TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 347, Number 12, December 1995

ON THE IDEAL CLASS GROUP OF REAL BIQUADRATIC FIELDS

PATRICK J. SIME

ABSTRACT. We discuss the structure of the ideal class group of real biquadratic fields K, concentrating on the case that the 4-rank of the ideal class groups of the quadratic subfields of K is 0. In this case, we give estimates for the 4-rank of the ideal class group of K. As an example, let $K = \mathbb{Q}(\sqrt{p}, \sqrt{627})$, where p is a prime satisfying certain congruence conditions. The 2-primary part of the ideal class group of K is then isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$, $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, or $(\mathbb{Z}/2\mathbb{Z})^4$. Further, each of the above occurs infinitely often.

INTRODUCTION

Let $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a real biquadratic field with quadratic subfields k_0, k_1, and k_2. In the 1920's, Herglotz [He] proved a relationship between the class number of K and the class numbers of its quadratic subfields. Let h be the class number of K, and let h_i be the class number of k_i for $i = 0, 1, 2$. Herglotz showed that $h = \frac{1}{n}h_0h_1h_2$, where $n =$ 1, 2, or 4 depending on the group of units of O_K, the ring of integers of K. It is natural to ask if the structure of the ideal class group of K is reflected by this formula.

To be more precise, let G be the ideal class group of K, and let G_i be the ideal class group of k_i for $i = 0, 1, 2$. There is a natural map $G_0 \times G_1 \times G_2 \to G$. Herglotz's formula suggests that G might be isomorphic to a quotient of $G_0 \times G_1 \times G_2$. Kubota, in [Kub], showed that the kernel and cokernel of the above map are elementary 2-groups, so it suffices to consider the 2-class group of K (i.e., the 2-primary subgroup of the ideal class group). We concentrate on the case where the 2-class groups of the quadratic subfields are elementary 2-groups, since interesting phenomena already occur here. In this case, one can ask whether the 2-class group of G might be an elementary 2-group as well. For this, we need the following definition. Let n be an integer greater than 1 and let A be a finite abelian group, and let $\bar{A}$ be the maximal quotient group which is a direct product of copies of $\mathbb{Z}/n\mathbb{Z}$. The n-rank of A is the number of copies of $\mathbb{Z}/n\mathbb{Z}$ in $\bar{A}$. Since the cokernel of the above map is an elementary 2-group, the 8-rank of G is 0. Thus, it suffices to consider the 4-rank. We show that the 4-rank of G can be greater than 0. In fact, the 4-rank can vary as much as possible. For example, consider $K = \mathbb{Q}(\sqrt{p}, \sqrt{627})$, where p is a prime that satisfies certain congruence conditions. For such primes, the 2-class groups of the quadratic subfields are elementary 2-groups. Also, $h = 16c$, where c is an odd integer. From the above comments, the 2-class group of K can be either

Received by the editors July 23, 1992 and, in revised form, October 31, 1994.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R16, 11R29.

$(\mathbb{Z}/4\mathbb{Z})^2$, $\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/2\mathbb{Z})^2$, or $(\mathbb{Z}/2\mathbb{Z})^4$. We show that each of these cases occurs infinitely often, and examples are provided for each case.

Let K be any real biquadratic field where the ramified prime ideals of its quadratic subfields generate the 2-class groups of the quadratic subfields. In this case, the 2-class groups are elementary 2-groups. We introduce an elementary 2-group H and let H' be a subgroup of H satisfying certain conditions relating to the ramified prime ideals, in the sense of Definition 2.2, of the quadratic subfields. Let s be the 2-rank of H/H'. We show that the 4-rank of the ideal class group of K is either s or $s-1$. Now suppose $K=\mathbb{Q}(\sqrt{p}, \sqrt{d})$, where p is a prime. Let $d=\prod_{i=1}^{n} q_i$ where q_i is prime for each i. Let $\mathfrak{p}_{q_i}$ be a prime ideal of $\mathbb{Q}(\sqrt{d})$ lying over q_i for each i, and let G_1' be the subgroup of G_1 generated by the ideals $\mathfrak{p}_{q_i}$ such that $(\frac{p}{q_i})=1$. We show that if r is the 4-rank of G and r' is the 2-rank of G_1/G_1', then $r'-3\le r\le r'+1$.

We now give a short description of the contents of this paper. We discuss real quadratic fields k, in §2. We give a sufficient condition for when the 2-class group of k is an elementary 2-group, and also define the genus characters of k. Moreover, we determine which products of ramified prime ideals of k are principal. In §3, we consider real biquadratic fields K. We state Herglotz's Theorem. Then we give all the possibilities for the generators of the units of O_K as in [Kur]. We also show which ideals of K that are products of ramified prime ideals of k_0, k_1, and k_2 become principal in K. We also discuss the map $G_0\times G_1\times G_2\to G$ mentioned above.

In §4, we define the group H, which is the group of equivalence classes of primes that split completely in K under a certain equivalence relation. In §4 and §5, the two theorems mentioned above, which give estimates for the 4-rank of G, are proved. In §6, we show that there are infinitely many fields K with 2-class groups isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$, $\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/2\mathbb{Z})^2$, and $(\mathbb{Z}/2\mathbb{Z})^4$, and give examples of each possibility.

1. Some notation

Let L be a number field. We will denote the ring of integers of L by O_L. Unless otherwise specified, we will write ideal of L to mean fractional ideal of O_L. Recall that the ideal class group of L is the group of ideals of L modulo the principal ideals. In the nineteenth century, it was proved that the ideal class group of any number field is finite. Its order is called the class number of L. Let M a finite normal extension field of L, α an element of M, and I, J ideals of L. Further, let c, d, m, n be integers, with d odd and $(c,d)=1$. We shall use the following notations:

$[I]_L$	ideal class of I in O_L
$I\sim_L J$	I and J belong to same ideal class in O_L
$I\approx_L J$	$[IJ^{-1}]_L$ has odd order in the ideal class group of L
$\Vert I\Vert$	order of the quotient ring O_L/I
$N_{M/L}(\alpha)$	norm of α for M over L
$\mathrm{Gal}(M/L)$	Galois group of M over L
$m=_2 n$	mn is a square rational integer
R^*	group of units of a ring R

$(\frac{c}{d})$ Jacobi symbol of c modulo d

For convenience, if c is an odd integer, we will define $(\frac{c}{2})$ to be $(\frac{2}{c})$. If M is an abelian extension of L, and I is a product of prime ideals that do not ramify in M, we denote by $\mathrm{Fr}_I^{M/L}$ the Frobenius automorphism of M/L of the ideal I. See [Ma] for more on Frobenius automorphisms.

Recall that a number field K is a biquadratic field if K is an extension of degree 4 over $\mathbb{Q}$ of the form $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, where a and b are distinct squarefree integers. The field K has three quadratic subfields and $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. We call a field E a polyquadratic field if it is obtained by adjoining square roots of finitely many integers.

2. Real quadratic fields

First, we give two definitions.

Definition 2.1. Let F be a finite abelian extension of $\mathbb{Q}$. The *genus field* of F is the maximal field contained in the Hilbert class field of F that is abelian over $\mathbb{Q}$.

Definition 2.2. A prime ideal $\mathfrak{p}$ of a quadratic field k is called *ramified* if $\mathfrak{p}$ lies over a prime p that ramifies in k. An ideal, not necessarily prime, of k is a *ramified ideal* if it is a product of powers of ramified prime ideals.

Let k be a real quadratic field with Hilbert class field M and let E be the genus field of k. By genus theory, E is a polyquadratic field and the 2-ranks of $\mathrm{Gal}(M/k)$ and $\mathrm{Gal}(E/k)$ are equal. For more on genus theory, see [Ja]. We provide a sufficient condition for E to be the Hilbert 2-class field of k.

Proposition 2.3. *Let $k = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Let G be the 2-ideal class group of k. Let E be the genus field of k, and let $G' = \mathrm{Gal}(E/k)$. If $\{\mathrm{Fr}_{\mathfrak{p}}^{E/k} | \mathfrak{p}$ is a ramified prime ideal of $k\}$ generates G', then $G \cong G'$ and E is the Hilbert 2-class field of k.*

Proof. By genus theory, $G^2 \cong \mathrm{Gal}(F/E)$, where F is the Hilbert 2-class field of k. The elements of order 2 in G generate G/G^2. By a result in group theory, G is an elementary 2-group. ■

Let $k = \mathbb{Q}(\sqrt{d})$ with d squarefree. Write $d = 2^e \prod_{i=1}^n p_i$, where the p_i are distinct odd primes and $e = 0$ or 1. Let m be the number of primes congruent to 1 modulo 4. Arrange the primes p_i so that $p_i \equiv 1 \pmod 4$ for $i \le m$ and $p_i \equiv 3 \pmod 4$ for $i > m$. We classify real quadratic fields into 6 different classes:

Case A	$e = 0, m = n$
Case B	$e = 0, n - m$ odd
Case C	$e = 0, n > m, n - m$ even
Case D	$e = 1, m = n$
Case E	$e = 1, n - m$ odd
Case F	$e = 1, n > m, n - m$ even

The discriminant of k for Cases A and C is d, otherwise the discriminant is $4d$. Also, the genus field E of k is generated by $\sqrt{p_i}$ for all $i \leq m$, and $\sqrt{p_i p_j}$ for all $i, j > m$ over k.

We now define genus characters for k. Let I be an ideal of k, and let d' be a squarefree integer such that $\sqrt{d'} \in E$. It follows that $d'|d$. We define $\chi^k_{d'}(I)$ as follows:

$$\mathrm{Fr}_I^{E/k}(\sqrt{d'}) = \chi^k_{d'}(I)\sqrt{d'}.$$

It follows from the properties of the Frobenius automorphisms that if J is another ideal of k and d'' is another square free integer such that $\sqrt{d''} \in E$, then $\chi^k_{d'}(IJ) = \chi^k_{d'}(I)\chi^k_{d'}(J)$ and $\chi^k_{d'd''}(I) = \chi^k_{d'}(I)\chi^k_{d''}(I)$. If I is a principal ideal, then the value of all the genus characters at I is 1. If $I \approx_k J$, then the values of any genus character at I and J are equal.

Let l be a prime. If l is inert in k, then $\mathfrak{p}_l$ is clearly a principal ideal of k. Thus, the values of all the genus characters at $\mathfrak{p}_l$ are 1. The following two lemmas describe the values of the genus characters at $\mathfrak{p}_l$ when l splits or ramifies in k. They both follow from the relation between the genus characters, the Jacobi symbol, and the Hilbert symbol as described in [Ha1] and [Ha2]. Proofs are also given in [Si].

Lemma 2.4. *Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field as above and suppose l is a prime that splits in k. Let $\mathfrak{p}_l$ be a prime ideal of k lying above l. Let d' be a squarefree integer such that $\sqrt{d'} \in E$. If l is odd, then $\chi^k_{d'}(\mathfrak{p}_l) = (\frac{d'}{l})$. If $l = 2$ and $d' \equiv 1 \pmod 4$, then $\chi^k_{d'}(\mathfrak{p}_2) = (\frac{2}{d'})$.*

Lemma 2.5. *Let k be a real quadratic field as above and suppose l is a prime that ramifies in k. Let $\mathfrak{p}_l$ be the prime ideal of k lying above l. Let d' be a squarefree integer such that $\sqrt{d'} \in E$. If l is odd, then*

$$\chi^k_{d'}(\mathfrak{p}_l) = \begin{cases} (\frac{d'}{l}), & \text{if } l \nmid d', \\ (\frac{d/d'}{l}), & \text{if } l | d'. \end{cases}$$

If $l = 2$ and $d' \equiv 1 \pmod 4$, then $\chi^k_{d'}(\mathfrak{p}_2) = (\frac{2}{d'})$.

We now want to see which of the ramified ideals of k are principal. We state the following two lemmas which are proved in [Hi, Satz 106].

Lemma 2.6. *Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with fundamental unit $\epsilon = a + b\sqrt{d}$ such that $N_{k/\mathbb{Q}}(\epsilon) = 1$. Let $\mathfrak{p}_i$ for $1 \leq i \leq \mu$ be the ramified prime ideals of k. Further, let r, s be the squarefree parts of $2(a+1)$, $2(a-1)$, respectively, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of k such that $\mathfrak{a}^2 = (r)$ and $\mathfrak{b}^2 = (s)$. Let $S = \{\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_\mu^{e_\mu} | e_i = 0, 1 \text{ for all } i\}$. Then S contains exactly 4 principal ideals, namely (1), $(\sqrt{d})$, $\mathfrak{a}$, and $\mathfrak{b}$.*

Lemma 2.7. *Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with fundamental unit ϵ such that $N_{k/\mathbb{Q}}(\epsilon) = -1$. Let $\mathfrak{p}_i$ for $i = 1, \ldots, \mu$ be the ramified prime ideals of k. Let $S = \{\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_\mu^{e_\mu} | e_i = 0, 1 \text{ for all } i\}$. Then S contains exactly 2 principal ideals, namely (1) and $(\sqrt{d})$.*

The following lemma gives a sufficient condition for when the fundamental unit of a quadratic field is not totally positive. The lemma is a consequence of [Hi, Satz 107].

Lemma 2.8. *Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field where d is a squarefree integer with no prime divisors $p \equiv 3 \pmod 4$, and let ϵ be the fundamental unit of k. Suppose the ramified prime ideals generate the 2-class group of k. Then $N_{k/\mathbb{Q}}(\epsilon) = -1$.*

3. Real biquadratic fields

We first state the following theorem, due to Herglotz [He], which relates the class number of biquadratic fields to the class numbers of its quadratic subfields.

