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 $n = 1, 2, 4$ 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-ranking. 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
(\mathbb{Z}/4\mathbb{Z})^2, \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2, \text{ or } (\mathbb{Z}/2\mathbb{Z})^4. \text{ 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 \( d = \prod_{i=1}^{r} q_i \), where \( q_i \) is prime for each \( i \). Let \( p_{q_i} \) 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 \( p_{q_i} \), 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 \( r' - 3 \leq r \leq r' + 1 \).

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 \( \mathcal{O}_K \) as in [Kur]. We also show which ideals of \( K \) that are products of ramified prime ideals of \( k_0, k_1, \text{ and } k_2 \) 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 \( (\mathbb{Z}/4\mathbb{Z})^2, \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2, \text{ and } (\mathbb{Z}/2\mathbb{Z})^4 \), 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 \( \mathcal{O}_L \). Unless otherwise specified, we will write ideal of \( L \) to mean fractional ideal of \( \mathcal{O}_L \). 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 \( L \), \( \alpha \) 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:

\[
\begin{align*}
[I]_L & \quad \text{ideal class of } I \text{ in } \mathcal{O}_L \\
I \sim_L J & \quad I \text{ and } J \text{ belong to same ideal class in } \mathcal{O}_L \\
I \approx_L J & \quad [IJ^{-1}]_L \text{ has odd order in the ideal class group of } L \\
\|I\| & \quad \text{order of the quotient ring } \mathcal{O}_L/I \\
N_{M/L}(\alpha) & \quad \text{norm of } \alpha \text{ for } M \text{ over } L \\
\text{Gal}(M/L) & \quad \text{Galois group of } M \text{ over } L \\
m =_2 n & \quad mn \text{ is a square rational integer} \\
R^* & \quad \text{group of units of a ring } R
\end{align*}
\]
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 $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. 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 $p$ of a quadratic field $k$ is called ramified if $p$ 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 $\text{Gal}(M/k)$ and $\text{Gal}(E/k)$ 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 $G' = \text{Gal}(E/k)$. If $\{\text{Fr}_p/E/k | p$ 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, $G^2 \cong \text{Gal}(F/E)$, 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 $i \leq m$ 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 $\sqrt{p_jp_j}$ 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 $\chi_{d'}^k(I)$ as follows:

$$\chi_{d'}^k(I) = \chi_{d'}^k(I)\sqrt{d'}.$$

It follows from the properties of the Frobenius automorphisms that if $J$ is another ideal of $k$ and $d''$ is another squarefree integer such that $\sqrt{d''} \in E$, then $\chi_{d'}^k(IJ) = \chi_{d'}^k(I)\chi_{d''}^k(J)$ and $\chi_{d'd''}^k(I) = \chi_{d'}^k(I)\chi_{d''}^k(I)$. 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 $p_l$ is clearly a principal ideal of $k$. Thus, the values of all the genus characters at $p_l$ are 1. The following two lemmas describe the values of the genus characters at $p_l$ 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 $p_l$ 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 $\chi_{d'}^k(p_l) = (\frac{d'}{l})$. If $l = 2$ and $d' \equiv 1 \pmod{4}$, then $\chi_{d'}^k(p_2) = (\frac{d'}{2})$.

**Lemma 2.5.** Let $k$ be a real quadratic field as above and suppose $l$ is a prime that ramifies in $k$. Let $p_l$ 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

$$\chi_{d'}^k(p_l) = \begin{cases} (\frac{d'}{l}), & \text{if } l \nmid d', \\ (\frac{d'}{l}), & \text{if } l|d'. \end{cases}$$

If $l = 2$ and $d' \equiv 1 \pmod{4}$, then $\chi_{d'}^k(p_2) = (\frac{d'}{2})$.

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 $p_i$ 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 $a$ and $b$ be ideals of $k$ such that $a^2 = (r)$ and $b^2 = (s)$. Let $S = \{p_1^{e_1} p_2^{e_2} ... p_\mu^{e_\mu} | e_i = 0, 1 \text{ for all } i\}$. Then $S$ contains exactly 4 principal ideals, namely $(1), (\sqrt{d}), a$, and $b$.

**Lemma 2.7.** Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with fundamental unit $\epsilon$ such that $N_{k/\mathbb{Q}}(\epsilon) = -1$. Let $p_i$ for $i = 1, ..., \mu$ be the ramified prime ideals of $k$. Let $S = \{p_1^{e_1} p_2^{e_2} ... p_\mu^{e_\mu} | e_i = 0, 1 \text{ for all } i\}$. 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 \( \varepsilon \) be the fundamental unit of \( k \). Suppose the ramified prime ideals generate the 2-class group of \( k \). Then \( N_{k/\mathbb{Q}}(\varepsilon) = -1 \).

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 \( k_0, k_1, \text{ and } k_2 \). 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. \( \varepsilon_0, \varepsilon_1, \varepsilon_2 \); 2. \( \varepsilon_0, \varepsilon_1, \sqrt{\varepsilon_2} \); 3. \( \varepsilon_0, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2} \); 4. \( \varepsilon_0, \varepsilon_1, \sqrt{\varepsilon_0^2 \varepsilon_2} \); 5. \( \varepsilon_0, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_0^2 \varepsilon_2} \); 6. \( \varepsilon_0, \sqrt{\varepsilon_0^2 \varepsilon_1}, \sqrt{\varepsilon_0^2 \varepsilon_2} \); 7. \( \varepsilon_0, \varepsilon_1, \sqrt{\varepsilon_0^2 \varepsilon_1 \varepsilon_2} \). Furthermore, if \( \sqrt{\varepsilon_i} \in K \), then \( \varepsilon_i \) must be totally positive. If \( \sqrt{\varepsilon_i \varepsilon_j} \in K \) for \( i \neq j \), then \( \varepsilon_i \) and \( \varepsilon_j \) are totally positive. If \( \sqrt{\varepsilon_0 \varepsilon_1 \varepsilon_2} \in K \), then either \( \varepsilon_i \) is totally positive for all \( i \) or \( \varepsilon_i \) is not totally positive for all \( i \). We have the following result which is proven in [Kub, Hilfssatz 4]:

Lemma 3.2. Let \( \eta \) 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 \( k_0, k_1, \text{ and } k_2 \) which follow from investigating the Jacobi symbols. Up to permutations of indices, there are five types of splitting in \( k_0, k_1, \text{ and } k_2 \):

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 \( \mathcal{P} \) be a prime ideal of \( K \) lying over \( l \). Then \( \mathcal{P}^2 \sim_K \mathcal{P} p q \) where \( b, p, q \) are prime ideals of \( k_0, k_1, k_2 \), respectively, lying over \( l \) and below \( \mathcal{P} \).

