \mathfrak{q}_A=\hat{Q}_A^2,\qquad \mathfrak{q}_A'=Q_AQ_A'',$$
$$\mathfrak{p}_B=\hat{P}_B^2,\qquad \mathfrak{p}_B'=P_BP_B'',\quad \mathfrak{q}_B=Q_BQ_B'',$$

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 K_8/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:

(4.1) *Q_A (resp. P_B) is the only finite prime of A_2 (resp. B_2), which is ramified in A_4 (resp. B_4).*

Arguing the ramification of the infinite primes in A_2 (resp. B_2) as in section 2, we obtain:

(4.2) *If $D<0$, then there is no (resp. only one (denoted by V_B)) infinite prime in A_2 (resp. B_2) which is ramified in A_4 (resp. B_4).*

(4.3) *If $D>0$, $4\|h(D)$, and $N_K\varepsilon_D=1$, then every infinite prime in A_2 (resp. B_2) is ramified in A_4 (resp. B_4).*

(4.4) *If $D>0$ and $8|h(D)$, then every infinite prime in A_2 (resp. B_2) is unramified in A_4 (resp. B_4).*

Let ψ_A (resp. ψ_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 ψ_A and ψ_B as follows:

Proposition 4.5. *Suppose D is of type* (R1) *and* $8|h^+(D)$. *Then*
(a) *if* $4\|h(D)$, *we have*

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

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

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

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

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

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

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

We have

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

where $\mathrm{ord}(\alpha_2)$ is the order of α_2 with respect to Q_A, and

$$\prod_{v|\infty} \left(\frac{\lambda,\ A_4/A_2}{v}\right) = \prod_{v|\infty} sgn\, \lambda^v = N_{A_2}\lambda.$$

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*

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

$$\psi_B((\mu))=\left(\frac{\mu,\,2}{P_B}\right)\,sgn\,N_{B_2}\mu \qquad (\mu\in O_{B_2}-P_B);$$

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

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

$$\psi_B((\mu))=\left(\frac{\mu,\,2}{P_B}\right) \qquad (\mu\in O_{B_2}-P_B)\,.$$

Proof. Since $B_4''=B_2(\sqrt{\beta_2''})$ is unramified at P_B,

$$\left(\frac{\mu,\,B_4/B_2}{P_B}\right)=\left(\frac{\mu,\,\beta_2}{P_B}\right)=\left(\frac{\mu,\,\beta_2\beta_2''}{P_B}\right)=\left(\frac{\mu,\,\beta'}{P_B}\right)$$
$$=\left(\frac{\mu,\,\beta\beta'}{P_B}\right)=\left(\frac{\mu,\,2}{P_B}\right).$$

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* $8\,|\,h(D)$, *then*

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

$$\psi_B((\mu))=\left(\frac{\mu}{P_B}\right)\left(\frac{\mu,\,\beta_2}{V_B}\right) \qquad (\mu\in O_{B_2}-P_B)\,.$$

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

$$\psi_A((\lambda))=\left(\frac{\lambda,\,2}{Q_A}\right) \qquad (\lambda\in O_{A_2}-Q_A);$$

$$\psi_B((\mu))=\left(\frac{\mu}{P_B}\right)\left(\frac{\mu,\,\beta_2}{V_B}\right) \qquad (\mu\in O_{B_2}-P_B)\,.$$

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

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

$$\psi_B((\mu))=\left(\frac{\mu,\,-2}{P_B}\right)\left(\frac{\mu,\,\beta_2}{V_B}\right) \qquad (\mu\in O_{B_2}-P_B)\,.$$

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

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

$$\psi_B((\mu)) = \left(\frac{\mu,\ -1}{P_B}\right)\left(\frac{\mu,\ \beta_2}{V_B}\right) \qquad (\mu \in O_{B_2} - P_B)\,.$$

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* $C^+(\mathfrak{p})$ *and* $C^+(\mathfrak{q})$ *belong to* $H^+(D)^8$;
(c) *both* $\mathfrak{p}$ *and* $\mathfrak{q}$ *split completely in* K_8.