Theorem 3.1. *Let K be a real biquadratic field with quadratic subfields k_0, k_1, k_2, and let h, h_0, h_1, h_2 be their respective class numbers. Then*

$$h = \frac{1}{4}[O_K^* : O_{k_0}^* O_{k_1}^* O_{k_2}^*]h_0 h_1 h_2.$$

We now investigate the units of the ring of integers of real biquadratic fields. Let K be a real biquadratic field with quadratic subfields k_0, k_1, and k_2. Kuroda, in [Kur, Satz 11] proved that, up to permutation of indices, there are seven possibilities for the generators of the group of units of O_K modulo $\{1, -1\}$: 1. $\epsilon_0, \epsilon_1, \epsilon_2$; 2. $\epsilon_0, \epsilon_1, \sqrt{\epsilon_2}$; 3. $\epsilon_0, \sqrt{\epsilon_1}, \sqrt{\epsilon_2}$; 4. $\epsilon_0, \epsilon_1, \sqrt{\epsilon_0\epsilon_2}$; 5. $\epsilon_0, \sqrt{\epsilon_1}, \sqrt{\epsilon_0\epsilon_2}$; 6. $\epsilon_0, \sqrt{\epsilon_0\epsilon_1}, \sqrt{\epsilon_0\epsilon_2}$; 7. $\epsilon_0, \epsilon_1, \sqrt{\epsilon_0\epsilon_1\epsilon_2}$. Furthermore, if $\sqrt{\epsilon_i} \in K$, then ϵ_i must be totally positive. If $\sqrt{\epsilon_i\epsilon_j} \in K$ for $i \neq j$, then ϵ_i and ϵ_j are totally positive. If $\sqrt{\epsilon_0\epsilon_1\epsilon_2} \in K$, then either ϵ_i is totally positive for all i or ϵ_i is not totally positive for all i. We have the following result which is proven in [Kub, Hilfssatz 4]:

Lemma 3.2. *Let η be unit of K, such that $\eta = \frac{\alpha^2}{\nu}$, where $\alpha \in K$ and $\nu \in \mathbb{Q}$. Then $\eta \in O_{k_0}^* O_{k_1}^* O_{k_2}^*$.*

We list the possibilities for splitting of primes in k_0, k_1, and k_2 which follow from investigating the Jacobi symbols. Up to permutations of indices, there are five types of splitting in k_0, k_1, and k_2.

(1) p splits in k_0, and is inert in k_1, k_2
(2) p splits in k_0, and ramifies in k_1, k_2
(3) p is inert in k_0, and ramifies in k_1, k_2
(4) p splits in k_0, k_1, k_2
(5) p ramifies in k_0, k_1, k_2

If (1), (2), or (3) occurs, then the splitting of p is clearly determined in K. Also, it follows from [Ma, Theorem 28] or by inspecting the decomposition and inertia groups of a prime p, that (4) occurs if and only if p splits completely in K, and (5) occurs if and only if p ramifies completely in K.

We now prove the following lemma:

Lemma 3.3. *Let l be a prime which splits completely in K. Let $\mathscr{P}$ be a prime ideal of K lying over l. Then $\mathscr{P}^2 \sim_K \mathfrak{b}\mathfrak{p}\mathfrak{q}$ where $\mathfrak{b}$, $\mathfrak{p}$, $\mathfrak{q}$ are prime ideals of k_0, k_1, k_2, respectively, lying over l and below $\mathscr{P}$.*

Proof. Suppose l splits completely in K. Then $lO_{k_0} = \mathfrak{b}\mathfrak{b}'$, $lO_{k_1} = \mathfrak{p}\mathfrak{p}'$, and $lO_{k_2} = \mathfrak{q}\mathfrak{q}'$, where $\mathfrak{b}$, $\mathfrak{b}'$, $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{q}$, and $\mathfrak{q}'$ are all prime ideals lying over l. Let $\mathscr{P}$, $\mathscr{P}'$, $\mathscr{P}''$, and $\mathscr{P}'''$ be the prime ideals of K lying over l. Since

Gal$(K/\mathbb{Q})$ acts transitively on these ideals, we may assume without loss of generality that $\mathscr{P}\mathscr{P}' = \mathfrak{b}$, $\mathscr{P}\mathscr{P}'' = \mathfrak{p}$, and $\mathscr{P}\mathscr{P}''' = \mathfrak{q}$. Then, $\mathscr{P}^2 \sim_K \mathscr{P}^2(l) = \mathscr{P}^2\mathscr{P}\mathscr{P}'\mathscr{P}''\mathscr{P}''' = \mathfrak{bpq}$. ∎

The next four lemmas will determine which ideals of the form $(I_0I_1I_2)O_K$, where I_i is a ramified ideal of k_i for $i = 0, 1, 2$, are principal ideals of K. Henceforth, if I is an ideal of a number field F and M is a field containing F, we will denote the ideal IO_M by I if no confusion will result.

Lemma 3.4. *Let p be a prime which ramifies in two quadratic fields k_1 and k_2. Let $\mathfrak{p}$, $\mathfrak{q}$ be the prime ideals lying above p in k_1, k_2, respectively. Then $(\mathfrak{pq})$ is a principal ideal in $K = k_1k_2$.*

Proof. Let k_0 be the other quadratic subfield of K. If p splits in k_0, then $(p) = \mathscr{P}_1^2\mathscr{P}_2^2$, where $\mathscr{P}_1$ and $\mathscr{P}_2$ are prime ideals of K lying above p. Thus $\mathfrak{p} = \mathfrak{q} = \mathscr{P}_1\mathscr{P}_2$ in K. Hence, $\mathfrak{pq} = (p)$.

If p is inert or ramifies in k_0, then $(p) = \mathscr{P}^2$ or $(p) = \mathscr{P}^4$, respectively, where $\mathscr{P}$ is the prime ideal of K lying above p. Now either $\mathfrak{p} = \mathfrak{q} = \mathscr{P}$, or $\mathfrak{p} = \mathfrak{q} = \mathscr{P}^2$. In either case, $\mathfrak{pq} = (p)$. ∎

Lemma 3.5. *Let K be a real biquadratic field with quadratic subfields $k_0 = \mathbb{Q}(\sqrt{d_0})$, $k_1 = \mathbb{Q}(\sqrt{d_1})$, $k_2 = \mathbb{Q}(\sqrt{d_2})$. Let $\epsilon_i = a_i + b_i\sqrt{d_i}$ be the fundamental unit of k_i for $i = 0, 1, 2$. Suppose $N_{k_i/\mathbb{Q}}(\epsilon_i) = 1$ for some i. Let c_i be the squarefree part of $2(a_i + 1)$ if $N_{k_i/\mathbb{Q}}(\epsilon_i) = 1$, otherwise let $c_i = 1$. (Note that $c_i|4d_i$.) Let*

$$S = \{\mu \in \mathbb{Z} | \mu =_2 c_0^{e_0}c_1^{e_1}c_2^{e_2}d_0^{f_0}d_1^{f_1},\ \text{with } e_i, f_i = 0, 1\}.$$

Let $\mathfrak{a} = (\mathfrak{b}_a\mathfrak{p}_b\mathfrak{q}_c)O_K$ be an ideal of K, where $\mathfrak{b}_a$, $\mathfrak{p}_b$, $\mathfrak{q}_c$ are ramified ideals of k_0, k_1, k_2, respectively, such that $\mathfrak{b}_a^2 = (a)$, $\mathfrak{p}_b^2 = (b)$, and $\mathfrak{q}_c^2 = (c)$. Then $\mathfrak{a}$ is principal in K if and only if $\mathfrak{a}^2 = (\mu)$ for some $\mu \in S$, or equivalently $abc \in S$.

Note: In particular, this shows which ramified ideals of k_i become principal in K.

Proof. ($\Leftarrow$) Suppose $\mathfrak{a}^2 = (\mu)$ for some $\mu \in S$. Then $\mu = \alpha^2c_0^{e_0}c_1^{e_1}c_2^{e_2}d_0^{f_0}d_1^{f_1}$. for some integer α. It follows that $(\alpha^{-1}\mathfrak{a})^2 = (c_0^{e_0}c_1^{e_1}c_2^{e_2}d_0^{f_0}d_1^{f_1})$, so that $\alpha^{-1}\mathfrak{a} = \mathfrak{b}_{c_0^{e_0}}\mathfrak{p}_{c_1^{e_1}}\mathfrak{q}_{c_2^{e_2}}\mathfrak{b}_{d_0^{f_0}}\mathfrak{p}_{d_1^{f_1}}$, where the ideals $\mathfrak{b}_{c_0}$, $\mathfrak{p}_{c_1}$, $\mathfrak{q}_{c_2}$, $\mathfrak{b}_{d_0}$, and $\mathfrak{p}_{d_1}$ are defined similarly to $\mathfrak{b}_a$. By Lemmas 2.6 and 2.7, the above ideals are principal. Therefore $\mathfrak{a}$ is a principal ideal of K.

($\Rightarrow$) Suppose $\mathfrak{a}$ is a principal ideal, and $\mathfrak{a}^2 = (\nu)$ where $\nu \notin S$. Let α be a generator for $\mathfrak{a}$. Then, $\alpha^2 = \nu\epsilon$ where ϵ is a totally positive unit of K. Also, by Lemma 3.2, $\epsilon \in O_{k_0}^*O_{k_1}^*O_{k_2}^*$. We may assume that $\epsilon = \epsilon_0^{g_0}\epsilon_1^{g_1}\epsilon_2^{g_2}$, where $g_i = 0$ or 1 if $N_{k_i/\mathbb{Q}}(\epsilon_i) = 1$, or $g_i = 0$ otherwise. If $N_{k_i/\mathbb{Q}}(\epsilon_i) = 1$, then $\sqrt{\epsilon_i} = u_i\sqrt{c_i} + v_i\sqrt{c_i'}$, where $u_i, v_i \in \mathbb{Q}$, c_i' is the squarefree part of $2(a-1)$, and $c_ic_i' = d_i$ or $4d_i$. It follows that $\sqrt{\nu\epsilon}\sqrt{\nu c_0^{g_0}c_1^{g_1}c_2^{g_2}} \in K$. Since $\nu \notin S$, then $\nu =_2 c_0^{g_0}c_1^{g_1}c_2^{g_2}\delta$ where δ is an integer not in S. It follows that $\sqrt{\nu c_0^{g_0}c_1^{g_1}c_2^{g_2}} \notin K$, so that $\sqrt{\nu\epsilon} \notin K$, which is a contradiction. ∎

Before we state a similar lemma for the case when $N_{k_i/\mathbb{Q}}(\epsilon_i) = -1$ for each i, we need the following lemma.

Lemma 3.6. *Let K be a real biquadratic field with quadratic subfields $k_0 = \mathbb{Q}(\sqrt{d_0})$, $k_1 = \mathbb{Q}(\sqrt{d_1})$, $k_2 = \mathbb{Q}(\sqrt{d_2})$. Let ϵ_i be the fundamental unit of k_i for $i = 0, 1, 2$. Suppose ϵ_i is not totally positive for each i. Then there exists a squarefree rational integer β dividing $\sqrt{d_0d_1d_2}$ such that $\sqrt{\beta}\sqrt{\epsilon_0\epsilon_1\epsilon_2} \in K$.*

Proof. Let $\eta = \sqrt{\epsilon_0\epsilon_1\epsilon_2}$. From [Kub, Hilfssatz 3], it follows that there exists a squarefree integer β such that $\sqrt{\beta}\eta \in K$.

Now let $\mathfrak{a} = (\sqrt{\beta}\eta)$. Then $\mathfrak{a}^2 = (\beta)$. Let p be a prime dividing β. Since β is squarefree, it follows from above that $(p) = I^2$ for some ideal I of K. Hence p is ramified in K and in one of the quadratic subfields k_i. Since $N_{k_i/\mathbb{Q}}(\epsilon_i) = -1$, the odd prime divisors of d_i are congruent to 1 modulo 4. In particular, d_i is either even or $d_i \equiv 1 \pmod 4$ for all i. Thus, $p|d_i$ and hence, $p|d_0d_1d_2$. Since β is squarefree, then $\beta|\sqrt{d_0d_1d_2}$. ■

Lemma 3.7. *Let K be a real biquadratic field with quadratic subfields $k_0 = \mathbb{Q}(\sqrt{d_0})$, $k_1 = \mathbb{Q}(\sqrt{d_1})$, $k_2 = \mathbb{Q}(\sqrt{d_2})$. Let $\epsilon_i = a_i + b_i\sqrt{d_i}$ be the fundamental unit of k_i for $i = 0, 1, 2$. Suppose ϵ_i is not totally positive for each i. Let β be a squarefree integer such that $\sqrt{\beta}\sqrt{\epsilon_0\epsilon_1\epsilon_2} \in K$. Let*

$$S = \{\mu \in \mathbb{Z} | \mu =_2 \beta^e d_0^{f_0} d_1^{f_1}, \ \textit{with } e, f_i = 0, 1\}.$$

Let $\mathfrak{a} = (\mathfrak{b}_a\mathfrak{p}_b\mathfrak{q}_c)O_K$ be an ideal of K, where $\mathfrak{b}_a, \mathfrak{p}_b, \mathfrak{q}_c$ are ramified ideals of k_0, k_1, k_2, respectively, such that $\mathfrak{b}_a^2 = (a)$, $\mathfrak{p}_b^2 = (b)$, and $\mathfrak{q}_c^2 = (c)$. Then $\mathfrak{a}$ is principal in K if and only if $\mathfrak{a}^2 = (\mu)$ for some $\mu \in S$, or equivalently, $abc \in S$.

Let G, G_0, G_1, G_2 be the ideal class groups of K, k_0, k_1, k_2, respectively. There is a natural map $\phi : G_0 \times G_1 \times G_2 \longrightarrow G$ defined by

$$\phi(([I_0]_{k_0}, [I_1]_{k_1}, [I_2]_{k_2})) = [(I_0I_1I_2)O_K]_K$$

where I_i is an ideal of k_i for $i = 0, 1, 2$. Kubota in [Kub] proved what the kernel and cokernel of this map can be.

Proposition 3.8. *The kernel and the cokernel of the natural map $\phi : G_0 \times G_1 \times G_2 \to G$ are elementary 2-groups.*

We see from the proposition that the odd part of G is determined by the odd parts of G_0, G_1, and G_2. In §4 and §5, we further investigate the 2-primary subgroup of G.