Proof. Suppose \( l \) splits completely in \( K \). Then \( l O_{k_0} = b b' \), \( l O_{k_1} = p p' \), and \( l O_{k_2} = q q' \), where \( b, b', p, p', q, \) and \( q' \) are all prime ideals lying over \( l \). Let \( \mathcal{P}, \mathcal{P}', \mathcal{P}'', \text{ and } \mathcal{P}''' \) be the prime ideals of \( K \) lying over \( l \). Since
Gal \((K/Q)\) acts transitively on these ideals, we may assume without loss of generality that \(P_1^p = b, \ P_2^p = p, \) and \(P_3^p = q. \) Then, \(P_2^{I} = P_2 P_1^p P_2^p P_3^p = b pq. \)

The next four lemmas will determine which ideals of the form \((I_0 I_1 I_2)O_K,\) 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 \(I O_M\) 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 \(p, q\) be the prime ideals lying above \(p\) in \(k_1, k_2,\) respectively. Then \((pq)\) is a principal ideal in \(K = k_1 k_2.\)

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

If \(p\) is inert or ramifies in \(k_0,\) then \((p) = \mathcal{P}_0^2\) or \((p) = \mathcal{P}_0^4,\) respectively, where \(\mathcal{P}_0\) is the prime ideal of \(K\) lying above \(p.\) Now either \(p = q = \mathcal{P}_0,\) or \(p = q = \mathcal{P}_0^2.\) In either case, \(pq = (p).\) ■

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

\[
S = \{\mu \in Z| \mu = 2 c_{i_0} c_{i_1} c_{i_2} d_{i_0} d_{i_1} d_{i_2}, \text{ with } e_i, f_i = 0, 1\}.
\]

Let \(a = (b_a p_b q_c)O_K\) be an ideal of \(K,\) where \(b_a, p_b, q_c\) are ramified ideals of \(k_0, k_1, k_2,\) respectively, such that \(b_0^2 = (a),\) \(p_0^2 = (b),\) and \(q_0^2 = (c).\) Then \(a\) is principal in \(K\) if and only if \(a^2 = (\mu)\) 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 \(a^2 = (\mu)\) for some \(\mu \in S.\) Then \(\mu = \alpha^2 c_{i_0} c_{i_1} c_{i_2} d_{i_0} d_{i_1} d_{i_2}\) for some integer \(\alpha.\) It follows that \((\alpha^{-1} a)^2 = (c_{i_0} c_{i_1} c_{i_2} d_{i_0} d_{i_1} d_{i_2}),\) so that \(\alpha^{-1} a = b_{i_0} p_{i_1} q_{i_2} b_{i_0} d_{i_0} p_{i_1} d_{i_1} c_{i_2},\) where the ideals \(b_{i_0}, p_{i_1}, q_{i_2}, b_{i_0} d_{i_0}, p_{i_1} d_{i_1}\) are defined similarly to \(b_a.\) By Lemmas 2.6 and 2.7, the above ideals are principal. Therefore \(a\) is a principal ideal of \(K.\)

\((\Rightarrow)\) Suppose \(a\) is a principal ideal, and \(a^2 = (\nu)\) where \(\nu \notin S.\) Let \(\alpha\) be a generator for \(a.\) Then, \(\alpha^2 = \nu\epsilon\) where \(\epsilon\) 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 \(\epsilon = \epsilon_{i_0}^{g_{i_0}} \epsilon_{i_1}^{g_{i_1}} \epsilon_{i_2}^{g_{i_2}},\) where \(g_i = 0\) or \(1\) if \(N_{k_i/Q}(\xi_i) = 1,\) or \(g_i = 0\) otherwise. If \(N_{k_i/Q}(\xi_i) = 1,\) then \(\sqrt{\epsilon_i} = u_i \sqrt{c_i} + v_i \sqrt{d_i},\) where \(u_i, v_i \in Q,\) \(c_i\) is the squarefree part of \(2(a - 1),\) and \(c_i c_i^* = d_i\) or \(4d_i.\) It follows that \(\sqrt{\nu} \epsilon \in \sqrt{\nu c_{i_0} c_{i_1} c_{i_2} d_{i_0} d_{i_1} d_{i_2}} K.\) Since \(\nu \notin S,\) then \(\nu = 2 c_{i_0} c_{i_1} c_{i_2} d_{i_0} d_{i_1} d_{i_2} \delta\) where \(\delta\) is an integer not in \(S.\) It follows that \(\sqrt{\nu c_{i_0} c_{i_1} c_{i_2} d_{i_0} d_{i_1} d_{i_2}} \notin K,\) so that \(\sqrt{\nu} \epsilon \notin K,\) which is a contradiction. ■

Before we state a similar lemma for the case when \(N_{k_i/Q}(\xi_i) = -1\) 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 $\epsilon_i$ be the fundamental unit of $k_i$ for $i = 0, 1, 2$. Suppose $\epsilon_i$ is not totally positive for each $i$. Then there exists a squarefree rational integer $\beta$ dividing $\sqrt{d_0}d_1d_2$ 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 $\eta$ such that $\sqrt{\beta} \eta \in K$.

Now let $\alpha = (\sqrt{\beta} \eta)$. Then $\alpha^2 = (\beta)$. Let $p$ be a prime dividing $\beta$. Since $\beta$ 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 $N_{k_i/k}(\epsilon_i) = -1$, 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 $\beta$ is squarefree, then $\beta | d_0d_1d_2$.

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 $\epsilon_i$ is not totally positive for each $i$. Let $\beta$ be a squarefree integer such that $\sqrt{\beta} \epsilon_0\epsilon_1\epsilon_2 \in K$. Let

$$S = \{ \mu \in \mathbb{Z} | \mu = \beta^{e_0}d_0^{f_0}a_1^{e_1}b_1^{f_1}, \text{ with } e_1, f_1 = 0, 1 \}.$$ 

Let $a = (b_0p_0q_0)_{O_K}$ be an ideal of $K$, where $b_a$, $p_b$, $q_c$ are ramified ideals of $k_0$, $k_1$, $k_2$, respectively, such that $b_a^2 = (a)$, $p_b^2 = (b)$, and $q_c^2 = (c)$. Then $a$ is principal in $K$ if and only if $a^2 = (\mu)$ 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 $\phi : G_0 \times G_1 \times G_2 \rightarrow G$ defined by

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

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 $\phi : G_0 \times G_1 \times G_2 \rightarrow G$ 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 $p_1, p_2, ..., p_n$ be distinct primes and for each $i$, let $e_i = \pm 1$ then there exist infinitely many primes $l$ such that $(\frac{e_i}{l}) = e_i$ for all $i$.

