

REAL QUADRATIC NUMBER FIELDS WITH 2-CLASS GROUP OF TYPE (2, 2)

ELLIOT BENJAMIN AND C. SNYDER

Abstract.

Let k be a real quadratic number field with the 2-Sylow subgroup of its ideal class group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and with discriminant divisible by a prime congruent to 3 mod 4. We use graph theory to describe the structure of the Galois group of the second 2-Hilbert class field of k over k .

§ 1. Introduction.

Let k be an algebraic number field and Cl_k its ideal class group in the wider sense. Suppose K is a finite algebraic extension of k . Then there is a canonical homomorphism

$$j: Cl_k \rightarrow Cl_K$$

obtained by extending the ideals of k to K . Then $\ker j$ consists of those ideal classes in k which become principal, i.e., capitulate, in K . One of the main goals in capitulation theory is to explicitly determine $\ker j$. Let k_1 denote the 2-Hilbert class field of k , i.e., k_1 is the maximal abelian extension of k which is unramified at all the (finite and infinite) primes of k and such that $[k_1 : k]$ is a power of 2. Let $k_2 = (k_1)_1$ and let $G = \text{Gal}(k_2/k)$. Also let $Cl_{k,2}$ be the 2-Sylow subgroup of Cl_k . If $Cl_{k,2}$ is isomorphic to the (Klein) four group, then it is well-known, [5], [12], that G is one of five types of groups:

- | | |
|---|-------------------|
| 1. Abelian | (A) |
| 2. quaternion of order 8 | (Q) |
| 3. generalized quaternion (of order > 8) | (Q _g) |
| 4. dihedral | (D) |
| 5. semidihedral | (S) |

The object of this paper is to classify G when k is a real quadratic number field with discriminant, D , divisible by a prime congruent to 3 mod 4. This is accomplished by determining the capitulation of the ideal classes of k in each of the three

unramified quadratic extensions of k . In light of [8] and [4], this project completes this classification problem for all quadratic fields with $Cl_{k,2}$ isomorphic to the four group.

§ 2. Preliminaries.

Let Q_m , D_m , and S_m denote the quaternion, dihedral, and semidihedral groups, respectively, of order 2^m , where $m \geq 3$ and $m \geq 4$ for S_m . Notice that $Q_3 = Q$ and $Q_m = Q_g$ for $m > 3$. In addition to these we let A (or A_4) be the four group. Each of these groups is generated by two elements, x and y , with the following presentations:

$$\begin{aligned} x^{2^{m-2}} = y^2, y^4 = 1, y^{-1}xy = x^{-1} & \quad \text{for } Q_m. \\ x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{-1} & \quad \text{for } D_m. \\ x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{2^{m-2}-1} & \quad \text{for } S_m. \\ x^2 = y^2 = 1, y^{-1}xy = x & \quad \text{for } A. \end{aligned}$$

Let $H_1 = \langle x \rangle$, $H_2 = \langle x^2, y \rangle$, $H_3 = \langle x^2, xy \rangle$ be the three maximal subgroups in each of these groups. In Q and A each H_i is cyclic. In D_m ($m > 3$), H_2 and H_3 are also dihedral. In Q_g , H_2 and H_3 are quaternion. Finally in S_m , H_2 is dihedral whereas H_3 is quaternion.

Now suppose k is a number field with $Cl_{k,2}$ isomorphic to the four group. As above, let $G = \text{Gal}(k_2/k)$. Then by Galois theory and class field theory G/G' is isomorphic to $Cl_{k,2}$. (G' denotes the commutator subgroup of G .) Thus G is of one of the five types of groups listed above. We determine the type of G by computing the order of the capitulation kernel of k in each of the three unramified quadratic extensions of k and according as each satisfies Tausky's condition A or B . Recall, [12], that if K/k is an unramified extension, then

$$K/k \text{ satisfies condition } A \text{ iff } |\ker j \cap N_{K/k}(Cl_K)| > 1$$

$$K/k \text{ satisfies condition } B \text{ iff } |\ker j \cap N_{K/k}(Cl_K)| = 1.$$

Now, in the case that K/k is an unramified quadratic extension then $\ker j$ is known, [5], to be an elementary subgroup of $Cl_{k,2}$. Moreover $[Cl_{k,2} : N_{K/k}(Cl_K)] = 2$. Thus if K/k satisfies condition B , then $|\ker j| = 2$.

Now let F_i be the subfield of k_2 fixed by H_i ($i = 1, 2, 3$). Then F_1 , F_2 , and F_3 constitute all of the unramified quadratic extensions of k . Let $j'_i: Cl_k \rightarrow Cl_{F_i}$ be the canonical homomorphisms described earlier. Then using [8], we have the following classification of G . (If $|\ker j'_i| = 4$, we know, from the argument above, that K_i/k satisfies condition A and thus in this case we do not write anything for the condition.)

	$ \ker j'_1 (A/B)$	$ \ker j'_2 (A/B)$	$ \ker j'_3 (A/B)$	G
1.	4	4	4	A
2.	$2A$	$2A$	$2A$	\underline{Q}
3.	4	$2B$	$2B$	D
4.	$2A$	$2B$	$2B$	\underline{Q}_g
5.	$2B$	$2B$	$2B$	S

Thus by determining the order of each $\ker j_i$ and the condition (A or B) if $|\ker j'_i| = 2$, we can determine the type of G .

We now carry out this program for real quadratic number fields with discriminant divisible by a prime congruent to 3 mod 4.

§ 3. Results.

From now on, let k be a real quadratic number field with discriminant, D , divisible by a prime $\equiv 3 \pmod 4$ and with $Cl_{k,2}$ isomorphic to the four group. Then by genus theory D is divisible by exactly four distinct primes. We compile a list of possible D . In what follows we use the following notational conventions:

p_i, p will denote primes $\equiv 1(4)$

q_i, q will denote primes $\equiv 3(4)$

r, r_i will denote any primes

r^* will denote a fundamental discriminant divisible only by the prime r

i.e. $r^* = (-1)^{\frac{r-1}{2}} r$ if r is odd and $2^* \in \{8, -8, -4\}$.