4. First theorem

As in the last section, let K be a real biquadratic field with quadratic subfields k_0, k_1, and k_2. Let G, G_0, G_1, G_2 be the ideal class groups of K, k_0, k_1, k_2, respectively, having orders h, h_0, h_1, h_2, respectively. We consider real biquadratic fields K such that the ramified prime ideals of k_i generate the 2-class groups of k_i for all $i = 0, 1, 2$. In this case, the 4-rank of G_i is 0 for each i, and it follows from Proposition 2.3 that the Hilbert 2-class field of k_i is the genus field. We want to see if the 4-rank of G is always 0, or if it is not, what the 4-rank can be.

We first state the following lemma, which is a consequence of Dirichlet's Theorem on primes in arithmetic progression.

Lemma 4.1. *Let $p_1, p_2, \ldots, p_n$ be distinct primes and for each i, let $e_i = \pm 1$ Then there exist infinitely many primes l such that $(\frac{p_i}{l}) = e_i$ for all i.*

If l is a prime, we will define $\mathfrak{b}_l, \mathfrak{p}_l, \mathfrak{q}_l$ to be prime ideals of k_0, k_1, k_2, respectively, lying over l. Let E_i be the genus field of k_i for $i = 0, 1, 2$. Let H be the set of equivalence classes of primes which split completely in K, with equivalence relation $\sim$ as follows: Let l, l' be primes which split completely in K. Then $l \sim l'$ if $\chi_{d_0'}^{k_0}(\mathfrak{b}_l) = \chi_{d_0'}^{k_0}(\mathfrak{b}_{l'})$, $\chi_{d_1'}^{k_1}(\mathfrak{p}_l) = \chi_{d_1'}^{k_1}(\mathfrak{p}_{l'})$, and $\chi_{d_2'}^{k_2}(\mathfrak{q}_l) = \chi_{d_2'}^{k_2}(\mathfrak{q}_{l'})$ for all $d_i'|d_i$ such that $\sqrt{d_i'} \in E_i$. Note that in particular, if $(\frac{p}{l}) = (\frac{p}{l'})$ for all primes p such that $p|d_0d_1d_2$, then $l \sim l'$. Suppose that the 2-Sylow subgroups of G_0, G_1, and G_2 are generated by the ramified prime ideals. Then the Hilbert 2-class field of k_i is the genus field, and G_0, G_1 and G_2 have 4-rank equal to 0. It follows from the comments in §2 that $l \sim l'$ if and only if $[\mathfrak{b}_l\mathfrak{b}_{l'}^{-1}]_{k_0}$, $[\mathfrak{p}_l\mathfrak{p}_{l'}^{-1}]_{k_1}$, $[\mathfrak{q}_l\mathfrak{q}_{l'}^{-1}]_{k_2}$ have odd order in G_0, G_1, G_2, respectively. We will denote the equivalence class of l by $[l]$.

We can define a group multiplication as follows: Let l, l' be primes which split completely in K. We set $[l][l'] = [l'']$, where l'' is a prime which splits completely in K, and $\chi_{d_0'}^{k_0}(\mathfrak{b}_l)\chi_{d_0'}^{k_0}(\mathfrak{b}_{l'}) = \chi_{d_0'}^{k_0}(\mathfrak{b}_{l''})$, $\chi_{d_1'}^{k_1}(\mathfrak{p}_l)\chi_{d_1'}^{k_1}(\mathfrak{p}_{l'}) = \chi_{d_1'}^{k_1}(\mathfrak{p}_{l''})$, and $\chi_{d_2'}^{k_2}(\mathfrak{q}_l)\chi_{d_2'}^{k_2}(\mathfrak{q}_{l'}) = \chi_{d_2'}^{k_2}(\mathfrak{q}_{l''})$ for all $d_i'|d_i$ such that $\sqrt{d_i'} \in E_i$. Such primes exist since by Lemma 4.1, there exist infinitely many primes l'' such that $(\frac{p}{l''}) = (\frac{p}{ll'})$ for all $p|d_0d_1d_2$. Further, it follows that that there are an even number of primes $p|d_i$ such that $(\frac{p}{l''}) = -1$, so that l'' splits completely in K. The identity of H is $[\hat{l}]$, where $\hat{l}$ is a prime which splits completely in K such that the value of all the genus characters at $\mathfrak{b}_{\hat{l}}$, $\mathfrak{p}_{\hat{l}}$, and $\mathfrak{q}_{\hat{l}}$ is 1. It can be shown, as suggested by David Rohrlich, that $H \cong \mathrm{Gal}(\mathscr{E}/K)$, where $\mathscr{E}$ is the genus field of K.

Again, suppose that the 2-Sylow subgroups of G_0, G_1, and G_2 are generated by the ramified prime ideals. If $[l''] = [l][l']$, then it follows that $\mathfrak{b}_{l''} \approx_{k_0} \mathfrak{b}_l\mathfrak{b}_{l'}$, $\mathfrak{p}_{l''} \approx_{k_1} \mathfrak{p}_l\mathfrak{p}_{l'}$, and $\mathfrak{q}_{l''} \approx_{k_2} \mathfrak{q}_l\mathfrak{q}_{l'}$. The converse also holds, since if $\mathfrak{b}_{l''} \approx_{k_0} \mathfrak{b}_l\mathfrak{b}_{l'}$ for example, then $\chi_{d_0'}^{k_0}(\mathfrak{b}_l)\chi_{d_0'}^{k_0}(\mathfrak{b}_{l'}) = \chi_{d_0'}^{k_0}(\mathfrak{b}_{l''})$ for all $d_0'|d_0$ such that $\sqrt{d_0'} \in E_0$.

We now prove the following theorem:

Theorem 4.2. *Let K be a real biquadratic field and assume the 2-class groups of its quadratic subfields k_0, k_1, k_2 are generated by the ramified prime ideals. Let H' be the subgroup of H defined by*

$$H' = \{[l] | \exists a, b, c \in \mathbb{Z} \text{ with } \mathfrak{b}_a \approx_{k_0} \mathfrak{b}_l, \mathfrak{p}_b \approx_{k_1} \mathfrak{p}_l, \mathfrak{q}_c \approx_{k_2} \mathfrak{q}_l, \text{ and } abc =_2 1\},$$

where $\mathfrak{b}_a, \mathfrak{p}_b, \mathfrak{q}_c$, are ramified ideals of k_0, k_1, k_2, respectively, such that $\mathfrak{b}_a^2 = (a)$, $\mathfrak{p}_b^2 = (b)$, and $\mathfrak{q}_c^2 = (c)$. Let r be the 2-rank of H/H'. Then the 4-rank of the ideal class group of K is r or $r - 1$. Furthermore, if the fundamental unit of k_i is totally positive for some i, then the 4-rank is r.

Proof. Let G be the ideal class group of K and let G_i be the ideal class group of k_i for $i = 0, 1, 2$. Let $\epsilon_i = u_i + v_i\sqrt{d_i}$ be the fundamental unit of k_i, and let c_i be the squarefree part of $2(u_i + 1)$ if $N_{k_i/\mathbb{Q}}(\epsilon_i) = 1$, otherwise, let $c_i = 1$ for $i = 0, 1, 2$. By Lemmas 2.6 and 2.7, the ideals $\mathfrak{b}_{c_0}, \mathfrak{p}_{c_1}, \mathfrak{q}_{c_2}$ are principal ideals of k_0, k_1, k_2, respectively.

Suppose $N_{k_i/\mathbb{Q}}(\epsilon_i) = 1$ for some i.

For $i \leq m$, let l_i be primes which split completely in K such that $[l_i]$ for $i \leq m$, generate H', and for $i > m$, let l_i be primes which split completely in K such that $[l_i]$ for $m+1 \leq i \leq n$ generate H'' where H'' is a subgroup of H so that $H = H' \times H''$.

Since each ideal class of K contains a prime ideal which lies over a prime that splits completely in K, it suffices to consider only those prime ideals in determining the 4-rank of G.

If l is a prime which splits completely in K, then $[l] = \prod_{j=1}^{s}[l_{i_j}]$, where $s \geq 0$, and $i_j \leq n$ for all j. By Lemma 3.3,

$$\mathscr{P}_l^2 \approx_K \mathfrak{b}_l \mathfrak{p}_l \mathfrak{q}_l \approx_K \prod_{j=1}^{s} \mathfrak{b}_{l_{i_j}} \prod_{j=1}^{s} \mathfrak{p}_{l_{i_j}} \prod_{j=1}^{s} \mathfrak{q}_{l_{i_j}} \approx_K \prod_{j=1}^{s} \mathscr{P}_{l_{i_j}}^2 .$$

Thus, $[\mathscr{P}_l]_K = \prod_{j=1}^{s}[\mathscr{P}_{l_{i_j}}]_K \gamma$, where $\gamma \in G$ has order less than or equal to 2. Thus, it suffices to consider the prime ideals $\mathscr{P}_{l_i}$ for $i \leq n$.

For $i \leq m$, we have $\mathscr{P}_{l_i}^2 \approx_K \mathfrak{b}_{l_i} \mathfrak{p}_{l_i} \mathfrak{q}_{l_i} \approx_K \mathfrak{b}_a \mathfrak{p}_b \mathfrak{q}_c$, where a, b, c divide the discriminants of k_0, k_1, k_2, respectively, and by hypothesis can be chosen so that $abc =_2 1$. Now $(\mathfrak{b}_a \mathfrak{p}_b \mathfrak{q}_c)^2 = (abc)$. Thus $\mathscr{P}_{l_i}^2$ is principal in K by Lemma 3.5.

Now consider $\prod_{j=1}^{t} \mathscr{P}_{l_{i_j}}$, with $t > 0$, and $m+1 \leq i_j \leq n$ for all j. We have

$$\prod_{j=1}^{t} \mathscr{P}_{l_{i_j}}^2 \approx_K \prod_{j=1}^{t} \mathfrak{b}_{l_{i_j}} \prod_{j=1}^{t} \mathfrak{p}_{l_{i_j}} \prod_{j=1}^{t} \mathfrak{q}_{l_{i_j}} \approx_K \mathfrak{b}_a \mathfrak{p}_b \mathfrak{q}_c ,$$

where a, b, c divide the discriminants of k_0, k_1, k_2, respectively, since the ramified ideals generate the 2-class groups of k_0, k_1, and k_2. Suppose $\mathfrak{b}_a \mathfrak{p}_b \mathfrak{q}_c$ is principal in K. Then, by Lemma 3.5, $abc =_2 c_0^{e_0} c_1^{e_1} c_2^{e_2} d_0^{f_0} d_1^{f_1}$, where $e_i, f_j = 0, 1$ for each i, j. Since $\mathfrak{b}_{c_0}$, $\mathfrak{b}_{d_0}$, $\mathfrak{p}_{c_1}$, $\mathfrak{p}_{d_1}$, and $\mathfrak{q}_{c_2}$ are principal ideals in their respective fields, it follows that $\mathfrak{b}_a \approx_{k_0} \mathfrak{b}_{a'}$, $\mathfrak{p}_b \approx_{k_1} \mathfrak{p}_{b'}$, and $\mathfrak{q}_c \approx_{k_2} \mathfrak{q}_{c'}$, where a', b', c' are the squarefree parts of $ac_0^{e_0} d_0^{f_0}$, $bc_1^{e_1} d_1^{f_1}$, $cc_2^{e_2}$, respectively. But from above, $a'b'c' =_2 ac_0^{e_0} d_0^{f_0} bc_1^{e_1} d_1^{f_1} cc_2^{e_2} =_2 1$. Since $[\prod_{j=1}^{t} l_{i_j}] \notin H'$, this is a contradiction. Therefore, $\prod_{j=1}^{t} \mathscr{P}_{l_{i_j}}^2$ is not principal in K. So by Proposition 3.8, $[\prod_{j=1}^{t} \mathscr{P}_{l_{i_j}}]_K$ has order 4 in G.

In particular, we have shown that $[\mathscr{P}_{l_i}]_K$ has order 4 in G for $m+1 \leq i \leq n$, and there are no non-trivial relations among $[\mathscr{P}_{l_i}]$, for $m+1 \leq i \leq n$. Thus, $\langle [\mathscr{P}_{l_{m+1}}], \ldots, [\mathscr{P}_{l_n}] \rangle \cong (\mathbb{Z}/4\mathbb{Z})^{n-m} = (\mathbb{Z}/4\mathbb{Z})^r$, so that the 4-rank of G is at least r. Since we have also shown for any prime ideal $\mathscr{P}$ of K, that $\mathscr{P}^2 \approx_K \prod_{j=1}^{t} \mathscr{P}_{l_{i_j}}^2$, where $m+1 \leq i_j \leq n$ for all j, then the 4-rank of G is at most r. Hence, the 4-rank of G is r.

Suppose $N_{k_i/\mathbb{Q}}(\epsilon_i) = -1$ for all i.

Let β be a squarefree integer such that $\sqrt{\beta}\sqrt{\epsilon_0 \epsilon_1 \epsilon_2} \in K$ and $\beta | \sqrt{d_0 d_1 d_2}$ as in Lemma 3.6. Also, let $\tilde{H}'$ be the subgroup of H defined by

$$\tilde{H}' = \{[l] | \exists a, b, c \in \mathbb{Z} \text{ with } \mathfrak{b}_a \approx_{k_0} \mathfrak{b}_l ,\ \mathfrak{p}_b \approx_{k_1} \mathfrak{p}_l ,\ \mathfrak{q}_c \approx_{k_2} \mathfrak{q}_l ,\ \text{and } abc =_2 1, \beta\},$$

An easy calculation shows that either $\tilde{H}' = H'$, or $|\tilde{H}'| = 2|H'|$. In either case, let $\tilde{H}''$ be a subgroup of H so that $H = \tilde{H}' \times \tilde{H}''$. It follows that the 2-rank of $\tilde{H}''$ is either r or $r-1$. Let r^* be the 2-rank of $\tilde{H}''$.