If $l$ is a prime, we will define $b_l, p_l, q_l$ 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 ~ as follows: Let $l, l'$ be primes which split completely in $K$. Then $l \sim l'$ if \[ \chi_{d_0}^{k_0}(b_l) = \chi_{d_0}^{k_0}(b_{l'}), \quad \chi_{d_1}^{k_1}(p_l) = \chi_{d_1}^{k_1}(p_{l'}), \quad \text{and} \quad \chi_{d_2}^{k_2}(q_l) = \chi_{d_2}^{k_2}(q_{l'}) \]
for all $d_i | d_l$ such that $\sqrt{d_l} \in E_i$. Note that in particular, if $(\frac{e_i}{l}) = (\frac{e_i}{l'})$ for all primes $p$ such that $p | d_0 d_1 d_2$, 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 $[b_l, p_l, q_l]_{k_0}, [p_l, p_{l'}, k_2], [q_l, q_{l'}]_{k_2}$ 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 \[ [l] [l'] = [l''], \quad \text{where} \quad l'' \text{ is a prime which splits completely in } K, \quad \text{and} \quad \chi_{d_0}^{c_k}(b_{l''}) = \chi_{d_0}^{c_k}(b_{l''}), \quad \chi_{d_1}^{c_k}(p_{l''}) = \chi_{d_1}^{c_k}(p_{l''}), \quad \text{and} \quad \chi_{d_2}^{c_k}(q_{l''}) = \chi_{d_2}^{c_k}(q_{l''}) \]
for all $d_i | d_{l''}$ such that $\sqrt{d_{l''}} \in E_i$. Such primes exist since by Lemma 4.1, there exist infinitely many primes $l''$ such that $(\frac{e_i}{l''}) = (\frac{e_i}{l''})$ for all $p | d_0 d_1 d_2$. Further, it follows that that there are an even number of primes $p | d_l$ such that $(\frac{e_i}{l}) = -1$, so that $l''$ splits completely in $K$. The identity of $H$ is $[\hat{1}]$, where $\hat{1}$ is a prime which splits completely in $K$ such that the value of all the genus characters at $b_l, p_l, q_l$ is $1$. It can be shown, as suggested by David Rohrlich, that $H \cong \text{Gal}(E/K)$, where $E$ 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 $b_{l'''} \approx (b_l b_{l'})$, $p_{l'''} \approx (p_l p_{l'})$, and $q_{l'''} \approx (q_l q_{l'})$. The converse also holds, since if $b_{l'''} \approx (b_l b_{l'})$, for example, then \[ \chi_{d_0}^{c_k}(b_{l''}) = \chi_{d_0}^{c_k}(b_{l''}) \]
for all $d_0 | d_0$ such that $\sqrt{d_{l''}} \in E_0$.

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

$$H' = \{ [l] \mid a, b, c \in \mathbb{Z} \text{ with } b_a \approx k_0 b_l, \quad b_b \approx k_1 p_l, \quad b_c \approx k_2 q_l, \quad \text{and} \quad abc = 2 \},$$

where $b_a, b_b, b_c$ are ramified ideals of $k_0, k_1, k_2$, respectively, such that $b_a^2 = (a)$, $b_b^2 = (b)$, and $b_c^2 = (c)$. 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 $e_i = u_i + v_i \sqrt{d_i}$ be the fundamental unit of $k_i$, and let $c_i$ be the squarefree part of $2(u_i + 1)$ if $N_{k_i/k}(e_i) = 1$, otherwise, let $c_i = 1$ for $i = 0, 1, 2$. By Lemmas 2.6 and 2.7, the ideals $b_{c_0}, p_{c_1}, q_{c_2}$ are principal ideals of $k_0, k_1, k_2$, respectively.

Suppose $N_{k_i/k}(e_i) = 1$ for some $i$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 $[l] = \prod_{j=1}^{s} [l_j]$, where $s \geq 0$, and $i_j \leq n$ for all $j$. By Lemma 3.3,

$$\mathcal{P}_l^2 \cong K b_l p_l q_l \cong K \prod_{j=1}^{s} b_{l_j} \prod_{j=1}^{s} p_{l_j} \prod_{j=1}^{s} q_{l_j} \cong K \prod_{j=1}^{s} \mathcal{P}_{l_j}^2.$$ 

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

For $i \leq m$, we have $\mathcal{P}_{l_i}^2 \cong K b_{l_i} p_{l_i} q_{l_i} \cong K b_{a_i} p_{b_i} q_{c_i}$, 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 $(b a p b q c)^2 = (abc)$. Thus $\mathcal{P}_{l_i}^2$ is principal in $K$ by Lemma 3.5.

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

$$\prod_{j=1}^{t} \mathcal{P}_{l_j} \cong K \prod_{j=1}^{t} b_{l_j} \prod_{j=1}^{t} p_{l_j} \prod_{j=1}^{t} q_{l_j} \cong K b_{a_j} p_{b_j} q_{c_j},$$ 

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 $b_{a_j} p_{b_j} q_{c_j}$ is principal in $K$. Then, by Lemma 3.5, $abc = 2, e_i f_j = 0, 1$ for each $i, j$. Since $b_{e_i}, b_{f_j}, p_{c_i}, p_{d_i}$, and $q_{c_i}$ are principal ideals in their respective fields, it follows that $b_{a_j} \cong b_{a_j'}, p_{b_j} \cong p_{b_j'},$ and $q_{c_j} \cong q_{c_j'},$ where $a', b', c'$ are the squarefree parts of $ac_i,d_i,bc_i,d_i$, and $cc_i$, respectively. But from above, $a'b'c' = ac_i d_i b c_i d_i c_i = 2, 1$. Since $\prod_{j=1}^{t} [l_j] \notin H'$, this is a contradiction. Therefore, $\prod_{j=1}^{t} \mathcal{P}_{l_j}^2$ is not principal in $K$. So by Proposition 3.8, $[\prod_{j=1}^{t} \mathcal{P}_{l_j}]_K$ has order 4 in $G$.

In particular, we have shown that $[\mathcal{P}]_K$ has order 4 in $G$ for $m + 1 \leq i \leq n$, and there are no non-trivial relations among $[\mathcal{P}]_l$, for $m + 1 \leq i \leq n$. Thus, $([\mathcal{P}_{l_1}], \ldots, [\mathcal{P}_{l_n}]) \cong (Z/4Z)^{n-m} = (Z/4Z)^r$, so that the 4-rank of $G$ is at least $r$. Since we have also shown for any prime ideal $\mathcal{P}$ of $K$, that $\mathcal{P}^2 \cong K \prod_{j=1}^{t} \mathcal{P}_{l_j}^2$, 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 $N_{k_i/q}(e_i) = -1$ for all $i$.

Let $\beta$ be a squarefree integer such that $\sqrt[\sqrt{\beta}]\epsilon_0 \epsilon_1 \epsilon_2 \in K$ and $\beta|\sqrt{d_0 d_1 d_2}$ as in Lemma 3.6. Also, let $H'$ be the subgroup of $H$ defined by $H' = \{l \mathcal{P} \mathcal{Q} a, b, c \in Z$ with $b_{a_j} \cong b_{a_j'}, p_{b_j} \cong p_{b_j'}, q_{c_j} \cong q_{c_j'},$ and $abc = 2, 1, \beta\}$.

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 $i \leq r^*$ be primes which split completely in $K$ such that $[l_i']$ generate $\hat{H}'$ for $i \leq r^*$. Consider $\prod_{j=1}^{r^*} \mathcal{P}_{l_i'}$, with $t > 0$ and $i_j \leq r^*$ for all $j$. We have as before $\prod_{j=1}^{r^*} \mathcal{P}_{l_i'} \approx_k b_a p_b q_c$, where $a, b, c$ divide the discriminants of $k_0, k_1, k_2$, respectively. Suppose $b_a p_b q_c$ is principal in $K$.