Let $D = r_1^* r_2^* r_3^* r_4^*$. Then D is of one of the following types:

1. $D = q_1 q_2 q_3 q_4$; let $r_i^* = -q_i$ ($i = 1, 2, 3, 4$)
2. $D = 4q_1 q_2 q_3$; let $r_4^* = -4, r_i^* = -q_i$ ($i = 1, 2, 3$)
3. $D = 8q_1 q_2 q_3$; let $r_4^* = -8, r_i^* = -q_i$ ($i = 1, 2, 3$)
4. $D = p_1 p_2 q_1 q_2$; let $r_i^* = p_i, r_{i+2}^* = -q_i$ ($i = 1, 2$)
5. $D = 8p q_1 q_2$; let $r_1^* = 8, r_2^* = p, r_{i+2}^* = -q_i$ ($i = 1, 2$)
6. $D = 8p_1 p_2 q$; let $r_i^* = p_i, r_3^* = -q, r_4^* = -8$ ($i = 1, 2$)
7. $D = 4p_1 p_2 q$; let $r_i^* = p_i, r_3^* = -q, r_4^* = -4$ ($i = 1, 2$).

THEOREM 1. *If D is divisible by at least three primes $\equiv 3 \pmod 4$, then G is Abelian.*

PROOF. Let $D = r_1^* r_2^* r_3^* r_4^*$ where $r_i \equiv 3 \pmod 4$ for $i = 1, 2, 3$. Then $K_1 = k(\sqrt{r_1^* r_2^*})$, $K_2 = k(\sqrt{r_1^* r_3^*})$, and $K_3 = k(\sqrt{r_2^* r_3^*})$ are the three unramified quadratic extensions of k . Each of these fields contains three real quadratic subfields whose discriminants are all divisible by a prime $\equiv 3 \pmod 4$. Thus the

norms of the fundamental units of all the quadratic fields are positive. Thus by the main theorem of [1], four ideal classes in k capitulate in $K_1, K_2,$ and K_3 . Therefore G is Abelian.

Now we consider D of type 4-7, which requires more work. We first determine conditions on the primes dividing D in order for $Cl_{k,2}$ to be elementary. Since D is divisible by a prime $\equiv 3(4)$, then $Cl_{k,2}^* = \mathbb{Z}/2\mathbb{Z} \times Cl_{k,2}$ denotes the narrow class group of k , [6]. Thus $Cl_{k,2}$ is elementary iff $Cl_{k,2}^*$ is elementary. We use Redei's elementary method to determine when $Cl_{k,2}^*$ is elementary, [11], [10]. Given $D = r_1^* r_2^* r_3^* r_4^*$, let A_D be the 4×4 matrix $[a_{ij}]$ where

$$a_{ij} = \begin{cases} 1 & \text{if } \left(\frac{r_i^*}{r_j}\right) = -1 \\ 0 & \text{if not} \end{cases}$$

where $\left(\frac{a}{b}\right)$ is the Kronecker symbol. Then $Cl_{k,2}^*$ is elementary iff the rank of the matrix A is 3 where $A = [c_{ij}]$ with

$$c_{ij} = \begin{cases} a_{ji} & \text{if } i \neq j \\ \sum_{l=1}^4 a_{li} & \text{if } i = j \end{cases}$$

where c_{ij} are considered mod 2.

PROPOSITION 1. *If $D = r_1^* r_2^* r_3^* r_4^*$ is of type 4, 5 or 6, then $Cl_{k,2}$ is elementary iff*

$$\begin{aligned} & \left(\frac{r_1}{r_2}\right) = 1 \ \& \ \left[\left(\frac{r_1}{r_3}\right) = -1 \ \text{or} \ \left(\frac{r_1}{r_4}\right) = -1\right] \ \& \ \left[\left(\frac{r_2}{r_3}\right) = -1 \ \text{or} \ \left(\frac{r_2}{r_4}\right) = -1\right] \\ & \ \& \ \text{not} \ \left(\frac{r_1}{r_3}\right) = \left(\frac{r_1}{r_4}\right) = \left(\frac{r_2}{r_3}\right) = \left(\frac{r_2}{r_4}\right) \end{aligned}$$

or

$$\left(\frac{r_1}{r_2}\right) = -1 \ \& \ \text{not} \ \left(\frac{r_1}{r_3}\right) = \left(\frac{r_2}{r_3}\right) = \left(\frac{r_1}{r_4}\right) = \left(\frac{r_2}{r_4}\right).$$

PROOF. (Sketch) For D of type 4-6, we have

$$a_{ij} = \begin{cases} 1 - a_{ji} & \text{if } \{i, j\} = \{3, 4\} \\ a_{ji} & \text{if not} \end{cases}.$$

Apply the following reduction steps to A (mod 2).

- i) add rows 2, 3, 4 to row 1;
- ii) add columns 1, 2, 4 to column 3;

iii) add appropriate mult. of row 1 to other rows to obtain column 4 = $[1, 0, 0, 0]^t$;

iv) add rows 2 and 3 to row 4.

Then A is reduced to $\begin{bmatrix} 0 & 0 & 0 & 1 \\ & & 0 & 0 \\ B & & 0 & 0 \\ & & 0 & 0 \end{bmatrix}$ where $B =$

$\begin{bmatrix} a_{12} & a_{13} & a_{12} + a_{13} + a_{14} \\ a_{12} + a_{32} + a_{42} & a_{23} & a_{12} \end{bmatrix}^t$. In order that A have rank 3, B must have rank 2. There are two possibilities

Case 1: $a_{12} = 1$ in which case

$$B \neq \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}^t \text{ or } \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}^t;$$

Case 2: $a_{12} = 0$ in which case

$$B \neq \begin{bmatrix} 0 & 0 & 0 \\ * & * & 0 \end{bmatrix}^t, \begin{bmatrix} 0 & * & * \\ 0 & 0 & 0 \end{bmatrix}^t, \text{ or } \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}^t.$$

This leads directly to the desired conclusion.