By following a similar argument as in the case above, we see that the 4-rank of G is at most r. Let l_i' for $i \le r^*$ be primes which split completely in K such that $[l_i']$ generate $\tilde{H}''$ for $i \le r^*$. Consider $\prod_{j=1}^{t} \mathscr{P}_{l'_{i_j}}$, with $t > 0$ and $i_j \le r^*$ for all j. We have as before $\prod_{j=1}^{t} \mathscr{P}_{l'_{i_j}}^2 \approx_K \mathfrak{d}_a \mathfrak{p}_b \mathfrak{q}_c$, where a, b, c divide the discriminants of k_0, k_1, k_2, respectively. Suppose $\mathfrak{d}_a \mathfrak{p}_b \mathfrak{q}_c$ is principal in K. Then by Lemma 3.7, we have $abc =_2 d_0^{f_0} d_1^{f_1} \beta^e$, where $f_i, e = 0, 1$ for each i. Thus as before, $\mathfrak{d}_a \approx_{k_0} \mathfrak{d}_{a'}$ and $\mathfrak{p}_b \approx_{k_1} \mathfrak{p}_{b'}$, where a', b' are the squarefree parts of $ad_0^{f_0}, bd_1^{f_1}$, respectively. But, $a'b'c =_2 ad_0^{f_0} bd_1^{f_1} c\beta^e =_2 1, \beta$, which again is a contradiction. Thus, the 4-rank of G is at least r^*. Hence the 4-rank of G is either r or $r-1$. ■

5. Second theorem

In this section we look at real biquadratic fields K with quadratic subfields $k_0 = \mathbb{Q}(\sqrt{p})$, $k_1 = \mathbb{Q}(\sqrt{d})$, and $k_2 = \mathbb{Q}(\sqrt{pd})$, where p is a prime and $p \nmid d$. We first classify these biquadratic fields into different classes. We classify k_1 into six different classes as in §2. Further, we classify k_0 into three classes as follows:

1. $p \equiv 1 \pmod 4$ 2. $p \equiv 3 \pmod 4$ 3. $p = 2$

Since k_2 is completely determined by k_0 and k_1, and since Cases 3D (i.e. k_0 is 3 and k_1 is D), 3E, and 3F cannot occur, this leaves us with 15 different classes.

As before, let G, G_0, G_1, and G_2 be the ideal class groups of K, k_0, k_1, k_2, respectively. We note that $|G_0|$ is odd. We further assume that the ramified prime ideals of k_i generate the 2-Sylow subgroup of G_i for $i = 1, 2$.

Let E_i be the genus field of k_i for $i = 1, 2$. It follows that E_i is the Hilbert 2-class field of k_i. Recall from §4 that if I and J are ideals of k_i and the values of all the genus characters at I and J are equal, then $I \approx_{k_i} J$. Let $\bar{G}_i$ be the quotient G_i modulo the odd part of G_i. For simplicity, we will denote $[I]_{k_i}$ to be the class of ideals J such that $J \approx_{k_i} I$. Also, $[I]_K$ will have a similar meaning.

We consider the group H discussed in §4. Let l, l' be primes which split completely in K. As before, we let $\mathfrak{p}_l, \mathfrak{q}_l$ be prime ideals of k_1, k_2, respectively, lying over l. Since $|G_0|$ is odd, it follows that $[l] = [l']$ if and only if $\mathfrak{p}_l \approx_{k_1} \mathfrak{p}_{l'}$, and $\mathfrak{q}_l \approx_{k_2} \mathfrak{q}_{l'}$. We now prove a lemma which relates the groups $\bar{G}_1$ and H.

Lemma 5.1. *Let K, $\bar{G}_1$ and H be as above. Then $H \cong \bar{G}_1$ except in cases* 2C, 2E, *and* 2F. *In those cases $|H| = 2|\bar{G}_1|$.*

Proof. We have a map $\phi : H \to G$, defined by $\phi([l]) = [\mathfrak{p}_l]_{k_1}$. Let $\mathfrak{p}$ be a prime ideal representing an ideal class of K. We may assume $\mathfrak{p}$ lies over a prime q that splits in K. Further, by Lemma 4.1, we can find a prime l such that $(\frac{q_i}{l}) = (\frac{q_i}{q})$ for all i and $(\frac{p}{l}) = 1$. Such a prime splits completely in K and $[\mathfrak{p}_l]_{k_1} [\mathfrak{p}]_{k_1}$. Thus ϕ is surjective.

We now show ϕ is an injection, except for cases 2C, 2E, and 2F. From §2 we see that $E_2 \subseteq E_1(\sqrt{p})$. Suppose l is an odd prime that splits completely in K such that $\mathfrak{p}_l \approx_{k_1} (1)$. Suppose a is a squarefree integer dividing pl such that $\sqrt{a} \in E_2$. Then using Lemma 2.4 and that $(\frac{a}{l}) = (\frac{a/p}{l})(\frac{p}{l}) = 1$ for $p|a$, it follows that $\mathfrak{q} \approx_{k_2} (1)$ as well. Therefore, ϕ is injective.

For Cases 2C, 2E, and 2F, we note that by inspecting E_1, if l is a prime that splits completely in K such that $(\frac{q_i}{l}) = 1$ for all $q_i \equiv 1 \pmod 4$ and $(\frac{q_i}{l})$ for all $q_i \equiv 3 \pmod 4$, then it fo llows that $\mathfrak{p}_l \approx_{k_1} (1)$. However, by inspecting E_2, we see that $\mathfrak{q}_l \not\approx_{k_2} (1)$. Now if l' is another prime that splits completely in K such that $[l'] \neq [l]$ and $(\frac{q_i}{l}) = -1$ for some i, then $\mathfrak{p}_l \not\approx_{k_1} (1)$. Thus, $|\ker \phi| = 2$. ∎

Theorem 5.2. *Let K be a real biquadratic field with quadratic subfields $k_0 = \mathbb{Q}(\sqrt{p})$, $k_1 = \mathbb{Q}(\sqrt{d})$, and $k_2 = \mathbb{Q}(\sqrt{pd})$, where p is a prime not dividing d. Let G, G_0, G_1, G_2 be the ideal class groups of K, k_0, k_1, k_2, respectively. Suppose that the ramified prime ideals of k_i generate the 2-Sylow subgroups of G_i for $i = 1, 2$. Let G_1' be the subgroup of G_1 generated by*

$$\{[\mathfrak{p}_q]_{k_1} \mid q|d, \text{ and } (\frac{p}{q}) = 1\}.$$

Let r be the 4-rank of G, and let r' be the 2-rank of G_1/G_1'. Then

$$r' - 3 \leq r \leq r' + 1.$$

Proof. Let $\bar{G}_i$ be the quotient of G_i modulo the odd part of G_i for $i = 0, 1, 2$. It follows that $\bar{G}_0$ is trivial. Let $\bar{G}_1'$ be the image of G_1' in the quotient $\bar{G}_1$. Note that $\bar{G}_1' \cong G_1'$. Let l be any prime which splits completely in K. As before, let $\mathfrak{b}_l$, $\mathfrak{p}_l$, and $\mathfrak{q}_l$ be prime ideals of k_0, k_1, and k_2, respectively, lying over l. Let $\mathscr{P}$ be a prime ideal of K lying above l. Since the 4-rank of G_i is 0 for $i = 1, 2$ and since $\bar{G}_0$ is trivial, the conclusion of Lemma 3.3 becomes $\mathscr{P}_l^2 \approx_K \mathfrak{p}_l\mathfrak{q}_l$.

Let q_i be the prime divisors of d, ordered so that for some positive integer m, $(\frac{p}{q_i}) = 1$ for all $i \leq m$, and $(\frac{p}{q_i}) = -1$ for all $i > m$.

For $1 \leq i \leq n$, let l_ν be an odd prime such that $(\frac{p}{l_\nu}) = 1$, $(\frac{q_i}{l_\nu}) = (\frac{q_i}{q_\nu})$ for $i \neq \nu$, and $(\frac{q_\nu}{l_\nu}) = (\frac{d/q_\nu}{q_\nu})$. Such primes exist by Lemma 4.1. Also, note that $(\frac{d}{l_\nu}) = 1$ and $(\frac{pd}{l_\nu}) = 1$. Thus, l_ν splits in k_0, k_1, and k_2, and splits completely in K. Further, by Lemmas 2.4 and 2.5, we have $\chi_{d_1'}^{k_1}(\mathfrak{p}_{l_\nu}) = \chi_{d_1'}^{k_1}(\mathfrak{p}_{q_\nu})$ for all $d_1'|d_1$ such that $\sqrt{d_1'}$ is contained in E_1. Since the Hilbert 2-class field of k_1 is the genus field, it follows that $\mathfrak{p}_{l_\nu} \approx_{k_1} \mathfrak{p}_{q_\nu}$, for $\nu \leq n$. Moreover, for $\nu \leq m$, we have $(\frac{p}{q_\nu}) = (\frac{p}{l_\nu}) = 1$, so that $\chi_{d_2'}^{k_2}(\mathfrak{q}_{l_\nu}) = \chi_{d_2'}^{k_2}(\mathfrak{q}_{q_\nu})$ for all $d_2'|d_2$ such that $\sqrt{d_2'}$ is contained in E_2. Hence, $\mathfrak{p}_{l_\nu} \approx_{k_2} \mathfrak{p}_{q_\nu}$, for $\nu \leq m$. For $\nu > m$, note that in general, $\mathfrak{q}_{l_\nu} \not\approx_{k_2} \mathfrak{q}_{q_\nu}$.

For $\nu \leq n$, let $\mathscr{P}_{l_\nu}$ be a prime ideal of K lying over l_ν. For $\nu \leq m$, we have by Lemmas 3.3 and 3.4 $\mathscr{P}_{l_\nu}^2 \approx_K \mathfrak{p}_{l_\nu}\mathfrak{q}_{l_\nu} \approx_K \mathfrak{p}_{q_\nu}\mathfrak{q}_{q_\nu} \approx_K (1)$, so that $[\mathscr{P}_{l_\nu}]_K$ has order 1 or 2 in G.

Suppose $m + 1 \leq \nu \leq n$. If $q_\nu \equiv 1 \pmod 4$ then since $(\frac{p}{q_\nu}) = -1$, we have by Lemma 2.5 and above that $\chi_{q_\nu}^{k_2}(\mathfrak{q}_{q_\nu}) = -\chi_{q_\nu}^{k_1}(\mathfrak{p}_{q_\nu})$. Thus,

$$\chi_{q_\nu}^{k_2}(\mathfrak{q}_{q_\nu}) = -\chi_{q_\nu}^{k_2}(\mathfrak{q}_{l_\nu}). \tag{1}$$

By a similar argument, if $q_\nu, q_\mu \equiv 3 \pmod 4$ where $1 \leq \mu \leq n$ and $\mu \neq \nu$, then

$$\chi_{q_\nu q_\mu}^{k_2}(\mathfrak{q}_{q_\nu}) = -\chi_{q_\nu q_\mu}^{k_2}(\mathfrak{q}_{l_\nu}). \tag{2}$$

Let H be the group as above, and let $\phi : H \to \bar{G}_1$ be the map $\phi([l]) = \mathfrak{p}_l$, where l is a prime which splits completely in K. Let $\bar{H}'$ be the subgroup of H generated by $[l_\nu]$ for $\nu \le m$. Note that $\bar{H}' \subseteq \phi^{-1}(\bar{G}_1')$. Since ϕ is surjective, it follows from Lemma 5.1 that for cases other than 2C, 2E, and 2F, we have $\bar{G}_1' \cong \bar{H}'$. For cases 2C, 2E, and 2F, then either $\bar{G}_1' \cong \bar{H}'$ or $|\bar{H}'| = 2|\bar{G}_1'|$.

Now let $\bar{G}_1''$ be a subgroup of $\bar{G}_1$ so that $\bar{G}_1 = \bar{G}_1' \times \bar{G}_1''$, and let $\bar{H}''$ be a subgroup so that $H = \bar{H}' \times \bar{H}''$. For cases other than 2C, 2E, and 2F, we have $\bar{G}_1'' \cong \bar{H}''$. The 2-rank of $\bar{H}''$ is r in these cases. For cases 2C, 2E, and 2F, then either $\bar{G}_1'' \cong \bar{H}''$ or $|\bar{H}''| = 2|\bar{G}_1''|$. Since $\bar{G}_1'' \cong \bar{G}_1/G_1'$, the 2-rank of $\bar{G}_1''$ is r and the 2-rank of $\bar{H}''$ is r or $r+1$. In any case, let r^* be the 2-rank of $\bar{H}''$, and for $1 \le \mu \le r^*$ let l_μ' be primes which split completely in K such that $[l_\mu']$ form a minimal set of generators for $\bar{H}''$. Thus, $[l_\mu']$, $[l_\nu]$ for all μ, ν generate H.

To compute the 4-rank of G, it suffices to consider the prime ideals of K which lie above primes which split completely in K, since all ideal classes contain such prime ideals. Let $\mathscr{P}$ be any prime ideal of K which lies above a prime l which splits completely in K. We have $[l] = \prod_{i=1}^{s}[l_{\nu_i}]\prod_{j=1}^{t}[l_{\mu_j}']$, where $1 \le \nu_i \le m$, and $1 \le \mu_j \le r^*$ for all i, j. Then again by Lemmas 3.3 and 3.4,

$$\mathscr{P}^2 \approx_K \mathfrak{p}_l\mathfrak{q}_l \approx_K \left(\prod_{i=1}^{s}\mathfrak{p}_{l_{\nu_i}}\prod_{j=1}^{t}\mathfrak{p}_{l'_{\mu_j}}\right)\left(\prod_{i=1}^{s}\mathfrak{q}_{l_{\nu_i}}\prod_{j=1}^{t}\mathfrak{q}_{l'_{\mu_j}}\right) = \left(\prod_{i=1}^{s}\mathfrak{p}_{l_{\nu_i}}\mathfrak{q}_{l_{\nu_i}}\right)\left(\prod_{j=1}^{t}\mathfrak{p}_{l'_{\mu_j}}\mathfrak{q}_{l'_{\mu_j}}\right)$$

$$\approx_K \left(\prod_{i=1}^{s}\mathfrak{p}_{q_{\nu_i}}\mathfrak{q}_{q_{\nu_i}}\right)\left(\prod_{j=1}^{t}\mathfrak{p}_{l'_{\mu_j}}\mathfrak{q}_{l'_{\mu_j}}\right) \approx_K \prod_{j=1}^{t}\mathfrak{p}_{l'_{\mu_j}}\mathfrak{q}_{l'_{\mu_j}} \approx_K \prod_{j=1}^{t}\mathscr{P}^2_{l'_{\mu_j}}.$$

Thus, $[\mathscr{P}]_K = [\prod_{j=1}^{t}\mathscr{P}_{l'_{\mu_j}}]\gamma$, where $\gamma \in G$ with order 1 or 2. This shows that the 4-rank of G is less than or equal to $r' + 1$.