Then by Lemma 3.7, we have $abc = \Delta_0^i \Delta_1^j \beta^e$, where $f_i, e = 0, 1$ for each $i$. Thus as before, $b_a \approx_k a', p_b \approx_k b', q_c \approx_k c'$, where $a', b', c'$ are the squarefree parts of $\Delta_0^i, \Delta_1^j, \beta^e$, respectively. But, $a'b'c = \Delta_0^i \Delta_1^j \beta^e = 2, 1, \beta$, 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 $G, G_0, G_1, G_2$ 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 $k_1$ 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 $G_i$ 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 $p_i, q_i$ 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 $p_i \approx_{k_i} p_i$, and $q_i \approx_{k_2} q_i$. We now prove a lemma which relates the groups $G_1$ and $H$.

Lemma 5.1. Let $K, G_1$ and $H$ be as above. Then $H \cong G_1$ except in cases 2C, 2E, and 2F. In those cases $|H| = 2|G_1|$.

Proof. We have a map $\phi : H \rightarrow G_1$ defined by $\phi([l]) = [p_i]_{k_1}$. Let $p$ be a prime ideal representing an ideal class of $K$. We may assume $p$ lies over a prime $q$ that splits in $K$. Further, by Lemma 4.1, we can find a prime $l$ such that $(\frac{l}{q}) = (\frac{q}{p})$ for all $i$ and $(\frac{l}{q}) = 1$. Such a prime splits completely in $K$ and $[p_i]_{k_i}[p_k]$. Thus $\phi$ is surjective.

We now show $\phi$ 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 $p_l \approx_{k_1} (1)$. Suppose $a$ is a squarefree integer dividing $pl$ such
that $\sqrt{a} \in E_2$. Then using Lemma 2.4 and that $(\frac{f}{a}) = (\frac{d_p}{a}) (\frac{f}{a}) = 1$ for $p | a$, it follows that $q \approx q_1 \ (1)$ as well. Therefore, $\phi$ 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 $(\frac{f}{a}) = 1$ for all $q_1 \equiv 1 \pmod{4}$ and $(\frac{f}{a})$ for all $q_1 \equiv 3 \pmod{4}$, then it follows that $p_l \approx q_1 \ (1)$. However, by inspecting $E_2$, we see that $q_1 \not\approx q_2 \ (1)$. Now if $l'$ is another prime that splits completely in $K$ such that $[l'] \neq [l]$ and $\left(\frac{f}{a}\right) = -1$ for some $i$, then $p_{l'} \not\approx q_{l'} \ (1)$. 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

$$\{[p_{q_1}]_{kl} | q | d, \text{ and } (\frac{p}{q}) = 1\}.$$

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 $G_i$ be the quotient of $G_i$ modulo the odd part of $G_i$ for $i = 0, 1, 2$. It follows that $G_0$ is trivial. Let $G_1'$ be the image of $G_1'$ in the quotient $G_1$. Note that $G_1' \approx G_1'$. Let $l$ be any prime which splits completely in $K$. As before, let $b_l$, $p_l$, and $q_l$ be prime ideals of $k_0$, $k_1$, and $k_2$, respectively, lying over $l$. Let $\mathcal{P}$ be a prime ideal of $K$ lying above $l$. Since the 4-rank of $G_i$ is 0 for $i = 1, 2$ and since $G_0$ is trivial, the conclusion of Lemma 3.3 becomes $\mathcal{P}_l^2 \approx_K p_l q_l$.

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

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

For $v \leq n$, let $\mathcal{P}_{l_v}$ be a prime ideal of $K$ lying over $l_{v_i}$. For $v \leq m$, we have by Lemmata 3.3 and 3.4 $\mathcal{P}_{l_v}^2 \approx_K p_{l_v} q_{l_v} \approx_K p_{l_v} q_{l_v} \approx_K (1)$, so that $[\mathcal{P}_{l_v}]_K$ has order 1 or 2 in $G$.

Suppose $m + 1 \leq v \leq n$. If $q_{l_v} \equiv 1 \pmod{4}$ then since $(\frac{p_{l_v}}{q_{l_v}}) = -1$, we have by Lemma 2.5 and above that $\chi_{d_{l_v}}^{k_0} (q_{l_v}) = -\chi_{d_{l_v}}^{k_0} (q_{l_v})$. Thus,

$$(1) \quad \chi_{d_{l_v}}^{k_0} (q_{l_v}) = -\chi_{d_{l_v}}^{k_0} (q_{l_v}).$$

By a similar argument, if $q_{l_v}, q_{l_u} \equiv 3 \pmod{4}$ where $1 \leq u \leq n$ and $u \neq v$, then

$$(2) \quad \chi_{d_{l_v}}^{k_2} (q_{l_v}) = -\chi_{d_{l_v}}^{k_2} (q_{l_v}).$$
Let $H$ be the group as above, and let $\phi : H \to G_1$ be the map $\phi([l]) = p_l$, where $l$ is a prime which splits completely in $K$. Let $H'$ be the subgroup of $H$ generated by $[l_v]$ for $\nu \leq m$. Note that $H' \subseteq \phi^{-1}(G'_1)$. Since $\phi$ is surjective, it follows from Lemma 5.1 that for cases other than 2C, 2E, and 2F, we have $G'_1 \cong H'$. For cases 2C, 2E, and 2F, then either $G'_1 \cong H'$ or $|H'| = 2|G'_1|$. Now let $G''_1$ be a subgroup of $G_1$ so that $G_1 = G'_1 \times G''_1$, and let $H''$ be a subgroup so that $H = H' \times H''$. For cases other than 2C, 2E, and 2F, we have $G''_1 \cong H''$. The 2-ranking of $H''$ is $r$ in these cases. For cases 2C, 2E, and 2F, then either $G''_1 \cong H''$ or $|H''| = 2|G''_1|$. Since $G''_1 \cong G_1/G'_1$, the 2-ranking of $G''_1$ is $r$ and the 2-ranking of $H''$ is $r$ or $r + 1$. In any case, let $r^*$ be the 2-ranking of $H''$, and for $1 \leq \mu \leq r^*$ let $l_{\mu}$ be primes which split completely in $K$ such that $[l_{\mu}]$ form a minimal set of generators for $H''$. Thus, $[l_{\mu}]$, $[l_v]$ for all $\mu$, $v$ 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 $\mathfrak{P}$ be any prime ideal of $K$ which lies above a prime $l$ which splits completely in $K$. We have $[l] = \prod_{i=1}^t [l_{i}] \prod_{j=1}^t [l_{j}]$, where $1 \leq \nu_i \leq m$, and $1 \leq \mu_j \leq r^*$ for all $i$, $j$. Then again by Lemmas 3.3 and 3.4,

$$\mathfrak{P}^2 \approx_K \prod_{i=1}^t p_{\nu_i} \prod_{j=1}^t p_{\mu_j} \prod_{i=1}^t q_{\nu_i} \prod_{j=1}^t q_{\mu_j} \approx \prod_{i=1}^t p_{\nu_i} q_{\nu_i} \prod_{j=1}^t p_{\mu_j} q_{\mu_j} \approx_K \prod_{j=1}^t \mathfrak{P}^2_{l_{\mu_j}}.$$