PROPOSITION 2. *If D is of type 7, then $Cl_{k,2}$ is elementary iff*

$$\begin{aligned} & \left(\frac{2}{p_1} \right) = \left(\frac{2}{p_2} \right) = 1 \ \& \ \left[\left(\frac{p_1}{p_2} \right) = 1 \ \& \ \left(\frac{p_1}{q} \right) = \left(\frac{p_2}{q} \right) = -1 \right] \text{ or} \\ & \left[\left(\frac{p_1}{p_2} \right) = -1 \ \& \ \left(\left(\frac{p_1}{q} \right) = -1 \text{ or } \left(\frac{p_2}{q} \right) = -1 \right) \right] \\ \text{or} \quad & \left(\frac{2}{p_1} \right) = - \left(\frac{2}{p_2} \right) = 1 \ \& \ \left[\left(\frac{p_1}{p_2} \right) = -1 \text{ or } \left(\frac{p_1}{q} \right) = -1 \right] \\ \text{or} \quad & \left(\frac{2}{p_1} \right) = \left(\frac{2}{p_2} \right) = -1 \ \& \ \left[\left(\frac{p_1}{q} \right) = -1 \text{ or } \left(\frac{p_2}{q} \right) = -1 \right]. \end{aligned}$$

PROOF. (Sketch) We have $a_{ij} = a_{ji}$ for $i, j \in \{1, 2, 3\}$, $a_{42} = a_{41} = a_{44} = 0$ and $a_{43} = 1$. We then divide the rest into three cases:

Case 1: $a_{14} = a_{24} = 0$;

Case 2: $a_{14} = 0, a_{24} = 1$;

Case 3: $a_{14} = a_{24} = 1$.

By reducing A in each case, we find that:

in case 1, $a_{12} = a_{32} = 1$ or $(a_{12} \neq a_{32} \ \& \ a_{13} = 1)$;

in case 2, $a_{12} \leq 1$ or $a_{13} = 1$,

in case 3, $a_{13} = 1$ or $a_{23} = 1$,

from which the proposition follows.

For D of types 4-7, we make the following conventions: Let $K_1 = k(\sqrt{r_1})$, $K_2 = k(\sqrt{r_2})$, and $K_3 = k(\sqrt{r_1 r_2})$. These are the unramified quadratic extensions of k . Let $j_i: Cl_k \rightarrow Cl_{K_i}$ denote the homomorphism induced by extension of ideals from k to K_i . For each $i = 1, 2, 3$, let F_{i1} and F_{i2} be the two quadratic subfields other than k ordered so that $F_{11} = Q(\sqrt{r_1})$, $F_{21} = Q(\sqrt{r_2})$, $F_{31} = Q(\sqrt{r_1 r_2})$. Let ε be the fundamental unit (> 1) of k and ε_{ij} the fundamental unit of F_{ij} . Notice that for $i = 1, 2, 3$ the norm $N(\varepsilon_{i2}) = 1$ since the discriminant of F_{i2} is divisible by a prime $\equiv 3 \pmod{4}$. On the other hand, for $i = 1, 2$ $N(\varepsilon_{i1}) = -1$. Finally we denote by δ, δ_i ($i = 1, 2, 3$) the square-free kernel (skf) of $N(1 + \varepsilon)$, $N(1 + \varepsilon_{i2})$ ($i = 1, 2, 3$), respectively.

PROPOSITION 3. For D of types 4-7, the following holds:

For $i = 1, 2$ $|\ker j_i| = 2$ iff δ or $\delta\delta_i \in K_i^2$;

$|\ker j_3| = 2$ iff $N\varepsilon_{31} = -1$ & $(\delta$ or $\delta\delta_3 \in K_3^2)$.

PROOF. This follows at once from the theorem of [1] and properties of δ_i , [9].

Now we obtain more information about δ .

LEMMA 1. Let F be a real quadratic number field with discriminant D and let $\eta \neq 1$ be a unit of F of norm 1. Then if $e = \text{skf } N(1 + \eta)$, then $(e, D/p) = 1$ for all $p \mid D$.

(Here $(-, -/p)$ denotes the Hilbert symbol with respect to p . See e.g. [2] for its definition and properties.)

PROOF. $N(1 + \eta) = a^2 - Db^2$ for some $a, b \in \frac{1}{2}\mathbf{Z}$, not both $= 0$. Also $N(1 + \eta) = c^2e$ for some integer $c \neq 0$. Hence the equation $ex^2 + Dy^2 - z^2 = 0$ has a nontrivial solution in Q , whence in Q_p . But this implies in particular that $(e, D/p) = 1$ for all $p \mid D$.

LEMMA 2. Let F be a real quadratic number field with discriminant, D , divisible by a prime $\equiv 3 \pmod{4}$. Furthermore suppose the narrow 2-class group, $Cl_{F,2}^*$ is elementary. Let ε be the fundamental unit of F . Then $\text{skf } N(1 + \varepsilon)$ is the unique positive integer e satisfying

$$e \mid D, e \neq 1, \text{ and } (e, D/p) = 1 \text{ for all primes } p \mid D.$$

PROOF. Recall [2], that an ideal, P , of F is in the principal narrow class genus iff $(NP, D/p) = 1$ for all $p | D$. Since $Cl_{F,2}^*$ is elementary, the principal narrow class genus coincides with the principal narrow ideal class. Since D is divisible by a prime $\equiv 3 \pmod 4$, the principal narrow class (genus) contains ambiguous ideals (cf. [3] pp. 190). But the only principal ambiguous ideals are obtained from (1) , $(1 + \varepsilon)$, (\sqrt{D}) , and $(\sqrt{D})(1 + \varepsilon)$ by dividing each by the largest ideal generated by a rational integer and containing the given ideal. Since (1) and $(1 + \varepsilon)$ are the only ideals in the principal narrow class, we see if e satisfies the statement of the lemma, then $e = \text{sfk } N(1 + \varepsilon)$.

Because of Proposition 3 and Lemma 2, we need to compute the Hilbert symbols of the divisors of D . We simplify the computations by employing some graph theory.