Cases 1A, 1D, 3A.

In these cases, p, $q_i \not\equiv 3 \pmod 4$ for all i. Since the ramified prime ideals generate G_i, it follows from Lemma 2.8 that $N_{k_i/\mathbb{Q}}(\epsilon_i) = -1$, where ϵ_i is the fundamental unit of k_i. Further, by Lemma 3.7, there exists an integer $\beta | pd$ such that $\sqrt{\beta}\sqrt{\epsilon_0\epsilon_1\epsilon_2} \in K$. We can choose β so that $\beta | d$. By Lemma 2.7, the ideal classes $[\mathfrak{p}_{q_i}]_{k_1}$ for $i \le n-1$, are independent generators for $\bar{G}_1$. Note that if $m = n$ or $m = n-1$, then $r' = 0$ and the theorem follows. So assume $m \le n-1$. We can choose $\bar{G}_1''$ to be the subgroup generated by $[\mathfrak{p}_{q_i}]_{k_1}$ for $m < i \le n-1$. Similarly, we can choose $\bar{H}''$ to be the subgroup generated by $[l_i]$ for $m < i \le n-1$. The 2-rank of $\bar{H}''$ is $r' = n - m - 1$.

Since all the odd prime divisors of d are congruent to 1 modulo 4, it follows from Lemma 2.5 and using the argument preceding (1) that if $q_i = 2 | d$ and $(\frac{2}{p}) = -1$, then $\chi_2^{k_2}(\mathfrak{q}_2) = -\chi_2^{k_2}(\mathfrak{q}_{l_i})$.

Subcase I. $\chi_{q_k}^{k_1}(\mathfrak{q}_\beta) = -1$ for some $k \le m$.

Let $\mathscr{B} = \prod_{j=1}^{t}\mathscr{P}_{l_{\mu_j}}$, where $t > 0$ and $m+1 \le \mu_j \le n-1$, and $\mu_i \ne \mu_j$ for $i \ne j$. Then $\mathscr{B}^2 \approx_K \prod_{j=1}^{t}(\mathfrak{p}_{l_{\mu_j}}\mathfrak{q}_{l_{\mu_j}})$. Also, $\prod_{j=1}^{t}\mathfrak{p}_{l_{\mu_j}} \approx_{k_1} \prod_{j=1}^{t}\mathfrak{p}_{q_{\mu_j}}$, and $\prod_{j=1}^{t}\mathfrak{q}_{l_{\mu_j}} \approx_{k_2} (\prod_{j=1}^{t}\mathfrak{q}_{q_{\mu_j}})\mathfrak{a}$, where $\mathfrak{a}$ is a ramified ideal of k_2. Thus, $\mathscr{B}^2 \approx_K \mathfrak{a}$. By Lemma 3.7, $\mathscr{B}^2$ is principal in K if and only if $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the same ideal class in k_2 as $\mathfrak{q}_p$, $\mathfrak{q}_\beta$, or $\mathfrak{q}_p\mathfrak{q}_\beta$. Note that the other ideals from Lemma 3.7 are equivalent to the above ideals. For example,

$\mathfrak{q}_d \approx_{k_2} \mathfrak{q}_p$. We will show that $\mathfrak{a}$ does not belong to the same ideal class as the above ideals by using the fact that for $\mu > m$, we have $\chi_{d'}^{k_2}(q_\mu) \neq \chi_{d'}^{k_2}(l_\mu)$ for appropriate choices of $d'|d$.

If $\mathfrak{a}$ is principal in k_2 then $\chi_{q_i}^{k_2}(\mathfrak{a}) = 1$ for all i. Thus, it follows from (1) or the above comment for $q_i = 2$ that

$$(3)\qquad (\prod_{j=1}^{t}\chi_{q_{\mu_1}}^{k_2}(\mathfrak{q}_{q_{\mu_j}}))\chi_{q_{\mu_1}}^{k_2}(\mathfrak{a}) = \prod_{j=1}^{t}\chi_{q_{\mu_1}}^{k_2}(\mathfrak{q}_{q_{\mu_j}}) = \chi_{q_{\mu_1}}^{k_2}(\mathfrak{q}_{q_{\mu_1}})\prod_{j=2}^{t}(\frac{q_{\mu_1}}{q_{\mu_j}})$$

$$= -\chi_{q_{\mu_1}}^{k_2}(\mathfrak{q}_{l_{\mu_1}})\prod_{j=2}^{t}(\frac{q_{\mu_1}}{l_{\mu_j}}) = -\prod_{j=1}^{t}\chi_{q_{\mu_1}}^{k_2}(\mathfrak{q}_{l_{\mu_j}}).$$

Since, $(\prod_{j=1}^{t}\mathfrak{q}_{q_{\mu_j}})\mathfrak{a} \not\approx_{k_2} \prod_{j=1}^{t}\mathfrak{q}_{l_{\mu_j}}$, we have a contradiction, so $\mathfrak{a}$ is not principal in k_2.

Similarly,

$$(4)\qquad (\prod_{j=1}^{t}\chi_{q_n}^{k_2}(\mathfrak{q}_{q_{\mu_j}}))\chi_{q_n}^{k_2}(\mathfrak{q}_p) = (\frac{q_n}{p})\prod_{j=1}^{t}(\frac{q_n}{q_{\mu_j}}) = (\frac{p}{q_n})\prod_{j=1}^{t}(\frac{q_n}{l_{\mu_j}}) = -\prod_{j=1}^{t}\chi_{q_n}^{k_2}(\mathfrak{q}_{l_{\mu_j}}).$$

$$(5)\qquad (\prod_{j=1}^{t}\chi_{q_k}^{k_2}(\mathfrak{q}_{q_{\mu_j}}))\chi_{q_k}^{k_2}(\mathfrak{q}_\beta) = -\prod_{j=1}^{t}(\frac{q_k}{q_{\mu_j}}) = -\prod_{j=1}^{t}(\frac{q_k}{l_{\mu_j}}) = -\prod_{j=1}^{t}\chi_{q_k}^{k_2}(\mathfrak{q}_{l_{\mu_j}}).$$

$$(6)\qquad (\prod_{j=1}^{t}\chi_{q_k}^{k_2}(\mathfrak{q}_{q_{\mu_j}}))\chi_{q_k}^{k_2}(\mathfrak{q}_p)\chi_{q_k}^{k_2}(\mathfrak{q}_\beta) = -\prod_{j=1}^{t}(\frac{q_k}{q_{\mu_j}}) = -\prod_{j=1}^{t}\chi_{q_k}^{k_2}(\mathfrak{q}_{l_{\mu_i}}).$$

Hence, $\mathfrak{q}_p \not\approx_{k_2} \mathfrak{a}$, $\mathfrak{q}_\beta \not\approx_{k_2} \mathfrak{a}$, and $\mathfrak{q}_p\mathfrak{q}_\beta \not\approx_{k_2} \mathfrak{a}$.

Therefore, $\mathscr{B}^2$ is not principal in K, and $[\mathscr{B}]$ has order 4 in G.

In particular, we have shown that $[\mathscr{P}_{l_j}]_K$ for $m+1 \leq j \leq n-1$, has order 4 in G, and that there are no non-trivial relations among $[\mathscr{P}_{l_j}]_K$ for $m+1 \leq j \leq n-1$. Thus, $\langle[\mathscr{P}_{l_{m+1}}]_K, \ldots, [\mathscr{P}_{l_{n-1}}]_K\rangle \cong (\mathbb{Z}/4\mathbb{Z})^{n-m-1}$. Hence, the 4-rank of G is at least $r = n-m-1$.

Subcase II. $\chi_{q_i}^{k_2}(\mathfrak{q}_\beta) = 1$ for $1 \leq i \leq m$, with $\beta \neq 1, d$.

If $\chi_{q_i}^{k_2}(\mathfrak{q}_\beta) = 1$ for all $i > m$ as well, then $\mathfrak{q}_\beta$ is principal so that $\beta = 1$. If $\chi_{q_i}^{k_2}(\mathfrak{q}_\beta) = -1$ for all $i > m$, then $\mathfrak{q}_\beta \approx_{k_2} \mathfrak{q}_p \approx_{k_2} \mathfrak{q}_d$, so that $\beta = d$ by our choice of β. Thus, after reordering the q_i if necessary, we may assume $\chi_{q_{n-1}}^{k_2}(\mathfrak{q}_\beta) = -1$ and $\chi_{q_n}^{k_2}(\mathfrak{q}_\beta) = 1$.

Let $\mathscr{B} = \prod_{j=1}^{t}\mathscr{P}_{l_{\mu_j}}$ with $t > 0$ and $m+1 \leq \mu_i \leq n-2$, and $\mu_i \neq \mu_j$ for all $i \neq j$. Then as above, $\mathscr{B}^2 \approx_K \mathfrak{a}$, for some ramified ideal $\mathfrak{a}$ in k_2 and $\prod_{j=1}^{t}\mathfrak{q}_{l_{\mu_j}} \approx_{k_2} (\prod_{j=1}^{t}\mathfrak{q}_{q_{\mu_j}})\mathfrak{a}$. As above, $\mathscr{B}^2$ is principal in K if and only if $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the same ideal class in k_2 as $\mathfrak{q}_p$, $\mathfrak{q}_\beta$, or $\mathfrak{q}_p\mathfrak{q}_\beta$. It follows from (3) and (4), that $\mathfrak{a}$ is not principal and $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p$. By replacing q_k with q_{n-1} in (5), and by replacing q_k with q_n in (6), we see that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_\beta$ or $\mathfrak{q}_p\mathfrak{q}_\beta$. Thus, $\langle[\mathscr{P}_{l_{m+1}}]_K, \ldots, [\mathscr{P}_{l-n-2}]_K\rangle \cong (\mathbb{Z}/4\mathbb{Z})^{n-m-2}$, so that the 4-rank of G is at least $r-1 = n-m-2$.

Subcase III. $\beta = 1$ or $\beta = d$.

Let $\mathscr{B} = \prod_{j=1}^{t} \mathscr{P}_{l_{\mu_j}}$ with $t > 0$ and $m+1 \le \mu_i \le n-1$, and $\mu_i \ne \mu_j$ for all $i \ne j$. Then, $\mathscr{B}^2 \approx_K \mathfrak{a}$ where $\mathfrak{a}$ is some ramified ideal of k_2. If $\beta = 1$, then $\mathfrak{q}_\beta$ is principal in k_2 and $\mathfrak{q}_p\mathfrak{q}_\beta \approx_{k_2} \mathfrak{q}_p$. If $\beta = d$, then $\mathfrak{q}_\beta \approx_{k_2} \mathfrak{q}_p$ and $\mathfrak{q}_p\mathfrak{q}_\beta$ is principal in k_2. Thus, it suffices to show that $\mathfrak{a}$ is not principal in k_2 and $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p$. Both follow from (3) and (4). Thus, $\langle [\mathscr{P}_{l_{m+1}}]_K, \dots, [\mathscr{P}_{l-n-1}]_K \rangle \cong (\mathbb{Z}/4\mathbb{Z})^{n-m-1}$, so that the 4-rank of G is at least $r = n-m-1$.

For each subcase, we have shown that the 4-rank of G is at least $r-1$. From above, the 4-rank of G is at most r. Therefore, the theorem follows for Cases 1A, 1D, and 3A.

Cases 1B, 1C, 1E, 1F, 3B, 3C.

Let $T = \{i | q_i \equiv 3 \pmod 4\}$. In Cases 1B and 3B, $2 \nmid d$ but 2 ramifies in k_1 and k_2. In these cases, let l_0 be a prime such that $(\frac{q_i}{l_0}) = \chi_{q_i}^{k_1}(\mathfrak{p}_2)$ and $(\frac{p}{l_0}) = 1$. By Lemma 4.1, such a prime exists. Also, $\mathfrak{p}_{l_0} \approx_{k_1} \mathfrak{p}_2$ and l_0 splits completely in K. Set $q_0 = 2$ in these cases. In Cases 1E and 1F, let l_0 be a prime that splits completely in K such that $\mathfrak{p}_{l_0} \approx \mathfrak{p}_2$. Note that in Cases 1C and 3C, 2 does not ramify in k_1. For these cases, let l_0 be a prime which splits completely in K such that $[l_0]$ is trivial in H.

Let $\tilde{H}'$ be the subgroup of H generated by $\bar{H}'$, $\prod_{i\in T}[l_i]$, and $[l_0]$. Let $\tilde{H}''$ be a subgroup so that $H = \tilde{H}' \times \tilde{H}''$. If s is the 2-rank of $\tilde{H}''$, then it follows that $s \ge r' - 2$. We may assume that $\tilde{H}''$ is the subgroup of H generated by $[l_{\mu_j}]$ for $j \in S$ where S is a subset of $\{i | m < i \le n\}$. We also may choose S so that $|S| = s$. If $s = 0$, then $r' \le 2$ and the theorem follows in this case. Therefore, assume $s > 0$.

In these cases, the fundamental unit of k_1 is totally positive. Let b be a square free positive integer which divides the discriminant of k_1, such that $b \ne 1, d$ and $\mathfrak{p}_b$ is principal in k_1, as in Lemma 2.6. The fundamental unit of k_0 is not totally positive, so in the notation of Lemma 3.5, $c_0 = 1$. It follows from Lemma 3.5, that if $\mathfrak{a}$ is a ramified ideal which is principal in K, then $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the same ideal class in k_2 as $\mathfrak{q}_p$, $\mathfrak{q}_b$, or $\mathfrak{q}_p\mathfrak{q}_b$.

Let S' be a non-empty subset of S, and let $\mathscr{B} = \prod_{i\in S'} \mathscr{P}_{l_i}$. We have as before $\mathscr{B}^2 \approx_K \mathfrak{a}$, where $\mathfrak{a}$ is a ramified ideal of k_2 such that $\prod_{i\in S'} \mathfrak{q}_{l_i} \approx_{k_2} (\prod_{i\in S'} \mathfrak{q}_{q_i})\mathfrak{a}$. Fix $\beta \in S'$.