Thus, $[\mathfrak{P}]_K = \prod_{j=1}^t [\mathfrak{P}_{l_{\mu_j}}]$, 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, $p_i q_i \not\equiv 3 \pmod{4}$ for all $i$. Since the ramified prime ideals generate $G_1$, it follows from Lemma 2.8 that $N_{k_i/Q}(e_i) = -1$, where $e_i$ is the fundamental unit of $k_i$. Further, by Lemma 3.7, there exists an integer $\beta | d$ such that $\sqrt{\beta} \sqrt{e_0 e_1 e_2} \in K$. We can choose $\beta$ so that $\beta | d$. By Lemma 2.7, the ideal classes $[p_{\mu_j}]_{k_i}$ for $i \leq n - 1$, are independent generators for $G_1$. Note that if $m = n$ or $m = n - 1$, then $r^* = 0$ and the theorem follows. So assume $m \leq n - 1$. We can choose $G'_1$ to be the subgroup generated by $[p_{\mu_j}]_{k_i}$ for $m < i \leq n - 1$. Similarly, we can choose $H''$ to be the subgroup generated by $[l_{\nu_i}]$ for $m < i \leq n - 1$. The 2-ranking of $H''$ 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 $\left(\frac{2}{q_i}\right) = -1$, then $\chi_2^{k_1}(q_i) = -\chi_2^{k_2}(q_i)$.

Subcase I. $\chi_2^{k_1}(q_i) = -1$ for some $k \leq m$.

Let $\mathfrak{B} = \prod_{j=1}^t [\mathfrak{B}_{l_{\mu_j}}]$, where $t > 0$ and $m + 1 \leq \mu_j \leq n - 1$, and $\mu_i \neq \mu_j$ for $i \neq j$. Then $\mathfrak{B}^2 \approx_K \prod_{j=1}^t (p_{\mu_j} q_{\mu_j})$.

By Lemma 3.7, $\mathfrak{B}^2$ is principal in $K$ if and only if $a$ is principal in $k_2$, or $a$ belongs to the same ideal class in $k_2$ as $q_p$, $q_\beta$, or $q_p q_\beta$. Note that the other ideas from Lemma 3.7 are equivalent to the above ideals. For example,
We will show that \( a \) 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 \( a \) is principal in \( k_2 \), then \( \chi_{d'}^{k_2}(a) = 1 \) for all \( i \). Thus, it follows from (1) or the above comment for \( q_i = 2 \) that

\[
\prod_{j=1}^{t} \chi_{q_{2i}}^{k_2}(a) = \prod_{j=1}^{t} \chi_{q_{2i}}^{k_2}(q_{\mu_j}) = \prod_{j=1}^{t} \left( \frac{q_{\mu_j}}{q_{2j}} \right) = -\prod_{j=1}^{t} \chi_{q_{2i}}^{k_2}(q_{\mu_j}).
\]

Since, \( \left( \prod_{j=1}^{t} q_{\mu_j} \right) a \neq q_{k_2} \prod_{j=1}^{t} q_{\mu_j} \), we have a contradiction, so \( a \) is not principal in \( k_2 \).

Similarly,

\[
\prod_{j=1}^{t} \chi_{q_{2i}}^{k_2}(q_{\mu_j}) = \prod_{j=1}^{t} \left( \frac{q_{\mu_j}}{q_{2j}} \right) = -\prod_{j=1}^{t} \chi_{q_{2i}}^{k_2}(q_{\mu_j}).
\]

Hence, \( q_{\beta} \neq q_{k_2}, a, q_{\beta} \neq q_{k_2}, a \), and \( q_{\beta} q_{\beta} \neq q_{k_2}, a \).

Therefore, \( B^2 \) is not principal in \( K \), and \( [B] \) has order 4 in \( G \).

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

Subcase II. \( \chi_{q_{2i}}^{k_2}(q_{\beta}) = 1 \) for \( 1 \leq i \leq m \), with \( \beta \neq 1, d \).

If \( \chi_{q_{2i}}^{k_2}(q_{\beta}) = 1 \) for all \( i > m \) as well, then \( q_{\beta} \) is principal so that \( \beta = 1 \).

If \( \chi_{q_{2i}}^{k_2}(q_{\beta}) = -1 \) for all \( i > m \), then \( q_{\beta} \approx q_{k_2} a \approx q_{k_2} d \), so that \( \beta = d \) by our choice of \( \beta \). Thus, after reordering the \( q_i \) if necessary, we may assume \( \chi_{q_{2i-1}}^{k_2}(q_{\beta}) = -1 \) and \( \chi_{q_{2i}}^{k_2}(q_{\beta}) = 1 \).

Let \( B = \prod_{j=1}^{t} B_{q_{2j}} \) 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, \( B^2 \approx_{K} a \), for some ramified ideal \( a \) in \( k_2 \) and \( \prod_{j=1}^{t} q_{\mu_j} \approx_{K} q_{k_2} \prod_{j=1}^{t} q_{\mu_j} \). As above, \( B^2 \) is principal in \( K \) if and only if \( a \) is principal in \( k_2 \), or \( a \) belongs to the same ideal class as \( q_{k_2} \) or \( q_{\beta} q_{\beta} \) or \( q_{\beta} q_{\beta} \).

It follows from (3) and (4), that \( a \) is not principal and \( a \neq q_{k_2} q_{\beta} \). By replacing \( q_k \) with \( q_{n-1} \) in (5), and by replacing \( q_k \) with \( q_n \) in (6), we see that \( a \neq q_{k_2} q_{\beta} \) or \( q_{\beta} q_{\beta} \).

Thus, \( ([B_{m+1}]_K, \ldots, [B_{n-2}]_K) \cong (\mathbb{Z}/4\mathbb{Z})^{n-m-2} \), so that the 4-rank of \( G \) is at least \( r-1 = n-m-2 \).

Subcase III. \( \beta = 1 \) or \( \beta = d \).
Let $\mathcal{B} = \prod_{i=1}^{t} P_{i}$ with $t > 0$ and $m + 1 \leq \mu_i \leq n - 1$, and $\mu_i \neq \mu_j$ for all $i \neq j$. Then, $\mathcal{B}^2 \approx K a$ where $a$ is some ramified ideal of $k_2$. If $\beta = 1$, then $q_{\beta}$ is principal in $k_2$ and $q_{\beta} q_{\beta} \approx q_2$. If $\beta = 2$, then $q_{\beta} \approx q_2$, $q_{\beta}$ and $q_{\beta} q_{\beta}$ is principal in $k_2$. Thus, it suffices to show that $a$ is not principal in $k_2$ and $a \neq q_2$. Both follow from (3) and (4). Thus, $([P_{i_{n-1}}], [P_{i_{n-2}}], \ldots, [P_{i_{m}}]) \approx (\mathbb{Z}/4\mathbb{Z})^{n-m-1}$, 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 $(\frac{2}{p}) = \chi_{k_1}^k(p_2)$ and $(\frac{2}{p}) = 1$. By Lemma 4.1, such a prime exists. Also, $p_{l_0} \approx q_1$, $p_2$, 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 $p_{l_0} \approx q_2$. 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 $H'$, $\prod_{i \in T} \{l_i\}$, 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 $s \geq r' - 2$. We may assume that $\tilde{H''}$ is the subgroup of $H$ generated by $[l_{i_j}]$ for $j \in S$ where $S$ is a subset of $\{i | m < i < n\}$. We also may choose $S$ so that $|S| = s$. If $s = 0$, then $r' \leq 2$ 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 $b \neq 1$, $d$ and $p_0$ 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 $a$ is a ramified ideal which is principal in $K$, then $a$ is principal in $k_2$, or $a$ belongs to the same ideal class in $k_2$ as $q_\beta$, $q_\beta$, or $q_\beta q_\beta$.