Using the notation of previous sections, we obtain easily:

Lemma 5.2. *The following conditions are equivalent*:
(a) $C^+(\mathfrak{p}) \in H^+(D)^8$ (*resp.* $C^+(\mathfrak{q}) \in H^+(D)^8$);
(b) $\mathfrak{p}$ (*resp.* $\mathfrak{q}$) *splits completely in* K_8;
(c) $\hat{P}_B$ (*resp.* $\hat{Q}_A$) *splits completely in* B_4 (*resp.* A_4);
(d) $\psi_B(\hat{P}_B)=1$ (*resp.* $\psi_A(\hat{Q}_A)=1$).

If $d_1 \neq -4$, we can set

$$(\alpha) = \mathfrak{q}_A^{h(d_1)} = \hat{Q}_A^{2h(d_1)}\,, \quad (\beta) = \mathfrak{p}_B^{h(d_2)} = \hat{P}_B^{2h(d_2)}\,.$$

Hence we have:

Lemma 5.3. *If* $d_1 \neq -4$, *then*

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

Theorem 5.4. *Suppose* D *is of type* (R1) *and* $8\,|\,h^+(D)$. *Then we have*
(a) $4\,||\,h(D)$ *if and only if* $\left(\frac{z}{p}\right)_4\left(\frac{x}{q}\right)_4 = -1$;

$\left(\frac{z}{p}\right)_4 = 1$ *and* $\left(\frac{x}{q}\right)_4 = -1$ *if and only if* $\mathfrak{p} \approx 1$ *and* $\mathfrak{q} \not\approx 1$;

$\left(\frac{z}{p}\right)_4 = -1$ *and* $\left(\frac{x}{q}\right)_4 = 1$ *if and only if* $\mathfrak{p} \not\approx 1$ *and* $\mathfrak{q} \approx 1$;

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

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

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

$$\psi_B(\hat{P}_B) = \psi_B(\hat{P}_B)^{h(q)} = \psi_B((\sqrt{\beta})) = \left(\frac{\sqrt{\beta}}{P_B}\right) sgn\, N_{B_2}\sqrt{\beta}\,,$$
$$\left(\frac{\sqrt{\beta}}{P_B}\right) = \left(\frac{\beta}{P_B}\right)_4 = \left(\frac{\beta}{\mathfrak{p}_B'}\right)_4 = \left(\frac{\beta+\beta'}{\mathfrak{p}_B'}\right)_4 = \left(\frac{z}{p}\right)_4, \quad \text{and}$$
$$N_{B_2}\sqrt{\beta} = N_B(-\beta) = \beta\beta' = p^{h(q)} > 0\,.$$

Hence $\psi_B(\hat{P}_B)=\left(\frac{z}{p}\right)_4$. We obtain $\psi_A(\hat{Q}_A)=\left(\frac{x}{q}\right)_4$ similarly. On the other hand, as $N_K\varepsilon_D=1$, we have either $\mathfrak{p}\approx 1$ and $\mathfrak{q}\not\approx 1$ or $\mathfrak{p}\not\approx 1$ and $\mathfrak{q}\approx 1$. 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

$$\psi_B(\hat{P}_B) = \psi_B((\sqrt{\beta})) = \left(\frac{\sqrt{\beta}}{P_B}\right) = \left(\frac{\beta}{P_B}\right)_4 = \left(\frac{z}{p}\right)_4,$$
$$\psi_A(\hat{Q}_A) = \psi_A((\sqrt{\alpha})) = \left(\frac{\sqrt{\alpha}}{Q_A}\right) = \left(\frac{\alpha}{Q_A}\right)_4 = \left(\frac{x}{q}\right)_4.$$

If $8\,||\,h(D)$ and $N_K\varepsilon_D=-1$, we have $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$, 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 $\psi_B(\hat{P}_B)=\psi_A(\hat{Q})=1$. Q.E.D.