Subcase I. $(\frac{p}{q_\alpha}) = 1$ for some $q_\alpha \equiv 3 \pmod 4$ for $1 \le \alpha \le m$.

Since b can be replaced with d/b or $4d/b$, we may assume that $q_\alpha \nmid b$.

If $q_\beta \equiv 1 \pmod 4$, then it follows from (1) that

$$(7) \quad \prod_{i\in S'} \chi_{q_\beta}^{k_2}(\mathfrak{q}_{q_i}) = \chi_{q_\beta}^{k_2}(\mathfrak{q}_{q_\beta}) \prod_{\substack{i\in S'\\ i\ne\beta}} \left(\frac{q_\beta}{q_i}\right) = -\chi_{q_\beta}^{k_2}(\mathfrak{q}_{q_\beta}) \prod_{\substack{i\in S'\\ i\ne\beta}} \left(\frac{q_\beta}{l_i}\right) = -\prod_{i\in S'} \chi_{q_\beta}^{k_2}(\mathfrak{q}_{l_i}).$$

Hence, $\prod_{i\in S'} \mathfrak{q}_{q_i} \not\approx_{k_2} \prod_{i\in S'} \mathfrak{q}_{l_i}$, so that $\mathfrak{a}$ is not principal in k_2. If $q_\beta \equiv 3 \pmod 4$, then it follows from (2) and by replacing q_β with $q_\beta q_\alpha$ in (7), that $\mathfrak{a}$ is not principal in k_2.

Since

$$\prod_{i>m} \mathfrak{p}_{l_i} \approx_{k_1} \prod_{i>m} \mathfrak{p}_{q_i} \approx_{k_1} \prod_{i\le m} \mathfrak{p}_{q_i} \approx_{k_1} \prod_{i\le m} \mathfrak{p}_{l_i} \quad \text{and} \quad [\mathfrak{p}_{l_i}]_{k_1} \in G_1',$$

then

$$\prod_{i>m}[\mathfrak{p}_{l_i}]_{k_1} \in \tilde{G}_1' \quad \Rightarrow \quad \prod_{i>m}[l_i] \in \bar{H}' \subseteq \tilde{H}'.$$

Since $\prod_{j\in S}[l_j]$ is a subproduct of $\prod_{i>m}[l_i]$ and the $[l_j]$ for $j \in S$ are independent generators for $\tilde{H}''$ there must exist $\gamma > m$ such that $l_\gamma \neq l_j$ for all $j \in S$. It follows that $q_\gamma \neq q_j$ for all $j \in S$. If $q_\gamma \equiv 1 \pmod 4$, then

$$(8) \quad (\prod_{i\in S'} \chi_{q_\gamma}^{k_2}(\mathfrak{q}_{q_i}))\chi_{q_\gamma}^{k_2}(\mathfrak{q}_p) = (\frac{q_\gamma}{p})\prod_{i\in S'}(\frac{q_\gamma}{q_i}) = (\frac{p}{q_\gamma})\prod_{i\in S'}(\frac{q_\gamma}{l_i}) = (\prod_{i\in S'}\chi_{q_\gamma}^{k_2}(\mathfrak{q}_{l_i})).$$

Hence, $(\prod_{i\in S'}\mathfrak{q}_{q_i})\mathfrak{q}_p \not\approx_{k_2} \prod_{i\in S'}\mathfrak{q}_{l_i}$, so that $\mathfrak{q}_p \not\approx_{k_2} \mathfrak{a}$. If $q_\gamma \equiv 3 \pmod 4$, then by replacing q_γ with $q_\gamma q_\alpha$ in (8), we see that $\mathfrak{q}_p \not\approx_{k_2} \mathfrak{a}$.

Since $\mathfrak{p}_b$ is principal in k_1,

$$\prod_{i\in S'}\mathfrak{p}_{l_i} \approx_{k_1} \prod_{i\in S'}\mathfrak{p}_{q_i} \approx_{k_1} (\prod_{i\in S'}\mathfrak{p}_{q_i})\mathfrak{p}_b \approx_{k_1} \mathfrak{p}_a = \prod_{i=1}^{t}\mathfrak{p}_{q_{\nu_i}} \approx_{k_1} \prod_{i=1}^{t}\mathfrak{p}_{l_{\nu_i}},$$

where a is the squarefree part of $b\prod_{i\in S'}q_i$; $a = \prod_{i=1}^{t}q_{\nu_i}$ for $t > 0$ and $0 \leq \nu_i \leq n$, and $\nu_i \neq \nu_j$, for $i \neq j$. Note that $q_\alpha \nmid a$. Since $[\mathfrak{p}_a]_{k_1} \notin \tilde{G}_1'$, we may assume that $(\frac{p}{q_{\nu_1}}) = -1$. Also, as above, there exists $q_{\gamma'}$ with $(\frac{p}{q_{\gamma'}}) = -1$, such that $q_{\gamma'} \neq q_{\nu_i}$ for all i. Now $b = \prod_{i=1}^{u}q_{k_i}$ for some integers k_i with $0 \leq k_i \leq n$. Further, in these cases, if 2 ramifies in k_1, then 2 ramifies in k_2 as well. It follows that $\mathfrak{p}_b \approx_{k_1} \prod_{i=1}^{u}\mathfrak{p}_{q_{k_i}} \approx_{k_1} \prod_{i=1}^{u}\mathfrak{p}_{l_{k_i}}$. Also, by the natural correspondence between H and $\tilde{G}_1$ in these cases, it follows from above that $\prod_{i\in S'}[l_i]\prod_{i=1}^{u}[l_{k_i}] = \prod_{i=1}^{t}[l_{\nu_i}]$. Now $\prod_{i=1}^{u}\chi_{d'}^{k_1}(\mathfrak{p}_{l_{k_i}}) = \chi_{d'}^{k_1}(\mathfrak{p}_b) = 1$ for all $d'|d$ such that $\sqrt{d'} \in E_1$ and $(\frac{p}{l_{k_i}}) = 1$. Since $E_2 \subseteq E_1(\sqrt{p})$, it follows that $\prod_{i=1}^{u}\chi_{d''}^{k_2}(\mathfrak{q}_{l_{k_1}}) = 1$ for all $d''|pd$ such that $\sqrt{d''} \in E_2$. Thus, $\prod_{i\in S'}\mathfrak{q}_{l_i} \approx_{k_2} \prod_{i=1}^{t}\mathfrak{q}_{l_{\nu_i}}$.

By following an argument similar to (7) using q_{ν_1} instead of q_β, we see that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_b$. Also, following an argument similar to (8) using $q_{\gamma'}$ instead of q_γ, we have $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_b$.

Subcase II. $(\frac{p}{q_i}) = -1$ for all $q_i \equiv 3 \pmod 4$.

Since $\prod_{i\in T}[l_i] \in \tilde{H}'$, then $\prod_{i\in T}[\mathfrak{p}_{q_i}]_{k_1} \in \tilde{G}_1'$. Hence, there exists $q_{\alpha'} \equiv 3 \pmod 4$ such that $\alpha' \notin S$. Choose b so that $q_{\alpha'} \nmid b$.

If $q_\beta \equiv 1 \pmod 4$, then by (7), it follows that $\mathfrak{a}$ is not principal in k_2. If $q_\beta \equiv 3 \pmod 4$, then by replacing q_β with $q_\beta q_{\alpha'}$ in (7), it follows that $\mathfrak{a}$ is not principal in k_2.

Suppose there exists an integer $\delta \notin S'$ such that $q_\delta \equiv 1 \pmod 4$ with $(\frac{p}{q_\delta}) = (\frac{p}{l_\delta}) = -1$. Then by replacing q_γ with q_δ in (8), it follows that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p$. We need to take care of the case that no such δ exists.

Let $T' = \{i | q_i \equiv 1 \pmod 4 \text{ and } (\frac{p}{q_i}) = -1\}$. Since we have $\prod_{i\in T'}[l_i] = \prod_{i\in T}[l_i]\prod_{i=1}^{m}[l_i] \in \tilde{H}'$, it follows that $\prod_{i\in T'}[l_i]\prod_{i\in T}[l_i] \in \tilde{H}'$ as well. If no such q_δ exists, then it follows that $\prod_{i\in T'}[l_i]$ is a subproduct of $\prod_{i\in S'}[l_i]$ which is not in $\tilde{H}'$. Thus, it follows there exists an integer $\delta' \in S'$ such that $q_{\delta'} \equiv 3 \pmod 4$ with $(\frac{p}{q_{\delta'}}) = (\frac{p}{l_{\delta'}}) = -1$. Then it follows from (2) that $(\prod_{i\in S'}\chi_{q_{\delta'}q_{\alpha'}}^{k_2}(\mathfrak{q}_{q_i}))\chi_{q_\delta q_{\alpha'}}^{k_2}(\mathfrak{q}_p) = -\prod_{i\in S'}\chi_{q_{\delta'}q_{\alpha'}}^{k_2}(\mathfrak{q}_{q_i})$. Thus, we have $(\prod_{i\in S'}\mathfrak{q}_{q_i})\mathfrak{q}_p \not\approx_{k_2} \prod_{i\in S'}\mathfrak{q}_{l_i}$, so that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p$.

There are similar arguments as in Subcase I to show that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_b$ and $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_b$.

In both subcases we have shown that $[\mathscr{B}]_K$ has order 4. Thus, it follows that $\langle [\mathscr{P}_{l_{\mu_1}}]_K, \ldots, [\mathscr{P}_{l_{\mu_s}}]_K \rangle \cong (\mathbb{Z}/4\mathbb{Z})^s$, so that the 4-rank of G is at least $s \geq r-2$. From above, the 4-rank is at most r. Hence, the theorem holds for Cases 1B, 1C, 1E, 1F, 3B, and 3C.

Cases 2A, 2B, 2C, 2D, 2E, and 2F.

Let $\bar{H}$ be the set of equivalence classes of primes that split in K with equivalence relation $\sim'$, where $l \sim' l'$ if $\mathfrak{p}_l \approx_{k_1} \mathfrak{p}_{l'}$. We denote the equivalence class containing l by $[l]'$. The group operation on H is defined as follows: Let l and l' be primes which split completely in K. Then $[l]'[l']' = [l'']'$ where l'' is a prime which splits completely in K and $\mathfrak{p}_{l''} \approx_{k_1} \mathfrak{p}_l\mathfrak{p}_{l'}$. As before, such an l'' exists. We see that $\bar{H} \cong \bar{G}_1$. It follows that either $\bar{H} \cong H$ or $|H| = 2|\bar{H}|$.

We define the following sets:

$$T_1 = \{i | m < i \leq n, q_i \equiv 3 \pmod 4\},$$
$$T_2 = \{i | m < i \leq n, q_i \equiv 3, 5 \pmod 8\},$$
$$T_3 = \{i | m < i \leq n, q_i \equiv 5, 7 \pmod 8\},$$
$$T_4 = \{i | m < i \leq n, q_i \equiv 1 \pmod 4\},$$
$$T_5 = \{i | m < i \leq n, q_i \equiv 1, 7 \pmod 8\},$$
$$T_6 = \{i | m < i \leq n, q_i \equiv 1, 3 \pmod 8\}.$$

In Case 2B, $2 \nmid d$ but 2 ramifies in k_1. As before, in Cases 2B, 2D, 2E, and 2F, let l_0 be be a prime which splits completely in K such that $\mathfrak{p}_{l_0} \approx_{k_1} \mathfrak{p}_2$. In these cases, let $q_0 = 2$. In Cases 2A and 2C, 2 does not ramify in k_1. Let $\hat{H}'$ be the subgroup of $\bar{H}$ generated by $[l_i]'$ for $i \leq m$, $\prod_{i \in T_1}[l_i]'$, $\prod_{i \in T_2}[l_i]'$, and $[l_0]'$ if 2 ramifies in K. Let $\hat{G}_1'$ be the subgroup of $\bar{G}_1$ generated by $\bar{G}_1'$, $\prod_{i \in T_1}[\mathfrak{p}_{q_i}]_{k_1}$, $\prod_{i \in T_2}[\mathfrak{p}_{q_i}]_{k_1}$, and $[\mathfrak{p}_2]_{k_1}$ if 2 ramifies in k_1. Let $\hat{H}''$ be a subgroup of $\bar{H}$ so that $\bar{H} = \hat{H}' \times \hat{H}''$. Then the 2-rank of $\hat{H}''$ is $s \geq r' - 3$. We choose $\hat{H}''$ to be the subgroup of H generated by $[l_{\mu_j}]'$ for $j \in S$ where S is a subset of $\{i | m < i \leq n\}$. Again we choose S so that $|S| = s$. If $s = 0$, then $r' \leq 3$ and the theorem follows in this case. Therefore, assume that $s > 0$.

Note that $\prod_{i \in T_3}[l_i]'$, $\prod_{i \in T_4}[l_i]' \in \hat{H}''$, $\prod_{i \in T_5}[l_i]'$, $\prod_{i \in T_6}[l_i]' \in \hat{H}''$. It follows as well that $\prod_{i \in T_j}[\mathfrak{p}_{q_i}]_{k_1} \in \hat{G}_1$ for $1 \leq j \leq 6$.