Let $S'$ be a non-empty subset of $S$, and let $\mathcal{B} = \prod_{i \in S'} P_i$. We have as before $\mathcal{B}^2 \approx_K a$, where $a$ is a ramified ideal of $k_2$ such that $\prod_{i \in S'} q_i \approx q_2 (\prod_{i \in S'} q_i) a$. Fix $\beta \in S'$.

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

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

\[\prod_{i \in S'} \chi_{q_\beta}^k(q_{\beta}) = \chi_{q_\beta}^k(q_{\beta}) \prod_{i \in S'} \chi_{q_\alpha}^k(q_{\alpha}) = -\chi_{q_\beta}^k(q_{\beta}) \prod_{i \in S'} \chi_{q_\alpha}^k(q_{i}) = -\prod_{i \in S'} \chi_{q_\alpha}^k(q_{i}).\]

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

Since

\[\prod_{i > m} p_i \approx q_1 \prod_{i \leq m} p_i \approx q_1 \prod_{i \leq m} p_i \approx q_1 \prod_{i \leq m} p_i \text{ and } [p_{i_k}]_{i_k} \in G_1',\]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
then
\[ \prod_{i > m} [l_i] \in G_1 \implies \prod_{i > m} [l_i] \in H' \subseteq H''. \]

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 \( H'' \), 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
\[
\left( \prod_{i \in S'} x_{q_i}^{k_i}(q_i) \right) x_{q_\gamma}^{k_\gamma}(q_\gamma) = \left( x_{q_\gamma}^{k_\gamma}(q_\gamma) \right) \left( \prod_{i \in S'} x_{q_i}^{k_i}(q_i) \right) = \left( \prod_{i \in S'} x_{q_i}^{k_i}(q_i) \right).
\]

Hence, \( \left( \prod_{i \in S'} q_i \right) q_\gamma \not\approx k_2 \prod_{i \in S'} q_i \), so that \( q_\gamma \not\approx k_2 a \). If \( q_\gamma \equiv 3 \pmod{4} \), then by replacing \( q_\gamma \) with \( q_\gamma a \) in (8), we see that \( q_\gamma \not\approx k_2 a \).

Since \( p_b \) is principal in \( k_1 \),
\[
\prod_{i \in S'} p_i \approx_{k_1} \prod_{i \in S'} q_i \approx_{k_1} \prod_{i \in S'} p_i \approx_{k_1} \prod_{i = 1}^{t} p_{q_i} \approx_{k_1} \prod_{i = 1}^{t} q_{q_i} \approx_{k_1} \prod_{i = 1}^{t} p_{q_i} \approx_{k_1} \prod_{i = 1}^{t} q_{q_i},
\]
where \( a \) is the squarefree part of \( b \prod_{i \in S'} q_i \); \( a = \prod_{i = 1}^{t} q_{v_i} \) for \( t > 0 \) and \( 0 \leq v_i \leq n \), and \( v_i \neq v_j \), for \( i \neq j \). Note that \( q_{q_i} \not\approx a \). Since \( [p_d] k_i \not\in G_1 \), we may assume that \( (\frac{p_d}{q_{q_i}}) = -1 \). Also, as above, there exists \( q_{q_i} \) with \( (\frac{p_d}{q_{q_i}}) = -1 \), such that \( q_{q_i} \not\approx q_{v_i} \) for all \( i \). Now \( b = \prod_{i = 1}^{t} q_{v_i} \) 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 \( p_b \approx_{k_1} \prod_{i = 1}^{t} p_{q_i} \approx_{k_1} \prod_{i = 1}^{t} p_{q_i} \). Also, by the natural correspondence between \( H \) and \( G_1 \) in these cases, it follows from above that \( \prod_{i \in S'} [l_i] \prod_{i = 1}^{m} [l_{v_i}] = \prod_{i = 1}^{t} [l_{v_i}] \). Now \( \prod_{i = 1}^{t} x_{d_i}^{k_i}(p_{d_i}) = x_{d_i}^{k_i}(p_{d_i}) = 1 \) for all \( d \mid d' \) such that \( \sqrt{d'} \in E_1 \) and \( (\frac{d}{d'}) = 1 \). Since \( E_2 \subseteq E_1(\sqrt{d'}) \), it follows that \( \prod_{i = 1}^{t} x_{d_i}^{k_i}(p_{d_i}) = 1 \) for all \( d' \mid pd \) such that \( \sqrt{d'} \in E_2 \). Thus, \( \prod_{i \in S'} q_i \approx_{k_3} \prod_{i = 1}^{t} q_{q_i} \). By following an argument similar to (7) using \( q_{v_i} \) instead of \( q_{q_i} \), we see that \( a \not\approx_{k_3} q_a \). Also, following an argument similar to (8) using \( q_{q_i} \) instead of \( q_{q_i} \), we have \( a \not\approx_{k_3} q_a \).

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

Since \( \prod_{i \in T'} [l_i] \in H' \), then \( \prod_{i \in T'} [p_{q_i}] k_i \approx_{k_1} G_1 \). Hence, there exists \( q_{q_i} \equiv 3 \pmod{4} \) such that \( a' \not\in S' \). Choose \( b \) so that \( q_{q_i} \not\approx b \).

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

Suppose there exists an integer \( \delta \not\in S' \) such that \( q_{q_i} \equiv 1 \pmod{4} \) with \( (\frac{p}{q_{q_i}}) = (\frac{p}{q_{q_i}}) = -1 \). Then by replacing \( q_{q_i} \) with \( q_{q_i} \) in (8), it follows that \( a \not\approx_{k_2} q_{q_i} \).

We need to take care of the case that no such \( \delta \) exists.

Let \( T' = \{ il \mid l_i \equiv 1 \pmod{4} \} \) and \( (\frac{p}{q_i}) = -1 \). Since we have \( \prod_{i \in T'} [l_i] = \prod_{i \in T'} [l_i] \prod_{i \in T'} [l_i] \in H' \), it follows that \( \prod_{i \in T'} [l_i] \prod_{i \in T'} [l_i] \in H' \) as well. If no such \( q_{q_i} \) 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 \( H' \). Thus, it follows there exists an integer \( \delta' \in S' \) such that \( q_{q_i} \equiv 3 \pmod{4} \) with \( (\frac{p}{q_{q_i}}) = (\frac{p}{q_{q_i}}) = -1 \). Then it follows from (2) that \( \prod_{i \in S'} x_{q_{q_i}}^{k_i}(q_{q_i}) x_{q_{q_i}}^{k_i}(q_{q_i}) = - \prod_{i \in S'} x_{q_{q_i}}^{k_i}(q_{q_i}) \). Thus, we have \( (\prod_{i \in S'} q_i) q_{q_i} \not\approx_{k_2} \prod_{i \in S'} q_i \), so that \( a \not\approx_{k_2} q_{q_i} \).
There are similar arguments as in Subcase I to show that \( a \neq_{k_2} q_b \) and \( a \neq_{k_1} q_b q_a \).