Let D be a fundamental discriminant (not necessarily positive) of a quadratic field. Let $V(D)$, the set of vertices of D , be the set of primes, r , dividing D . Let R be the subset of $V(D) \times V(D)$ given by

$$R = \left\{ (r_1, r_2) \mid \left[\begin{matrix} r_2 \\ r_1 \end{matrix} \right] = -1 \text{ or } \left[\begin{matrix} r_1 \\ r_2 \end{matrix} \right] = -1, \text{ if } r_1 = 2 \text{ and } r_2 \equiv 3(4) \right\}.$$

Then R determines the edges of a graph with vertices $V(D)$. If (r_1, r_2) and (r_2, r_1) are in R , then we say the edge runs both ways between r_1 and r_2 and represent this by $\overset{\curvearrowright}{r_1 - r_2}$. If, however, $(r_1, r_2) \in R$ but not (r_2, r_1) , then we say the edge runs from r_1 to r_2 and denote it by $\overset{\rightarrow}{r_1 - r_2}$.

PROPOSITION 4. Suppose D is the discriminant of a quadratic number field. Let d be a positive square-free divisor of D , $d \neq 1, D$. Also let r be a prime divisor of D . Finally let $N_m = |\{q : q \text{ is prime, } q \equiv 3(4), q | m\}|$ for any positive integer m .

(1) If $D \equiv 1(2)$ or $(D \equiv 0(8) \ \& \ N_D \equiv 0(2))$, then $\left(\frac{d, D}{r}\right) = 1 \Leftrightarrow$

$$\left\{ \begin{array}{ll} \# \text{ of edges from } r \text{ into } V(d) \text{ is even} & \text{if } r \nmid d \\ \# \text{ of edges from } r \text{ into } V\left(\text{sfk}\left(\frac{D}{d}\right)\right) \text{ is} & \begin{cases} \text{even if } r | d \ \& \ (r \equiv 1(4) \text{ or } r = 2) \\ \text{odd if } r | d \ \& \ r \equiv 3(4) \end{cases} \end{array} \right.$$

(2) If $D \equiv 0(8)$ & $N_D = 1(2)$, then $\left(\frac{d, D}{r}\right) = 1 \Leftrightarrow$

$$\left\{ \begin{array}{ll} \text{same as (1)} & \text{if } r \text{ is odd} \\ \# \text{ of edges from } 2 \text{ into } V(d) \text{ is} & \begin{cases} \text{even} & \text{if } r = 2 \nmid d \text{ \& } N_d \equiv 0(2) \\ \text{odd} & \text{if } r = 2 \nmid d \text{ \& } N_d \equiv 1(2). \end{cases} \\ \# \text{ of edges from } 2 \text{ into } V\left(\text{sfk}\left(\frac{D}{d}\right)\right) \text{ is} & \begin{cases} \text{even} & \text{if } r = 2 \mid d \text{ \& } N_d \equiv 0(2) \\ \text{odd} & \text{if } r = 2 \mid d \text{ \& } N_d \equiv 1(2). \end{cases} \end{array} \right.$$

(3) If $D \equiv 4(8)$, then $\left(\frac{d, D}{r}\right) = 1 \Leftrightarrow$

$$\left\{ \begin{array}{ll} \text{same as (1)} & \text{if } r \text{ is odd} \\ N_d \equiv 0(2) & \text{if } r = 2 \nmid d \\ \# \text{ of edges from } 2 \text{ into } V(D) \text{ is} & \begin{cases} \text{even} & \text{if } r = 2 \mid d \text{ \& } N_d \equiv 0(2) \\ \text{odd} & \text{if } r = 2 \mid d \text{ \& } N_d \equiv 1(2). \end{cases} \end{array} \right.$$

PROOF. (1 & 2) Let $D = 8^a p_1 \dots p_s q_1 \dots q_t$ where $a \in \{0, 1\}$. Let $d = 2^b p_1 \dots p_u q_1 \dots q_v$ where $b \in \{0, 1\}$. If $r \neq 2$ and $r \nmid d$, then

$$\left(\frac{d, D}{r}\right) = \left(\frac{d, r}{r}\right) = \left(\frac{2}{r}\right)^b \left(\frac{p_1}{r}\right) \dots \left(\frac{p_u}{r}\right) \left(\frac{q_1}{r}\right) \dots \left(\frac{q_v}{r}\right) = 1$$

iff the number of edges from r into $V(d)$ is even. If $r = 2 \nmid d$ (so $b = 0$ and $a = 1$)

$$\begin{aligned} \left(\frac{d, D}{r}\right) &= \left(\frac{p_1, D}{2}\right) \dots \left(\frac{p_u, D}{2}\right) \left(\frac{q_1, D}{2}\right) \dots \left(\frac{q_v, D}{2}\right) \\ &= \left(\frac{2}{p_1}\right)^3 \dots \left(\frac{2}{p_u}\right)^3 \left(\frac{2}{q_1}\right)^3 (-1)^t \dots \left(\frac{2}{q_v}\right)^3 (-1)^t \\ &= \left(\frac{2}{p_1}\right) \dots \left(\frac{2}{p_u}\right) \left(\frac{2}{q_1}\right) \dots \left(\frac{2}{p_v}\right) (-1)^{vt} = 1 \end{aligned}$$

iff the number of edges from 2 into $V(d)$ is $\equiv vt \pmod{2}$.