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

(a) $4\,||\,h(D)$ *if and only if* $\left(\frac{z-2^{h(q)}}{2}\right)_4\left(\frac{x}{q}\right)_4=-1$;

$\left(\frac{z-2^{h(q)}}{2}\right)_4 = 1$ *and* $\left(\frac{x}{q}\right)_4 = -1$ *if and only if* $\mathfrak{p}\approx 1$ *and* $\mathfrak{q}\not\approx 1$;

$\left(\frac{z-2^{h(q)}}{2}\right)_4 = -1$ *and* $\left(\frac{x}{q}\right)_4 = 1$ *if and only if* $\mathfrak{p}\not\approx 1$ *and* $\mathfrak{q}\approx 1$;

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

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

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

$$\psi_B(\hat{P}_B) = \psi_B((\sqrt{\beta})) = \left(\frac{\sqrt{\beta}\,,2}{P_B}\right) sgn\, N_{B_2}\sqrt{\beta}$$
$$= \left(\frac{\sqrt{\beta}\,,2}{P_B}\right) = \left(\frac{\beta}{\mathfrak{p}_B'}\right)_4,$$

where $\left(\frac{\beta}{\mathfrak{p}'_B}\right)_4=1$ if $\beta\equiv 1 \pmod{\mathfrak{p}'^4_B}$ and $\left(\frac{\beta}{\mathfrak{p}'_B}\right)_4=-1$ if $\beta\equiv 9 \pmod{\mathfrak{p}'^4_B}$. Since $\beta\equiv 1 \pmod{\mathfrak{p}'^3_B}$ and $\beta'\not\equiv 1 \pmod{\mathfrak{p}'_B}$, we see that $\beta\equiv 1 \pmod{\mathfrak{p}'^4_B}$ if and only if $(\beta-1)(\beta'-1)=2^{h(q)}-z+1\equiv 0 \pmod{16}$, so that $\psi_B(\hat{P}_B)=\left(\frac{z-2^{h(q)}}{2}\right)_4$. 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* (I1) *and* $8\,|\,h(D)$, *then*

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

where x is a rational integer satisfying the conditions (c), (d) (I1)** *of proposition* 2.13.

Proof. Since $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$, it follows from proposition 5.1 and lemma 5.2 that $\psi_B(\hat{P}_B)=\psi_A(\hat{Q}_A)=(-1)^{h(D)/8}$. By proposition 4.7 and lemma 5.3, $\psi_A(\hat{Q}_A)=\psi_A((\sqrt{\alpha}))=\left(\frac{\sqrt{\alpha}}{Q_A}\right)=\left(\frac{\alpha}{Q_A}\right)_4=\left(\frac{x}{q}\right)_4$. Q.E.D.

Theorem 5.7. *Suppose D is of type* (I2) *and* $8\,|\,h(D)$, *then*

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

where x is a rational integer satisfying the conditions (c), (d) (I2)** *of proposition* 2.13.

Proof. Since $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$, it follows from proposition 5.1 and lemma 5.2 that $\psi_B(\hat{P}_B)=\psi_A(\hat{Q}_A)=(-1)^{h(D)/8}$. By proposition 4.8 and lemma 5.3, we have $\psi_A(\hat{Q}_A)=\psi_A((\sqrt{\alpha}))=\left(\frac{\sqrt{\alpha},2}{Q_A}\right)$, and we deduce that $\left(\frac{\sqrt{\alpha},2}{Q_A}\right)=\left(\frac{x-2^{h(-p)}}{2}\right)_4$ as in the proof of theorem 5.5. Q.E.D.

Theorem 5.8. *Suppose D is of type* (I3) *and* $8\,|\,h(D)$, *then*

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

where x is a rational integer satisfying the conditions (c), (d) (I3)** *of proposition* 2.13.

Proof. Since $\mathfrak{p}\approx\mathfrak{q}\not\approx 1$, we have $\psi_B(\hat{P}_B)=\psi_A(\hat{Q}_A)=(-1)^{h(D)/8}$. By proposition 4.9, we have $\psi_A(\hat{Q}_A)=\psi_A((\sqrt{\alpha}))=\left(\frac{\sqrt{\alpha}}{Q_A}\right)=\left(\frac{\alpha}{Q_A}\right)=\left(\frac{2x}{q}\right)_4$. Q.E.D.