In both subcases we have shown that \( [\mathcal{P}]_K \) has order 4. Thus, it follows that \( \langle [\mathcal{P}]_K, \ldots, [\mathcal{P}]_K \rangle \cong \langle \mathbb{Z}/4\mathbb{Z} \rangle^4 \), 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 \( H \) be the set of equivalence classes of primes that split in \( K \) with equivalence relation \( \sim' \), where \( l \sim' l' \) if \( p_l \equiv_{k_1} p_{l'} \). 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 \( p_{l''} \equiv_{k_1} p_{l'} \). As before, such an \( l'' \) exists. We see that \( H \cong \tilde{G}_1 \). It follows that either \( H \cong H \) or \(|H| = 2|H'| \).

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, \( d \neq d' \) but 2 ramifies in \( k_1 \). As before, in Cases 2B, 2D, 2E, and 2F, let \( l_0 \) be a prime which splits completely in \( K \) such that \( p_{l_0} \equiv_{k_1} p_2 \). In these cases, let \( q_0 = 2 \). In Cases 2A and 2C, 2D does not ramify in \( k_1 \). Let \( \tilde{H}' \) be the subgroup of \( \tilde{H} \) generated by \([l]'\) for \( i \leq m \), \( \prod_{i \in T_1}[l]' \), \( \prod_{i \in T_2}[l]' \), and \([l_0]'\) if 2 ramifies in \( K \). Let \( \tilde{G}_1' \) be the subgroup of \( \tilde{G}_1 \) generated by \( \tilde{G}_1', \prod_{i \in T_1}[p_i]_{k_1}, \prod_{i \in T_2}[p_i]_{k_1}, \) and \([p_2]_{k_1}\) if 2 ramifies in \( k_1 \). Let \( \tilde{H}'' \) be a subgroup of \( \tilde{H} \) so that \( \tilde{H} = \tilde{H}' \times \tilde{H}'' \). Then the 2-rank of \( \tilde{H}'' \) is \( s' \geq r' - 3 \).

We choose \( \tilde{H}'' \) to be the subgroup of \( \tilde{H} \) generated by \([l_j]'\) 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 \( \prod_{i \in T_3}[l_i]' \), \( \prod_{i \in T_4}[l_i]' \), \( \prod_{i \in T_5}[l_i]' \), \( \prod_{i \in T_6}[l_i]' \) \( \tilde{H}'' \). It follows as well that \( \prod_{i \in T_7}[p_i]_{k_1} \) \( \tilde{G}_1 \) 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 \( p_b \) is principal in \( k_1 \) as in Lemma 2.6. Let \( a \) 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 \( q_{c_2} \) is principal in \( k_2 \). Thus \( a \) is principal in \( k_2 \), or \( a \) belongs to the ideal class containing \( q_{a}, q_2 \), or \( q_{a} q_2 \) in \( k_2 \). It follows similarly that in Case 2B, \( a \) is principal in \( k_2 \), or \( a \) belongs to the ideal class containing \( q_{a}, q_2 \), or \( q_{a} q_2 \) in \( k_2 \), if \( 2 \nmid b \); otherwise \( a \) is principal in \( k_2 \), or \( a \) belongs to the ideal class containing \( q_{a}, q_{2}, q_{a} q_2 \), or \( q_{a} q_2 q_2 \) in \( k_2 \).

In Cases 2C, 2E, and 2F, \( a \) is principal in \( k_2 \), or \( a \) belongs to the ideal class containing \( q_{a}, q_2, q_{a} q_2, q_2, q_{a} q_2, q_{a} q_2, q_{a} q_2 q_2 \). Let \( S' \) be a nonempty subset of \( S \) and let \( \mathcal{B} = \prod_{i \in S'}[p_i]_{k_1} \). Again, we have \( \mathcal{B}^2 \approx_K a \), where \( a \) is a ramified ideal of \( k_2 \) such that \( \prod_{i \in S'}[q_i]_{k_2} \approx_{k_2} (\prod_{i \in S'}, [q_i])a \).
As in the previous cases, to show that \( a \) is not one of the ideals of \( k_2 \) which becomes principal in \( K \), we will also use the fact that \( \prod_{i \in S'} [l]_{y_i} \neq \prod_{i \in T} [l]_{y_i} \) where \( 1 \leq j \leq 6 \), since such products are in \( \hat{H} \). Fix \( \beta \in S \).

If there exists an integer \( \alpha_1 > m \) such that \( \alpha_1 \equiv 1 \pmod{4} \) and \( \alpha_1 \in S' \), then it follows similarly to (7) that \( a \) is not principal in \( k_2 \). If not, then \( \alpha_i \equiv 3 \pmod{4} \) for all \( i \in S' \). Also, since \( \prod_{i \in T} [p_q]_{k_i} \in \hat{G}_1 \), 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 \( q_{\beta} \) with \( q_{\beta}q_{\gamma_1} \) in (7) that \( a \) is not principal in \( k_2 \).

If there exists an integer \( \alpha_2 > m \) such that \( \alpha_2 \equiv 1 \pmod{4} \) and \( \alpha_2 \notin S' \), then by replacing \( q_{\gamma_1} \) with \( q_{\alpha_2} \) in (8), it follows that \( a \neq k_2 q_{\beta} \). If there is no such \( \alpha_2 \), then \( \Pi_{i \in T} [p_q]_{k_i} \in \hat{G}_1 \), then one of the \( q_i \)'s, say \( q_{\beta'} \equiv 3 \pmod{4} \). Since \( \prod_{i \in T} [p_q]_{k_i} \prod_{i \in T} [p_q]_{k_i} \in \hat{G}_1 \), 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 \( a \neq k_2 q_{\beta} \).

Suppose there exists \( \alpha_3 > m \) such that \( \alpha_3 \equiv 1 \pmod{4} \), \( \alpha_3 \in S' \), or there exists \( \alpha'_3 > m \) such that \( \alpha'_3 \equiv 1 \pmod{4} \), \( \alpha'_3 \in S' \), and \( \alpha'_3 \notin S' \). In both these cases it follows that \( a \neq k_2 q_{\beta} \).

If no such \( \alpha_3 \), \( \alpha'_3 \) exists, then \( \Pi_{i \in S'} [l]_{y_i} \) contains the subproduct \( \Pi_{i \in S} [l]_{y_i} \). Since \( \Pi_{i \in S} [p_q]_{k_i} \), then there is an integer \( y_i > m \) such that \( q_{y_i} \equiv 3 \pmod{4} \) and \( y_i \notin S' \). Thus, it follows from (2) that \( a \neq k_2 q_{\beta} \).