Now suppose $r \mid d$. First suppose (without loss of generality) $r = p_1$. Then

$$\begin{aligned} \left(\frac{d, D}{r}\right) &= \left(\frac{2^b, D}{p_1}\right) \left(\frac{p_1, D}{p_1}\right) \cdots \left(\frac{p_u, D}{p_1}\right) \left(\frac{q_1, D}{p_1}\right) \cdots \left(\frac{q_v, D}{p_1}\right) \\ &= \left(\frac{2}{p_1}\right)^b \left(\frac{2}{p_1}\right)^{3a} (1) \left(\frac{p_2}{p_1}\right) \cdots \left(\frac{p_s}{p_1}\right) \left(\frac{q_1}{p_1}\right) \\ &\quad \cdots \left(\frac{q_t}{p_1}\right) \left(\frac{p_2}{p_1}\right) \cdots \left(\frac{p_u}{p_1}\right) \left(\frac{q_1}{p_1}\right) \cdots \left(\frac{q_v}{p_1}\right) \\ &= \left(\frac{2}{p_1}\right)^{3a+b} \left(\frac{p_{u+1}}{p_1}\right) \cdots \left(\frac{p_s}{p_1}\right) \left(\frac{q_{v+1}}{p_1}\right) \cdots \left(\frac{q_t}{p_1}\right) = 1 \end{aligned}$$

iff the number of edges from p_1 into $V\left(\text{sfk}\left(\frac{D}{d}\right)\right)$ is even.

Next suppose $r = q_1$. Then, arguing as above, we see

$$\left(\frac{d, D}{r}\right) = -\left(\frac{2}{q_1}\right)^{3a+b} \left(\frac{p_{u+1}}{q_1}\right) \cdots \left(\frac{p_s}{q_1}\right) \left(\frac{q_{v+1}}{q_1}\right) \cdots \left(\frac{q_t}{q_1}\right) = 1$$

iff the number of edges from q_1 into $V\left(\text{sfk}\left(\frac{D}{d}\right)\right)$ is odd.

Suppose $r = 2|d$ so $a = 1$ and $b = 1$. Then

$$\begin{aligned} \left(\frac{d, D}{2}\right) &= \left(\frac{2, D}{2}\right) \left(\frac{p_1, D}{2}\right) \cdots \left(\frac{p_u, D}{2}\right) \left(\frac{q_1, D}{2}\right) \cdots \left(\frac{q_v, D}{2}\right) \\ &= \left(\frac{2}{p_1}\right) \left(\frac{2}{p_2}\right) \cdots \left(\frac{2}{p_s}\right) \left(\frac{2}{q_1}\right) \cdots \left(\frac{2}{q_t}\right) \left(\frac{2}{p_1}\right)^3 \\ &\quad \cdots \left(\frac{2}{p_u}\right)^3 \left(\frac{2}{q_1}\right) (-1)^t \cdots \left(\frac{2}{q_v}\right) (-1)^t \\ &= (-1)^{vt} \left(\frac{2}{p_{u+1}}\right) \cdots \left(\frac{2}{p_u}\right) \left(\frac{2}{q_{v+1}}\right) \cdots \left(\frac{2}{q_t}\right) = 1 \end{aligned}$$

iff the number of edges from 2 into $V\left(\text{sfk}\left(\frac{D}{d}\right)\right) \equiv vt \pmod{2}$.

(3) Let $D = 4p_1 \dots p_s q_1 \dots q_t$. (Notice $t \equiv 1(2)$.) If r is odd then the proof is similar to the cases above. So let $r = 2$ and first suppose $2 \nmid d$, say $d = p_1 \dots p_u q_1 \dots q_v$. Then

$$\left(\frac{d, D}{r}\right) = \left(\frac{p_1, D}{2}\right) \cdots \left(\frac{p_u, D}{2}\right) \left(\frac{q_1, D}{q}\right) \cdots \left(\frac{q_v, D}{2}\right) = (-1)^{vt} = (-1)^v = 1$$

iff v is even. Finally suppose $2|d$, say $d = 2p_1 \dots p_u q_1 \dots q_v$. Then

$$\left(\frac{d, D}{r}\right) = \left(\frac{2, D}{2}\right) \left(\frac{d/2, D}{2}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_s}\right) \left(\frac{2}{q_1}\right) \cdots \left(\frac{2}{q_t}\right) (-1)^v = 1$$

iff the number of edges from 2 into $V(D)$ is $\equiv v \pmod 2$.

This result will help us determine $|\ker j_i|$ for $i = 1, 2, 3$. When $|\ker j_i| = 2$ for each i , we need to consider whether or not K_i/k satisfies condition A or B . We accomplish this with the help of the following proposition, which is proved in [13].

PROPOSITION 5. *Let F be a quadratic number field with discriminant D . Suppose $D = D_1 D_2$ is a factorization of D into relatively prime fundamental discriminants D_1 and D_2 . If $D > 0$, we further assume $D_i > 0$ for $i = 1, 2$. Let $E = F(\sqrt{D_1})$ and suppose $A = P_1 \cdots P_s$ is an ideal of F where P_i are distinct prime ideals of F such that the rational primes p_i contained in P_i divide D_1 . Then the ideal class (in the wider sense), \bar{A} , is in $N_{E/F}(Cl_E)$ iff $\left(\frac{D_2}{NA}\right) = 1$.*

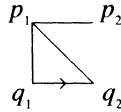
If F is a real quadratic number field with discriminant, D , divisible by a prime $\equiv 3 \pmod 4$ and such that $Cl_{F,2}$ is elementary, then each genus (in the wider sense), coincides with an ideal class (in the wider sense). Moreover each genus contains ambiguous ideals. The principal class contains only the ambiguous ideals whose norms are $1, \delta, D$, where $\delta = \text{sfk } N(1 + \varepsilon)$, ε the fundamental unit of F . See [3]. Hence there are always nonprincipal ambiguous ideals in F . For $F = k$, if $|\ker j_i| = 2$ for $i = 1, 2, 3$, then we shall find a nonprincipal ambiguous ideal whose class is in $\ker j_i$. Using Proposition 5, we determine if this class is in $N_{K_i/k}(Cl_{K_i})$ from which we can determine if K_i/k satisfies condition A or B .

§ 4. Description of Tables.