For Cases 2B, 2C, 2E, and 2F, let b be a squarefree integer which divides the discriminant of k_1, such that $b \neq 1, d$, and $\mathfrak{p}_b$ is principal in k_1 as in Lemma 2.6. Let $\mathfrak{a}$ be a ramified ideal of k_2 which is principal in K. Consider Cases 2A and 2D. In Lemma 3.5, we have $c_0 = 2$ or $2p$ since $p \equiv 3 \pmod 4$. It follows from Lemma 2.8 that $c_1 = 1$ and $\mathfrak{q}_{c_2}$ is principal in k_2. Thus $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the ideal class containing $\mathfrak{q}_p$, $\mathfrak{q}_2$, or $\mathfrak{q}_p\mathfrak{q}_2$ in k_2. It follows similarly that in Case 2B, $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the ideal class containing $\mathfrak{q}_p$, $\mathfrak{q}_b$, or $\mathfrak{q}_p\mathfrak{q}_b$ in k_2, if $2 \nmid b$; otherwise $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the ideal class containing $\mathfrak{q}_p$, $\mathfrak{q}_{\frac{b}{2}}$, or $\mathfrak{q}_p\mathfrak{q}_{\frac{b}{2}}$ in k_2. In Cases 2C, 2E, and 2F, $\mathfrak{a}$ is principal in k_2, or $\mathfrak{a}$ belongs to the ideal class containing $\mathfrak{q}_p$, $\mathfrak{q}_2$, $\mathfrak{q}_p\mathfrak{q}_2$, $\mathfrak{q}_b$, $\mathfrak{q}_p\mathfrak{q}_b$, $\mathfrak{q}_2\mathfrak{q}_b$, or $\mathfrak{q}_p\mathfrak{q}_2\mathfrak{q}_b$ in k_2.

Let S' be a nonempty subset of S and let $\mathscr{B} = \prod_{i \in S'} \mathscr{P}_{l_i}$. Again, we have $\mathscr{B}^2 \approx_K \mathfrak{a}$, where $\mathfrak{a}$ is a ramified ideal of k_2 such that $\prod_{i \in S'} \mathfrak{q}_{l_i} \approx_{k_2} (\prod_{i \in S'} \mathfrak{q}_{q_i})\mathfrak{a}$.

As in the previous cases, to show that $\mathfrak{a}$ is not one of the ideals of k_2 which becomes principal in K, we will also use the fact that $\prod_{i\in S'}[l_i]' \neq \prod_{i\in T_j}[l_j]'$ where $1 \le j \le 6$, since such products are in $\hat{H}'$. Fix $\beta \in S$.

If there exists an integer $\alpha_1 > m$ such that $q_{\alpha_1} \equiv 1 \pmod 4$ and $\alpha_1 \in S'$, then it follows similarly to (7) that $\mathfrak{a}$ is not principal in k_2. If not, then $q_i \equiv 3 \pmod 4$ for all $i \in S'$. Also, since $\prod_{i\in T_1}[\mathfrak{p}_{q_i}]_{k_1} \in \hat{G}_1$, there exists an integer $\gamma_1 > m$ such that $q_{\gamma_1} \equiv 3 \pmod 4$ and $\gamma_1 \notin S'$. Thus, it follows from (2) and by replacing q_β with $q_\beta q_{\gamma_1}$ in (7) that $\mathfrak{a}$ is not principal in k_2.

If there exists an integer $\alpha_2 > m$ such that $q_{\alpha_2} \equiv 1 \pmod 4$ and $\alpha_2 \notin S'$, then by replacing q_γ with q_{α_2} in (8), it follows that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p$. If there is no such α_2, then $\prod_{i=1}^{t}[\mathfrak{p}_{q_i}]_{k_1}$ contains the subproduct $\prod_{i\in T_4}[\mathfrak{p}_{q_i}]_{k_1}$. Since $\prod_{i\in T_4}[\mathfrak{p}_{q_i}]_{k_1} \in \hat{G}_1$, then one of the q_i's, say $q_{\beta'} \equiv 3 \pmod 4$. Since $\prod_{i\in T_4}[\mathfrak{p}_{q_i}]_{k_1}\prod_{i\in T_1}[\mathfrak{p}_{q_i}]_{k_1} \in \hat{G}_1$, then there is an integer $\gamma_1 > m$ such that $q_{\gamma_1} \equiv 3 \pmod 4$ and $\gamma_1 \notin S'$. Thus, it follows from (2) that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p$.

Suppose there exists $\alpha_3 > m$ such that $q_{\alpha_3} \equiv 1 \pmod 4$, $(\frac{2}{q_{\alpha_3}}) = 1$, and $\alpha_3 \in S'$, or there exists $\alpha_3' > m$ such that $q_{\alpha_3'} \equiv 1 \pmod 4$, $(\frac{2}{q_{\alpha_3'}}) = -1$, and $\alpha_3' \notin S'$. In both these cases it follows that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_2$.

If no such α_3, α_3' exists, then $\prod_{i\in S'}[l_i]'$ contains the subproduct $\prod_{i\in S_1}[l_i]'$, where $S_1 = \{i | i > m \text{ and } q_i \equiv 5 \pmod 8\}$, and for all $c > m$ such that $q_c \equiv 1 \pmod 8$, $q_c \neq q_i$ for all $i \in S'$. We now show that there exist integers γ_3, $\gamma_3' > m$ such that q_{γ_3}, $q_{\gamma_3'} \equiv 3 \pmod 4$ and one of the following occurs:

$$\text{(9)}\quad \begin{aligned}
&(\frac{2}{q_{\gamma_3}}) = 1, \quad \text{where } \gamma_3 \in S', \quad \text{and} \quad (\frac{2}{q_{\gamma_3'}}) = 1, \quad \text{where } \gamma_3' \notin S',\\
&(\frac{2}{q_{\gamma_3}}) = 1, \quad \text{where } \gamma_3 \in S', \quad \text{and} \quad (\frac{2}{q_{\gamma_3'}}) = -1, \quad \text{where } \gamma_3' \in S',\\
&(\frac{2}{q_{\gamma_3}}) = 1, \quad \text{where } \gamma_3 \notin S', \quad \text{and} \quad (\frac{2}{q_{\gamma_3'}}) = -1, \quad \text{where } \gamma_3' \notin S',\\
&(\frac{2}{q_{\gamma_3}}) = -1, \quad \text{where } \gamma_3 \in S', \quad \text{and} \quad (\frac{2}{q_{\gamma_3'}}) = -1, \quad \text{where } \gamma_3' \notin S',
\end{aligned}$$

To see this, we note that if the first case does not occur, then one of the following occurs: $q_i \equiv 7 \pmod 8$ for some $i > m$ and for all $\delta > m$ such that $q_\delta \equiv 7 \pmod 8$, we have $\delta \in S'$; $q_i \equiv 7 \pmod 8$ for some $i > m$ and for all $\delta > m$ such that $q_\delta \equiv 7 \pmod 8$, we have $\delta \notin S'$; and $q_i \not\equiv 7 \pmod 8$ for all $i > m$. These situations lead to the latter cases.

In each case it follows from (2) that

$$\left(\prod_{i\in S'} \chi^{k_2}_{q_{\gamma_3}q_{\gamma_3'}}(\mathfrak{q}_{q_i})\right) \chi^{k_2}_{q_{\gamma_3}q_{\gamma_3'}}(\mathfrak{q}_2) = \prod_{i\in S'} \chi^{k_2}_{q_{\gamma_3}q_{\gamma_3'}}(\mathfrak{q}_{q_i}) = -\prod_{i\in S'} \chi^{k_2}_{q_{\gamma_3}q_{\gamma_3'}}(\mathfrak{q}_{l_i}).$$

Thus, $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_2$.

If there exists $\alpha_4 > m$ such that $q_{\alpha_4} \equiv 1 \pmod 4$, $(\frac{2}{q_{\alpha_4}}) = -1$, and $\alpha_4 \in S'$, or if there exists $\alpha_4' > m$ such that $q_{\alpha_4'} \equiv 1 \pmod 4$, $(\frac{2}{q_{\alpha_4'}}) = 1$, and $\alpha_4' \notin S'$, then it follows that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_2$.

If there does not exist any such α_4, α_4', then $\prod_{i\in S'}[l_i]'$ contains the subproduct $\prod_{i\in S_2}[l_i]'$, where $S_2 = \{i | i > m \text{ and } q_i \equiv 1 \pmod 8\}$, and for all $c > m$ such that $q_c \equiv 5 \pmod 8$, $q_c \neq q_{\mu_{j_i}}$ for all $i \in S'$. If we use the fact that $\prod_{i\in T_5}[l_i]', \prod_{i\in T_6}[l_i]' \in \hat{H}''$, then by following a similar argument as above, there exists $\gamma_3, \gamma_3' > m$ in which one of the cases in (9) occurs. It also follows similarly that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_2$.

As in Subcase I of Cases 1B, 1C, 1E, 1F, 3B, and 3C, we have $\prod_{i\in S'}\mathfrak{p}_{l_i} \approx_{k_1} \prod_{i=1}^{t}\mathfrak{p}_{l_{\nu_i}}$. Using arguments similar to those above it follows that $\mathfrak{a}$ does not belong to the same ideal class containing $\mathfrak{q}_b$, $\mathfrak{q}_p\mathfrak{q}_p$, $\mathfrak{q}_2\mathfrak{q}_b$, or $\mathfrak{q}_p\mathfrak{q}_2\mathfrak{q}_b$.

For Case 2B when $2|b$, we need to show that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_{\frac{b}{2}}$ and $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_{\frac{b}{2}}$. In this case, since $E_2 \subseteq E_1(\sqrt{p})$, it follows that $\prod_{i=1}^{t}\mathfrak{q}_{l_{\nu_i}} \approx_{k_2} \prod_{i\in S'}\mathfrak{q}_{l_i}$. Suppose $\mathfrak{a} \approx_{k_2} \mathfrak{q}_{\frac{b}{2}}$. Then

$$(10) \qquad \prod_{i=1}^{t}\mathfrak{q}_{l_{\nu_i}} \approx_{k_2} \prod_{i\in S'}\mathfrak{q}_{l_i} \approx_{k_2} \Big(\prod_{i\in S'}\mathfrak{q}_{q_i}\Big)\mathfrak{q}_{\frac{b}{2}} \approx_{k_2} \prod_{\substack{1\le i\le t \\ \nu_i\neq 0}} \mathfrak{q}_{q_{\nu_i}} \approx_{k_2} \mathfrak{q}_{l_0} \prod_{\substack{1\le i\le t \\ \nu_i\neq 0}} \mathfrak{q}_{q_{\nu_i}}.$$

By an argument similar to the one used in showing that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_2$, it follows that (10) does not occur. Hence, $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_{\frac{b}{2}}$. By an argument similar to the one used in showing that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_2$, it follows that $\mathfrak{a} \not\approx_{k_2} \mathfrak{q}_p\mathfrak{q}_{\frac{b}{2}}$.

Thus, $\mathfrak{a}$ is not principal in K, so that $[\mathscr{B}]_K$ has order 4 in G, and it follows as before that the 4-rank of G is at least $r - 3$. Since the 4-rank of G is at most $r + 1$, the theorem follows in these cases as well. ∎

6. Examples

In the last section we found an approximation for the 4-rank of the ideal class group of certain real biquadratic fields. We can explicitly compute the ideal class group for such fields using the ideas in the previous sections.

Theorem 6.1. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{627})$, where p is a prime. Let G be the 2-class group of K. Then each of the following cases*

(1) $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$,
(2) $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
(3) $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

occurs for infinitely many primes.

Remark. The ideal class group of $\mathbb{Q}(\sqrt{627})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For any prime p, the class number of $\mathbb{Q}(\sqrt{p})$ is odd, and for infinitely many primes p, the 2-class group of $\mathbb{Q}(\sqrt{627p})$ is an elementary 2-group. Thus for such primes p, the 2-class groups of all the quadratic subfields of K are elementary 2-groups. This theorem shows that the ideal class group of K is not necessarily isomorphic to a quotient of the product of the ideal class groups of its quadratic subfields as might be suggested from Herglotz's formula for the class number of K. In fact, we show that the 4-rank of the ideal class group of K can vary as much as possible, and there are infinitely many examples of each possibility.

Proof. Let $k_0 = \mathbb{Q}(\sqrt{p})$, $k_1 = \mathbb{Q}(\sqrt{627})$, and $k_2 = \mathbb{Q}(\sqrt{627p})$, Let G_i be the ideal class group of k_i for $i = 0, 1, 2$ and let h', h'_0, h'_1, h'_2 be the order of the 2-class groups of K, k_0, k_1, k_2, respectively. We have $G_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $h'_0 = 1$. Then G_0 has odd order. Let L_i be the Hilbert 2-class field of k_i and let E_i be the genus field of k_i for each i. Then $E_1 = L_1 = \mathbb{Q}(\sqrt{3}, \sqrt{11}, \sqrt{19})$, and if $p \equiv 1 \pmod 4$, then $E_2 = \mathbb{Q}(\sqrt{3}, \sqrt{11}, \sqrt{19}, \sqrt{p})$. Also, for any prime l let $\mathfrak{p}_l$ be a prime ideal of k_1 lying over l and let $\mathfrak{q}_l$ be a prime ideal of k_2 lying over l.

Case 1.

Let p be a prime such that

$$p \equiv 1 \pmod 8, \quad p \equiv 2 \pmod 3, \quad p \equiv 8 \pmod{11}, \quad p \equiv 3 \pmod{19}.$$

Thus, $(\frac{2}{p}) = 1$ and $(\frac{3}{p}) = (\frac{11}{p}) = (\frac{19}{p}) = -1$. Many other choices for congruences modulo 3, 11, and 19, would give a similar result. Below, we compute some of the values of the genus characters χ^{k_1} and χ^{k_2}.

$\chi_l^{k_1}(\mathfrak{p}_q)$

	3	11	19
$\mathfrak{p}_3$	-1	-1	1
$\mathfrak{p}_{11}$	1	-1	-1
$\mathfrak{p}_{19}$	-1	1	-1
$\mathfrak{p}_2$	1	1	1

$\chi_l^{k_2}(\mathfrak{q}_q)$

	3	11	19	p
$\mathfrak{q}_3$	1	-1	1	-1
$\mathfrak{q}_{11}$	1	1	-1	-1
$\mathfrak{q}_{19}$	-1	1	1	-1
$\mathfrak{q}_2$	1	1	1	1
$\mathfrak{q}_p$	-1	-1	-1	-1

Note that $\mathrm{Fr}_{\mathfrak{q}_3}^{E_2/k_2}$, $\mathrm{Fr}_{\mathfrak{q}_{11}}^{E_2/k_2}$, and $\mathrm{Fr}_{\mathfrak{q}_{19}}^{E_2/k_2}$ generate $\mathrm{Gal}(E_2/k_2)$. Thus, by Proposition 2.3, $L_2 = E_2$, so that $h'_2 = 8$.