For discriminants of type (I4), 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

$$K_4 = K_2(\sqrt{\varepsilon_q}) = \boldsymbol{Q}(\sqrt{-1}, \sqrt{\varepsilon_q}),$$

where $\varepsilon_q = T + U\sqrt{q} > 1$ is the fundamental unit of B. The field K_8 has been explicitly constructed by H. Cohn and G. Cooke [4] (cf. also [10]):

Lemma 6.1 (Cohn-Cooke).

$$K_8 = K_4(\sqrt{(f+\sqrt{-q})(1+\sqrt{-1})\sqrt{\varepsilon_q}}),$$

where e and f are rational integral solutions of

$$-q = f^2 - 2e^2;\ e > 0,\ f \equiv -1 \pmod 4. \tag{6.2}$$

We let $\lambda = (f+\sqrt{-q})(1+\sqrt{-1})\sqrt{\varepsilon_q}$, so that $K_8 = K_4(\sqrt{\lambda})$. As P_B is ramified in K_4, we have $P_B = \mathcal{P}^2$ where $\mathcal{P}$ is a prime ideal of K_4. It is easy to see that the completion of K_4 at $\mathcal{P}$ is isomorphic to $\boldsymbol{Q}_2(\sqrt{-1})$ and we may fix the isomorphism by taking

$$\sqrt{q} \equiv \frac{q+1}{2} \pmod{\mathfrak{p}_B'^3} \quad\text{and}\quad \sqrt{\varepsilon_q} \equiv \frac{\varepsilon_q+1}{2} \pmod{P_B^3}. \tag{6.3}$$

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

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

$$\mu \in O_{\mathcal{P}}^{\times 2} \text{ if and only if } \mu \equiv \pm 1 \pmod{\mathcal{P}^5}.$$

As $\lambda/\pi^2 \in O_{\mathcal{P}}^{\times}$, we have

Lemma 6.5. *The following conditions are equivalent*:

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

(b) *$\mathcal{P}$ splits completely in K_8*;

(c) $\lambda/\pi^2 \equiv \pm 1 \pmod{\mathcal{P}^5}$.

By simple calculations we have:

Lemma 6.6. (a) $f \equiv -\dfrac{q+1}{2} \pmod 8$;

(b) $\dfrac{f+\sqrt{-q}}{\pi} \equiv -\dfrac{q+1}{2} \pmod{\mathcal{P}^5}$.

Theorem 6.7 (Williams [17]). *Suppose D is of type* (I4) *and* $8|h(D)$. *Then* $16|h(D)$ *if and only if* $T\equiv q-1 \pmod{16}$, *equivalently,* $(-1)^{T/8}\left(\frac{q}{2}\right)_4=(-1)^{h(D)/8}$, *where* $\varepsilon_q=T+U\sqrt{q}>1$ *is the fundamental unit of* $\boldsymbol{Q}\sqrt{(q)}$.

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

$$\lambda/\pi^2=\frac{f+\sqrt{-q}}{\pi}\sqrt{\varepsilon_q}\equiv-\frac{q+1}{2}\frac{\varepsilon_q+1}{2} \pmod{\mathcal{P}^5},$$

and so $\lambda/\pi^2\equiv\pm1 \pmod{\mathcal{P}^5}$ if and only if

$$\frac{\varepsilon_q+1}{2}\equiv\pm\frac{q+1}{2} \pmod{\mathcal{P}^5}. \tag{6.8}$$

As $q\equiv1 \pmod 8$ and $\varepsilon_q\equiv1 \pmod{\mathfrak{p}_B'^3}$, that is, $q\equiv\varepsilon_q\equiv1 \pmod{\mathcal{P}^6}$, we obtain (6.8) if and only if $\varepsilon_q\equiv q \pmod{\mathcal{P}^7}$, that is, if and only if $\varepsilon_q\equiv q \pmod{\mathfrak{p}_B'^4}$. It follows from lemma 6.5 that $16|h(D)$ if and only if $\varepsilon_q\equiv q \pmod{\mathfrak{p}_B'^4}$. Since $\varepsilon_q\equiv1 \pmod{'^3_B}$ and $\varepsilon_q\equiv-1 \pmod{\mathfrak{p}_B^2}$, we have $\varepsilon_q\equiv1 \pmod{\mathfrak{p}_B'^4}$ if and only if $(\varepsilon_q-1)(\varepsilon_q'-1)=2T\equiv0 \pmod{32}$. Hence we deduce $\varepsilon_q-1\equiv T \pmod{\mathcal{P}_B'^4}$.