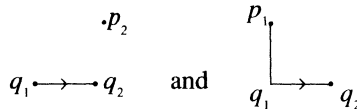
The tables at the end of paper give a complete list of real quadratic fields, k , with discriminant, D , of types 4-7 for which $Cl_{k,2}$ is elementary. The second column displays the graph of such a field. The columns headed by $\delta_0, \delta_1, \delta_2$ give the values of $\delta, \delta_1, \delta_2$ by using Proposition 4. By Lemma 2, δ is uniquely determined. However δ_1 and δ_2 may not be uniquely determined. If δ_1 or δ_2 is not uniquely determined we say that this case is a type II ambiguity. For this type of ambiguity the possible values of δ_1 or δ_2 are given as an ordered n -tuple. (Actually n is always 3). Corresponding to these values we write the type of groups of $G = \text{Gal}(k_2/k)$ in the last column by an order n -tuple. By Proposition 3 we determine $|\ker j_i|$ for $i = 1, 2, 3$ by knowledge of $\delta, \delta_1, \delta_2, \delta_3$. Notice that δ_3 is not given since δ_3 is always r_3 or r_4 . Sometimes $|\ker j_3| = 2$ or 4 depending on the sign of $N(\varepsilon_{31})$. We call these cases type I ambiguities. In such cases, the sign of $N(\varepsilon_{31})$ is given as an ordered pair $(+, -)$ in the third column and again the possible

corresponding type of groups is given in the last column as an ordered pair. If $|\ker j_i| = 2$ for $i = 1, 2, 3$ we need to check the conditions of K_i/k . This is done in columns 7, 8, 9 by finding a nonprincipal ambiguous ideal of k which becomes principal in K_i and then applying Proposition 5.

We now provide an example which shows how the tables were constructed. Consider D of type 4, case c_9 . Then $D = p_1 p_2 q_1 q_2$ and has graph



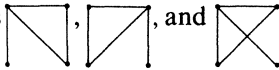
By Proposition 1, $Cl_{k,2}$ is elementary. Notice that $N(\epsilon_{31}) = -1$ since $\left(\frac{p_1}{p_2}\right) = -1$; hence we do not write anything in column 3. By using Proposition 4, we find $\delta = q_1 q_2$. By Proposition 3, since $\delta \in K_3^2$, the set of squares of K_3 , we have $|\ker j_3| = 2$. Next, to determine δ_1 and δ_2 we look at the subgraphs



respectively, and find, once again using Proposition 4, that $\delta_1 = p_2, q_1$, or $p_2 q_1$ and $\delta_2 = q_1 q_2$. Hence in the column headed δ_1 we have $(p_2, q_1, p_2 q_1)$. Now if $\delta_1 = p_2$, then $\delta \delta_1 = q_1 q_2 p_2 \in K_1^2$ implying, by Proposition 3, that $|\ker j_1| = 2$. If $\delta_1 = q_1$ or $p_2 q_1$ then $\delta, \delta \delta_1 \notin K_1^2$, implying that $|\ker j_1| = 4$. Since $\delta \delta_2 = (q_1 q_2)^2 \in K_2^2$, $|\ker j_2| = 2$. Thus in the cases $\delta_1 = q_1$ or $p_2 q_1$ we see G is dihedral (D), by the table in §2. On the other hand, if $\delta_1 = p_2$, then $|\ker j_i| = 2$ for each $i = 1, 2, 3$ and thus we need to check condition A or B for K_i/k . To this end, since $\delta = q_1 q_2$, we see that the prime ideal \mathfrak{p}_1 of k containing p_1 is nonprincipal but becomes principal in K_1 . Since the number of edges from p_1 into $V(p_2 q_1 q_2)$ in the graph of k is $= 3$ which is odd we see $\mathfrak{p}_1 \notin N_{K_1/k}(Cl_{K_1})$ by Proposition 5. Hence $\ker j_1 \cap N_{K_1/k}(Cl_{K_1})$ has only one element in it so K_1/k satisfies condition B . Similarly K_2/k satisfies condition B . Let \mathfrak{q}_1 be the prime ideal of k containing q_1 . Then \mathfrak{q}_1 is nonprincipal in k but becomes principal when extended to K_3 , since the prime of F_{32} over q_1 is principal. Since the number of edges from q_1 into $V(p_1 p_2)$ is odd we see, by Proposition 5, that K_3/k satisfies condition B . Thus G is semidihedral (S). In the last column under G we put (S, D, D) corresponding to the triple $(p_2, q_1, p_2 q_1)$ in the column headed δ_1 .

§5. More Results.


When looking at the tables we can see that the type of G is determined by the graph associated with k . We summarize this in the form of a theorem. But first we


need some terminology. If $D = r_1^* r_2^* r_3^* r_4^*$ is of type 4-7, then in the corresponding graph r_1 and r_2 are always the points on the top and r_3, r_4 those on the bottom. We shall call two graphs equivalent if we can transform one into the other by flipping the one through a vertical line through the center of the graph (thought of as a square), by twisting the one by interchanging the two top vertices, or both operations. For example, the graphs  are all equivalent.


Also by convention $\bullet \text{---} \bullet$ shall mean $\bullet \quad \bullet, \bullet \text{---} \bullet, \bullet \text{---} \bullet, \text{or} \bullet \text{---} \bullet$.


THEOREM 2. *Suppose D is of type 4, 5, 6, or 7. Then $G = \text{Gal}(k_2/k)$ can be determined in the following way.*

(1) *Unambiguous cases:*


$G = Q \Leftrightarrow$ its graph is equivalent to 

$G = A \Leftrightarrow$ its graph is equivalent to 


$G = Q_g \Leftrightarrow$ its graph is equivalent to 

$G = D \Leftrightarrow$ its graph is equivalent to 

(2) *Type I Ambiguities*


$G = D \text{ or } Q_g \Leftrightarrow$ its graph is equivalent to 

$(G = Q_g \Leftrightarrow N\epsilon_{31} = -1)$


$G = D \text{ or } Q \Leftrightarrow$ its graph is equivalent to 

$(G = Q \Leftrightarrow N\epsilon_{31} = -1)$

(3) *Type II Ambiguities*

$G = D \text{ or } S \Leftrightarrow$ its graph is equivalent to 

$(G = S \Leftrightarrow \alpha)$

$G = D$ or $Q_g \Leftrightarrow$ its graph is equivalent to 

$(G = Q_g \Leftrightarrow \beta)$.


Here α and β refer to statements involving quadratic and biquadratic residues of rational integers arising from the primes dividing the discriminant of k . These statements are rather complicated and are not given here but may be retrieved from [7]. The main point is that the statements only involve rational integers.