Let ϵ_i be the fundamental unit of k_i. Since $p \equiv 1 \pmod 4$, then by Lemma 2.8, ϵ_0 is not totally positive. Also, $\sqrt{\epsilon_1} = \frac{1}{2}(\sqrt{1254} + 25\sqrt{2})$. From the above table, we see that $\mathfrak{p}_2$ and $\mathfrak{p}_3\mathfrak{p}_{11}\mathfrak{p}_{19}\mathfrak{p}_2$ are principal ideals of k_1, while $\mathfrak{q}_2$ and $\mathfrak{q}_3\mathfrak{q}_{11}\mathfrak{q}_{19}\mathfrak{q}_2\mathfrak{q}_p$ are principal ideals of k_2. It follows from the proof of Lemma 2.6 that $\sqrt{\epsilon_2} = \frac{1}{2}(a\sqrt{2} + b\sqrt{1254p})$ for some $a, b \in \mathbb{Z}$. By analyzing the expressions for the units and using [Kur] $O_K^* = \langle -1, \epsilon_0, \epsilon_1, \sqrt{\epsilon_1\epsilon_2}\rangle$, and $[O_K^* : O_{k_0}^* O_{k_1}^* O_{k_2}^*] = 2$. By Herglotz's Theorem, $h' = \frac{1}{4}h'_0 h'_1 h'_2 = 16$.

By applying Lemma 4.1, there exist primes l_1 and l_2 which split completely in K such that $(\frac{q}{l_1}) = (\frac{q}{3})$ and $(\frac{q}{l_2}) = (\frac{q}{11})$ for $q = 3$, 11, and 19. Then $\mathfrak{p}_{l_1} \approx_{k_1} \mathfrak{p}_3$, and $\mathfrak{p}_{l_2} \approx_{k_1} \mathfrak{p}_{11}$. Since l_1 and l_2 split in k_0, then $(\frac{p}{l_1}) = (\frac{p}{l_2}) = 1$. It follows from the above table that $\mathfrak{q}_{l_1} \approx_{k_2} \mathfrak{q}_3\mathfrak{q}_{19}$, and $\mathfrak{q}_{l_2} \approx_{k_2} \mathfrak{q}_{11}\mathfrak{q}_3$. Let $\mathscr{P}_1$, $\mathscr{P}_{l_2}$ be prime ideals of K lying over l_1, l_2, respectively. It follows from Lemmas 3.3 and 3.4 that

$$\mathscr{P}_{l_1}^2 \approx_K \mathfrak{p}_{l_1}\mathfrak{q}_{l_1} \approx_K \mathfrak{p}_3\mathfrak{q}_3\mathfrak{q}_{19} \approx_K \mathfrak{q}_{19},$$

$$\mathscr{P}_{l_2}^2 \approx_K \mathfrak{p}_{l_2}\mathfrak{q}_{l_2} \approx_K \mathfrak{p}_{11}\mathfrak{q}_{11}\mathfrak{q}_3 \approx_K \mathfrak{q}_3.$$

Using the notation in Lemma 3.5, we have $c_0 = 1$, $c_1 = 1254$, and $c_2 = 2$ or 1254. It then follows that $\mathfrak{q}_{19}$, $\mathfrak{q}_3$, and $\mathfrak{q}_{19}\mathfrak{q}_3$ are not principal in K. Hence, $[\mathscr{P}_{l_1}]_K$ and $[\mathscr{P}_{l_2}]_K$ have order 4 in G, and there are no non-trivial relations between them. Hence, the 4-rank of G is at least 2. Since $h' = 16$, it follows that $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Case 2.

Now let p be a prime such that

$$p \equiv 1 \pmod 8, \quad p \equiv 2 \pmod 3, \quad p \equiv 6 \pmod{11}, \quad p \equiv 17 \pmod{19}.$$

Thus, $(\frac{19}{p}) = (\frac{2}{p}) = 1$, and $(\frac{3}{p}) = (\frac{11}{p}) = -1$. Again many other congruences are possible. We compute some of the values of the genus characters χ^{k_1} and χ^{k_2} below.

$\chi_l^{k_1}(\mathfrak{p}_q)$

	3	11	19
$\mathfrak{p}_3$	−1	−1	1
$\mathfrak{p}_{11}$	1	−1	−1
$\mathfrak{p}_{19}$	−1	1	−1
$\mathfrak{p}_2$	1	1	1

$\chi_l^{k_2}(\mathfrak{q}_q)$

	3	11	19	p
$\mathfrak{q}_3$	1	−1	1	−1
$\mathfrak{q}_{11}$	1	1	−1	−1
$\mathfrak{q}_{19}$	−1	1	−1	1
$\mathfrak{q}_2$	1	1	1	1
$\mathfrak{q}_p$	−1	−1	1	1

Again, we see that $L_2 = E_2$, and that $\mathfrak{q}_2$ and $\mathfrak{q}_3\mathfrak{q}_{11}\mathfrak{q}_{19}\mathfrak{q}_2\mathfrak{q}_p$ are principal ideals of k_2. By Lemma 2.6, $\sqrt{\epsilon_2} = \frac{1}{2}(a\sqrt{2} + b\sqrt{1254p})$ for some $a, b \in \mathbb{Z}$. As in Case 1, $[O_K^* : O_{k_0}^* O_{k_1}^* O_{k_2}^*] = 2$, so that $h' = 16$.

Let l_1 and l_2 be a prime which splits completely in K such that $(\frac{q}{l_1}) = (\frac{q}{3})$ and $(\frac{q}{l_2}) = (\frac{q}{19})$ for $q = 3$, 11, and 19. It follows that $\mathfrak{p}_{l_1} \approx_{k_1} \mathfrak{p}_3$ and $\mathfrak{p}_{l_2} \approx_{k_1} \mathfrak{p}_{19}$. Hence, $[\mathfrak{p}_{l_1}]_{k_1}$ and $[\mathfrak{p}_{l_2}]_{k_1}$ generate G_1. Since $(\frac{p}{l_1}) = (\frac{p}{l_2}) = 1$, we have $\mathfrak{q}_{l_1} \approx_{k_2} \mathfrak{q}_3\mathfrak{q}_{11}\mathfrak{q}_{19}$ and $\mathfrak{q}_{l_2} \approx_{k_2} \mathfrak{q}_{19}$. Let $\mathscr{P}_{l_1}$ and $\mathscr{P}_{l_2}$ be prime ideals of K lying over l_1. By Lemmas 3.3 and 3.4 we have

$$\mathscr{P}_{l_1}^2 \approx_K \mathfrak{p}_{l_1}\mathfrak{q}_{l_1} \approx_K \mathfrak{p}_3\mathfrak{q}_3\mathfrak{q}_{11}\mathfrak{q}_{19} \approx_K \mathfrak{q}_{11}\mathfrak{q}_{19},$$

$$\mathscr{P}_{l_2}^2 \approx_K \mathfrak{p}_{l_2}\mathfrak{q}_{l_2} \approx_K \mathfrak{p}_{19}\mathfrak{q}_{19} \approx_K (1).$$

Again, by Lemma 3.5, $\mathfrak{q}_{11}\mathfrak{q}_{19}$ is not principal in K. Thus, $[\mathscr{P}_{l_1}]_K$ has order 4 in K.

Now, let l be any prime which splits completely in K. Since $[\mathfrak{p}_{l_1}]_{k_1}$ and $[\mathfrak{p}_{l_2}]_{k_1}$ generate G_1, we have $\mathfrak{p}_l \approx_{k_1} \mathfrak{p}_{l_1}^{e_1}\mathfrak{p}_{l_2}^{e_2}$ where e_1 and e_2 are integers. It follows that $(\frac{q}{l}) = (\frac{q}{l_1^{e_1}l_2^{e_2}})$ for $q = 3$, 11, and 19. Also, since l splits completely in K, $(\frac{p}{l}) = (\frac{p}{l_1^{e_1}l_2^{e_2}}) = 1$. Thus $\mathfrak{q}_l \approx_{k_2} \mathfrak{q}_{l_1}^{e_1}\mathfrak{q}_{l_2}^{e_2}$. Let $\mathscr{P}_l$ be a prime ideal of K lying above l. Then from above,

$$\mathscr{P}_l^2 \approx_K \mathfrak{p}_l\mathfrak{q}_l \approx_K \mathfrak{p}_{l_1}^{e_1}\mathfrak{p}_{l_2}^{e_2}\mathfrak{q}_{l_1}^{e_1}\mathfrak{q}_{l_2}^{e_2} \approx_K \mathfrak{q}_{11}^{e_1}\mathfrak{q}_{19}^{e_2}.$$

Thus, either $[\mathscr{P}_l]_K$ has order less than or equal to 2, or $[\mathscr{P}_l]_K^2 = [\mathscr{P}_{l_1}]_K^2$. Since every ideal class of K contains an ideal lying above a prime which splits completely in K, it follows that the 4-rank is 1. Hence, $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 3.

Now let p be a prime such that

$$p \equiv 1 \pmod 8, \quad p \equiv 1 \pmod 3, \quad p \equiv 7 \pmod{11}, \quad p \equiv 16 \pmod{19}.$$

Thus, $(\frac{3}{p}) = (\frac{19}{p}) = (\frac{2}{p}) = 1$, and $(\frac{11}{p}) = -1$. The values of the genus characters χ^{k_1} and χ^{k_2} are below.

$\chi_l^{k_1}(\mathfrak{p}_q)$

	3	11	19
$\mathfrak{p}_3$	−1	−1	1
$\mathfrak{p}_{11}$	1	−1	−1
$\mathfrak{p}_{19}$	−1	1	−1
$\mathfrak{p}_2$	1	1	1

$\chi_l^{k_2}(\mathfrak{q}_q)$

	3	11	19	p
$\mathfrak{q}_3$	−1	−1	1	1
$\mathfrak{q}_{11}$	1	1	−1	−1
$\mathfrak{q}_{19}$	−1	1	−1	1
$\mathfrak{q}_2$	1	1	1	1
$\mathfrak{q}_p$	1	−1	1	−1

It follows that $L_2 = E_2$ again, and that $\mathfrak{q}_2$ and $\mathfrak{q}_3\mathfrak{q}_{11}\mathfrak{q}_{19}\mathfrak{q}_2\mathfrak{q}_p$ are principal ideals of k_2. By Lemma 2.6, $\sqrt{\epsilon_2} = \frac{1}{2}(a\sqrt{2}+b\sqrt{1254})$ for some $a, b \in \mathbb{Z}$. As in the previous cases, $h' = 16$.

Let l be any prime which splits completely in K, and let $\mathscr{P}_l$ be any prime ideal of K lying over l. Since $[\mathfrak{p}_3]_{k_1}$ and $[\mathfrak{p}_{19}]_{k_1}$ generate G_1, then $\mathfrak{p}_l \approx_{k_1} \mathfrak{p}_3^{e_1}\mathfrak{p}_{19}^{e_2}$, where $e_i = 0, 1$. Further, since $\chi_q^{k_1}(\mathfrak{p}_l) = \chi_q^{k_2}(\mathfrak{q}_l)$, $\chi_q^{k_1}(\mathfrak{p}_3) = \chi_q^{k_2}(\mathfrak{q}_3)$, and $\chi_q^{k_1}(\mathfrak{p}_{19}) = \chi_q^{k_2}(\mathfrak{q}_{19})$ for $q = 3, 11, 19$, and $\chi_p^{k_2}(\mathfrak{q}_l) = \chi_p^{k_2}(\mathfrak{q}_3) = \chi_p^{k_2}(\mathfrak{q}_{19}) = 1$, it follows that $\mathfrak{q}_l \approx_{k_2} \mathfrak{q}_3^{e_1}\mathfrak{q}_{19}^{e_2}$. Thus, by Lemmas 3.3 and 3.4,

$$\mathscr{P}_l^2 \approx_K \mathfrak{p}_l\mathfrak{q}_l \approx_K \mathfrak{p}_3^{e_1}\mathfrak{p}_{19}^{e_2}\mathfrak{q}_3^{e_1}\mathfrak{q}_{19}^{e_2} \approx_K (1).$$

Hence, all ideals have order less than or equal to 2 in G. Therefore, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

By Dirichlet's Theorem on primes in arithmetic progression, there exist infinitely many primes p which satisfy the congruences in each of the three cases. Hence, there are infinitely many primes such that G is isomorphic to each of the three groups above. ■

The primes 41, 17, and 73 satisfy the congruences in Cases 1, 2, and 3, respectively. Let G_p be the ideal class group for $\mathbb{Q}(\sqrt{p}, \sqrt{627})$. The class numbers of $\mathbb{Q}(\sqrt{41})$, $\mathbb{Q}(\sqrt{17})$, and $\mathbb{Q}(\sqrt{73})$ are all equal to 1, and the ideal class groups of $\mathbb{Q}(\sqrt{627})$, $\mathbb{Q}(\sqrt{627p})$ are elementary 2-groups for $p = 41, 17$, and 73. Hence, G_{41}, G_{17}, and G_{73} are 2-groups. It follows that

$$G_{41} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$
$$G_{17} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$G_{73} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Acknowledgement

This paper is part of the author's University of Maryland doctoral dissertation written under the direction of Lawrence C. Washington.

References

[Ha1] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkorpen*, J. Math. Soc. Japan **3** (1951), 45–51.

[Ha2] H. Hasse, *Number theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[He] G. Herglotz, *Über einen Dirichletschen Satz*, Math. Z. **12** (1922), 225–261.

[Hi] D. Hilbert, *Gesammelte Abhandlungen,* Vol. I, Chelsea, New York, 1965.

[Ja] G. Janusz, *Algebraic number fields*, Academic Press, New York and London, 1973.

[Kub] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1955), 65–85.

[Kur] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I **4** (1943), 383–406.

[Ma] D. Marcus, *Number fields*, Springer-Verlag, New York, Heidelberg and Berlin, 1977.

[Si] P. Sime, *On the ideal class groups of real biquadratic fields*, Ph.D. Thesis, University of Maryland, College Park, 1992.

Department of Mathematics, Caldwell College, Caldwell, New Jersey 07006
E-mail address: `sime@pilot.njin.net`