Q.E.D.

References

[1] P. Barrucand and H. Cohn: *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70.

[2] E. Brown: *The class number of* $\mathbf{Q}(\sqrt{-p})$, *for* $p\equiv1$ (mod 8) *a prime*, Proc. Amer. Math. Soc. **31** (1972), 381–383.

[3] J. Bucher: *Neues über die Pell'schen Gleichung,* Naturforschende Gesellschaft Mitteilungen Luzern **14** (1943), 1–18.

[4] H. Cohn and G. Cooke: *Parametric form of an eight class field,* Acta Arith. **30** (1976), 367–377.

[5] H. Hasse: *Uber die Klassenzahl sәp Körpers* $\boldsymbol{P}(\sqrt{-2p})$ *mit einer Primzahl* $p\neq2$, J. Number Theory **1** (1969), 231–234.

[6] H. Hasse: *Uber die Klassenzahl des Körpers* $\boldsymbol{P}(\sqrt{-p})$ *mit einer Primzahl* $p\equiv1$ mod. 2^3, Aequationes Math. **3** (1969), 165–169.

[7] H. Hasse: *Uber die Teilbarkeit durch* 2^3 *der Klassenzahl imaginär-quadratischer Zahlkorper mit genau zwei verschiedenen Diskriminantenprimteilern,* J. Reine Angew. Math. **241** (1970), 1–6.

[8] H. Hasse: *Uber die Teilbarkeit durch* 2^3 *der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Discriminantenprimteilern,* Math. Nachr. **46** (1970), 61–70.

[9] P. Kaplan: *Divisibilité par* 8 *du nombre des classes des corps quadratiques dont le* 2*-groupe des classes est cyclique, et réciprocité biquadratique,* J. Math. Soc. Japan **25** (1973), 596–608.

[10] P. Kaplan: *Unité de norme* -1 *du* $\boldsymbol{Q}(\sqrt{p})$ *et corps de classes de degré* 8 *de* $\boldsymbol{Q}(\sqrt{-p})$ *ou p est un nombre premier congru à* 1 *modulo* 8, Acta Arith. **32** (1977), 239–243.

[11] E. Lehmer: *On the quadratic character of some quadratic surds,* J. Reine Angew. Math. **250** (1971), 42–48.

[12] L. Rédei: *Uber die Grundeinheit und die durch* 8 *teilbaren Invarianten der absoluten Klasseengruppe im quadratischen Zahlkörpers,* J. Reine Angew. Math. **171** (1934), 131–148.

[13] L. Rédei und H. Reichardt: *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers,* J. Reine Angew. Math. **170** (1933), 69–74.

[14] H. Reichardt: *Zur Struktur der absoluten Ioealklassengruppe im quadratischen Zahlkörper,* J. Reine Angew. Math. **170** (1933), 75–82.

[15] H. Reichardt: *Uber die 2-Klassengruppe gewisser quadratischer Zahlkörper,* Math. Nachr. **46** (1970), 71–80.

[16] C.L. Siegel: Lectures on advanced analytic number theory, Bombey, 1961.

[17] K.S. Williams: *On the class number of* $\boldsymbol{Q}(\sqrt{-p})$ *modulo* 16, *for* $p \equiv 1$ (mod 8) *a prime,* Acta Arith. **34** (1981), 381–398.

[18] Y. Yamamoto: 16-*divisibilities of class numbers of quadratic fields,* RIMS Kokyuroku **378** (1980), 82–87. (in Japanese)

[19] Y. Yamamoto: *On the 2-parts of class numbers of quadratic fields,* Report of symposium on group theory and its applications held at Osaka Univ. (1981), 66–74. (in Japanese)

Department of Mathematics
Osaka University
Toyonaka, Osaka 560, Japan