We may also use the graphs to determine which maximal subgroup (H_1, H_2, H_3) of G each K_i belongs to. If G is D, Q_g , or S , let K_c be the (unique) unramified quadratic extension of k such that $\text{Gal}(k_2/K_c)$ is cyclic, i.e. H_1 . Moreover if G is S let K_d be the fixed field of H_2 in k_2 (which is dihedral) and K_q be the fixed field of H_3 in k_2 (which is quaternion). Also denote by a, b, c, d the prime

divisors of D such that the associated graph has vertices $\begin{matrix} a & b \\ \cdot & \cdot \\ \cdot & \cdot \\ c & d \end{matrix}$


THEOREM 3. *Suppose D is of type 4, 5, 6, or 7. Then the following hold.*


(1) *Unambiguous cases:*

$G = Q_g$ so graph is equivalent to , then $K_c = k(\sqrt{ab})$;


$G = D$ so graph is equivalent to , then $K_c = k(\sqrt{ab})$.


(2) *Type I Ambiguities:*

$G = D$ or Q_g so graph is equivalent to 
 if $G = D$, then $K_c = k(\sqrt{a})$;
 if $G = Q_g$, then $K_c = k(\sqrt{ab})$.

$G = D$ or Q so graph is equivalent to 
 if $G = D$, then $K_c = k(\sqrt{ab})$.

(3) *Type II Ambiguities:*

$G = D$ or S so graph is equivalent to 
 if $G = D$, then $K_c = k(\sqrt{a})$;
 if $G = S$, then $K_c = k(\sqrt{a}), K_d = k(\sqrt{ab}), K_q = k(\sqrt{b})$.

$G = D$ or Q_g so graph is equivalent to 

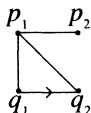
if $G = D$, then $K_c = k(\sqrt{a})$;

if $G = Q_g$, then $K_c = k(\sqrt{b})$.

PROOF. If $G = D$, then K_c corresponds to the unique K_i for which $|\ker j_i| = 4$. Checking the tables yields the result.

If $G = Q_g$, then K_c corresponds to the unique K_i for which K_i/k satisfies condition A.

If $G = S$, then each K_i/k satisfies condition B and so we cannot determine K_c , K_d , and K_q by symmetry. However, by applying the transfer maps $t_i: G/G' \rightarrow H_i/H'_i$, see [8], we see that $\ker t_1 = \ker t_3 \subseteq H_2$ (dihedral); whereas $\ker t_2 \subseteq H_3$ (quaternion). The tables then give the result. For example, consider D of type 4, Case c_9 . $D = p_1 p_2 q_1 q_2$ and the graph is



We see $\delta = q_1 q_2, \delta_1 = p_2, \delta_2 = q_1 q_2$ (we are assuming $G = S$). Then notice that if P_i is the prime ideal of k containing p_i ($i = 1, 2$) then $\bar{P}_i \in \ker j_i$ and $\bar{P}_i \neq (1)$.

Moreover $\left(\frac{q_1 q_2}{p_i}\right) = 1$. Thus $\bar{P}_i \in N_{K_3/k}(Cl_{K_3})$. Thus $K_3 = K_d$. If \mathfrak{q} is the prime






ideal of k containing q_1 then $\bar{\mathfrak{q}} \in \ker j_3$ and $\bar{\mathfrak{q}} \neq (1)$. Moreover $\left(\frac{p_2}{q_1}\right) = 1$, thus $\bar{\mathfrak{q}} \in N_{K_2/k}(Cl_{K_2})$ and so $K_2 = K_q$. By elimination $K_1 = K_c$.

D-type 4 & 5

$p_1 \cdot \dots \cdot p_2 \quad r_1 = p_1$ or $2, r_2 = p_2$ or p

Cond A/B

$q_1 \cdot \dots \cdot q_2$

cases	graph	sgn $N\epsilon_{31}$	δ_0	δ_1	δ_2	K_1	K_2	K_3	G
c_1		$(+, -)$	$r_1 r_2 q_1$	$r_2 q_1$	$r_1 q_1$	B	B	A	(D, Q_g)
c_2		$(+, -)$	q_2	q_2	q_2	B	B	A	(D, Q_g)
c_3			$r_1 q_1 q_2$	$q_1 q_2$	$r_1 q_1$				D
c_4			$r_1 q_1 q_2$	$q_1 q_2$	q_2				D
c_5			$r_1 q_1$	q_1	$r_1 q_1$				D


















c_7			$r_1 r_2 q_1$	$(r_2, q_1, r_2 q_1)$	$r_1 q_1$	A	B	B	(D, D, Q_g)
c_8			q_2	$(r_2, q_2, r_2 q_2)$	q_2	A	B	B	(D, D, Q_g)
c_9			$q_1 q_2$	$(r_2, q_1, r_2 q_1)$	$q_1 q_2$	B	B	B	(S, D, D)
c_{10}			$r_1 r_2 q_1$	$r_2 q_1$	$r_1 q_1$	A	A	A	Q
c_{11}			q_2	q_2	q_2	A	A	A	Q
c_{12}			$r_2 q_2$	$r_2 q_1$	$q_1 q_2$				A
c_{13}			$r_1 q_1$	q_2	$q_1 q_2$				A
c_{14}			$r_2 q_2$	$r_2 q_1$	q_1				A

D-type 6

$p_1 \cdot \cdot p_2$
 $2 \cdot \cdot q$

Cond A/B

cases	graph	$\text{sgn } N\epsilon_{31}$	δ_0	δ_1	δ_2	K_1	K_2	K_3	G
c_1		$(+, -)$	$2p_1 p_2$	$2p_2$	$2p_1$	B	B	A	(D, Q_g)
c_2		$(+, -)$	q	q	q	B	B	A	(D, Q_g)
c_3			$2p_1$	2	$2p_1$				D
c_4			$p_2 q$	$p_2 q$	q				D
c_5			$2p_1 q$	$2q$	$2p_1$				D
c_6			$2p_1 q$	$2q$	q				D
c_7		$(+, -)$	2	2	2	B	B	A	(D, Q_g)
c_8		$(+, -)$	$p_1 p_2 q$	$p_2 q$	$p_1 q$	B	B	A	(D, Q_g)
c_9			$2p_1 q$	$2q$	2				D

c_{10}			$2p_1q$	$2q$	p_1q				D
c_{11}			$2p_1p_2$	$2p_2$	$(2, p_1, 2p_1)$	B	A	B	(D, D, D_q)
c_{12}			q	q	(q, p_1, p_1q)	B	A	B	(Q_g, D, D)
c_{13}			2	2	$(2, p_1, 2p_1)$	B	A	B	(Q_g, D, S)
c_{14}			p_1p_2q	p_2q	(q, p_1, p_1q)	B	A	B	(D, D, Q_g)
c_{15}			$2q$	$2q$	$(2, p_1, 2p_1)$	B	B	B	(D, S, D)
c_{16}			$2q$	$2q$	(q, p_1, p_1q)	B	B	B	(D, S, D)
c_{17}			$2p_1p_2$	$2p_2$	$2p_1$	A	A	A	Q
c_{18}			q	q	q	A	A	A	Q
c_{19}			p_1q	2	$2p_1$				A
c_{20}			$2p_2$	p_2q	q				A
c_{21}			p_1q	$2q$	$2p_1$				A
c_{22}			$2p_2$	$2q$	q				A
c_{23}			2	2	2	A	A	A	Q
c_{24}			p_1p_2q	p_2q	p_1q	A	A	A	Q
c_{25}			p_2q	$2q$	2				A
c_{26}			$2p_1$	$2q$	p_1q				A









D-type 7

$p_1 \cdot \cdot p_2$

$2 \cdot \cdot q$

Cond A/B

cases	graph	sgn $N\epsilon_{31}$	δ_0	δ_1	δ_2	K_1	K_2	K_3	G
c_1			p_2	p_2	2				D
c_2			p_2	p_2	$2p_1q$				D
c_3			$2p_1q$	$2q$	2				D
c_4			$2p_2$	$2p_2$	$2p_1q$				D
c_5			p_1	$2q$	p_1				D
c_6			p_1	$2p_2$	p_1				D
c_7		(+, -)	$2p_1p_2$	$2q$	$2q$	A	A	A	(D, Q)
c_8		(+, -)	$2q$	$2p_2$	$2p_1$	A	A	A	(D, Q)
c_9		(+, -)	2	2	2	B	B	A	(D, Q_g)
c_{10}		(+, -)	$2p_1p_2q$	$2p_2q$	$2p_1q$	B	B	A	(D, Q_g)
c_{11}			p_1p_2	p_2	$(2, p_1, 2p_1)$	B	A	B	(D, Q_g, D)
c_{12}			p_1p_2	p_2	$(p_1, 2q, 2p_1q)$	B	A	B	(Q_g, D, D)
c_{13}			$2q$	$2q$	$(2, p_1, 2p_1)$	B	B	B	(D, D, S)
c_{14}			$2p_1p_2$	$2p_2$	$(p_1, 2q, 2p_1q)$	B	B	B	(D, S, D)
c_{15}			$2p_2q$	p_2	2				A
c_{16}			$2p_1$	p_2	$2p_1q$				A
c_{17}			$2p_2q$	$2q$	2				A
c_{18}			$2p_1$	$2p_2$	$2p_1q$				A

c_{19}			$2p_1$	$2q$	p_1				A
c_{20}			$2p_2q$	$2p_2$	p_1				A
c_{21}			$2p_1p_2$	$2q$	$2q$	B	B	A	Q_θ
c_{22}			$2q$	$2p_2$	$2p_1$	B	B	A	Q_θ
c_{23}			2	2	$(2, p_1, 2p_1)$	B	A	B	(Q_θ, D, D)
c_{24}			$2p_1p_2q$	$2p_2q$	$(p_1, 2q, 2p_1q)$	B	A	B	(D, D, Q_θ)
c_{25}			2	2	2	A	A	A	Q
c_{26}			$2p_1p_2q$	$2p_2q$	$2p_1q$	A	A	A	Q

REFERENCES

1. E. Benjamin, F. Sanborn and C. Snyder, *Capitulation in unramified quadratic extensions of real quadratic number fields*, Glasgow Math. J. 36 (1994), 385–392.
2. Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, London, 1967.
3. H. Cohn, *A Second Course in Number Theory*, John Wiley & Sons, New York, London, 1962.
4. R. Couture and A. Derhem, *Un problème de capitulation*, C.R. Acad. Sci. Paris 314, Série I (1992), 785–788.
5. Ph. Furtwängler, *Über die Klassenzahl abelscher Zahlkörper*, Crelle 134 (1908), 91–94.
6. D. Hilbert, *Gesammelte Abhandlungen*, Bd. 1. *Zahlentheorie*, Springer-Verlag, Berlin/New York, 1932.
7. P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, Crelle 283/284 (1974), 313–363.
8. H. Kisilevsky, *Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94*, J. Number Theory 8 (1976), 271–279.
9. T. Kubota, *Über den bzyklischen biquadratischen Zahlkörpern*, Nagoya Math. J. 10 (1956), 65–85.
10. J. Lagarias, *On Determining the 4-Rank of the ideal class group of a quadratic field*, J. Number Theory 12 (1980), 191–196.
11. L. Redei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörper*, Crelle 171 (1934), 55–60.
12. O. Taussky, *A remark on the class field tower*, J. London Math. Soc. 12 (1937), 82–85.
13. E. Benjamin, *Lower bounds on the 2-class number of the 2-Hilbert class field of imaginary quadratic fields with elementary 2-class group of rank 3*, Houston J. Math. (to appear).

DEPARTMENT OF MATHEMATICS
 UNITY COLLEGE
 UNITY, ME 04988
 U.S.A.

DEPARTMENT OF MATHEMATICS
 UNIVERSITY OF MAINE
 ORONO, ME 04469-5752
 U.S.A.