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 \( q_i \neq 7 \pmod{8} \) for all \( i > m \). These situations lead to the latter cases.

In each case it follows from (2) that

\[
\prod_{i \in S'} x^k_{\gamma_1, q_{\gamma_1}}(q_{\gamma_1}) x^k_{\gamma_3, q_{\gamma_3}}(q_{\gamma_3}) = \prod_{i \in S'} x^k_{\gamma_1, q_{\gamma_1}}(q_{\gamma_1}) = - \prod_{i \in S'} x^k_{\gamma_1, q_{\gamma_1}}(q_{\gamma_1}).
\]

Thus, \( a \neq k_2 q_{\beta} \).

If there exists \( \alpha_4 > m \) such that \( \alpha_4 \equiv 1 \pmod{4} \), \( \alpha_4 \in S' \), or if there exists \( \alpha'_4 > m \) such that \( \alpha'_4 \equiv 1 \pmod{4} \), \( \alpha'_4 \notin S' \), then it follows that \( a \neq k_2 q_{\beta} q_{\gamma_1} q_{\gamma_3} \).
If there does not exist any such \( \alpha_4, \alpha'_4 \), then \( \prod_{i \in S'} [l_i]' \) contains the sub-product \( \prod_{i \in S'} [l_i]' \), where \( S_2 = \{ i | i > m \text{ and } q_i \equiv 1 \pmod{8} \} \), and for all \( c > m \) such that \( q_c \equiv 5 \pmod{8} \), \( q_c \neq q_{\mu_i} \) for all \( i \in S' \). If we use the fact that \( \prod_{i \in T_i} [l_i]' \), \( \prod_{i \in T_i} [l_i]' \in \hat{H}' \), 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 \( \neq k_2 q_\beta q^2 \).

As in Subcase I of Cases 1B, 1C, 1E, 1F, 3B, and 3C, we have \( \prod_{i \in S'} p_i \approx k_1 \prod_{i=1}^t p_{\nu_i} \). Using arguments similar to those above it follows that a does not belong to the same ideal class containing \( q_b, q_p q_p, q_2 q_b, \) or \( q_\beta q_\gamma q_\beta \).

For Case 2B when \( 2|b \), we need to show that \( \neq k_2 q_\beta \) and \( \neq k_2 q_p q_\beta \). In this case, since \( E_2 \leq E_1(\sqrt{p}) \), it follows that \( \prod_{i=1}^t q_{\nu_i} \approx k_2 \prod_{i \in S'} q_i \). Suppose \( a \approx k_2 q_\beta \). Then

\[
\prod_{i=1}^t q_{\nu_i} \approx k_2 \prod_{i \in S'} q_i \approx k_2 \left( \prod_{i \in S'} q_i \right) q_\beta \approx k_2 \prod_{1 \leq i \leq t, \nu_i \neq 0} q_{\nu_i} \approx k_2 q_\beta \prod_{1 \leq i \leq t, \nu_i \neq 0} q_{\nu_i}.
\]

By an argument similar to the one used in showing that \( \neq k_2 q_\beta \), it follows that (10) does not occur. Hence, \( \neq k_2 q_\beta \). By an argument similar to the one used in showing that \( \neq k_2 q_p q_\beta \), it follows that \( \neq k_2 q_p q_\beta \).

Thus, \( a \) is not principal in \( K \), so that \( \mathbb{Q}(K) \) 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 \( \mathbb{Q}(\sqrt{627}p) \) 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.
ON THE IDEAL CLASS GROUP OF REAL Biquadratic Fields

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 \( p_l \) be a prime ideal of \( k_1 \) lying over \( l \) and let \( q_l \) 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 \( \chi_{k_1} \) and \( \chi_{k_2} \).

\[
\begin{array}{ccc|ccc|c}
3 & 11 & 19 & 3 & 11 & 19 & p \\
p_3 & -1 & -1 & 1 & q_3 & 1 & -1 & 1 & -1 \\
p_{11} & 1 & -1 & -1 & q_{11} & 1 & 1 & -1 & 1 \\
p_{19} & -1 & 1 & -1 & q_{19} & -1 & 1 & 1 & -1 \\
p_{2} & 1 & 1 & 1 & q_{2} & 1 & 1 & 1 & 1 \\
q_{p} & -1 & -1 & -1 & 1 & -1 & -1 \\
\end{array}
\]

Note that \( Fr_{E_2/k_2}, Fr_{E_2/k_2}, \) and \( Fr_{E_2/k_2} \) generate \( \text{Gal}(E_2/k_2) \). Thus, by Proposition 2.3, \( L_2 = E_2 \), so that \( h'_2 = 8 \).

Let \( \epsilon_i \) be the fundamental unit of \( k_i \). Since \( p \equiv 1 \pmod{4} \), then by Lemma 2.8, \( \epsilon_0 \) is not totally positive. Also, \( \sqrt{\epsilon_1} = \frac{1}{2}(\sqrt{1254} + 25\sqrt{2}) \). From the above table, we see that \( p_2 \) and \( p_3p_{11}p_{19}p_2 \) are principal ideals of \( k_1 \), while \( q_2 \) and \( q_3q_{11}q_{19}q_{2p} \) 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 \( [\text{Kur}] \), \( O_K^* = \langle -1, \epsilon_0, \epsilon_1, \sqrt{\epsilon_1\epsilon_2} \rangle \), and \( [O_K^*: O_{k_0}^*O_{k_1}^*O_{k_2}^*] = 2 \). By Herglotz’s Theorem, \( h' = \frac{1}{2}h'_0h'_1h'_2 = 16 \).

By applying Lemma 4.1, there exist primes \( l_1 \) and \( l_2 \) which split completely in \( K \) such that \( (\frac{q}{l_i}) = (\frac{3}{l}) \) and \( (\frac{q}{l_i}) = (\frac{11}{l}) \) for \( q = 3, 11, 19, \) and 19. Then \( p_{l_i} \approx k_i, \), and \( p_{l_i} \approx k_i, p_{l_i} \). Since \( l_i \) and \( l_2 \) split in \( k_0 \), then \( (\frac{p}{l_i}) = (\frac{p}{l_i}) = 1 \). It follows from the above table that \( q_{l_i} \approx k_2, q_3q_{19}, \) and \( q_{l_i} \approx k_2, k_{11}q_{3} \). Let \( \mathcal{P}_1, \mathcal{P}_2 \) be prime ideals of \( K \) lying over \( l_1, l_2 \), respectively. It follows from Lemmas 3.3 and 3.4 that

\[
\begin{align*}
\mathcal{P}_1^2 &\approx_K p_{l_1}q_{l_1} \approx_K p_{3}q_{3}q_{19} \approx_K q_{19}, \\
\mathcal{P}_2^2 &\approx_K p_{l_2}q_{l_2} \approx_K p_{11}q_{11}q_{3} \approx_K q_{3}.
\end{align*}
\]

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 \( q_{19}, q_3, \) and \( q_{19}q_3 \) are not principal in \( K \). Hence, \( [\mathcal{P}_1]_K \) and \( [\mathcal{P}_2]_K \) 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, $(\frac{12}{p}) = (\frac{p}{3}) = 1$, and $(\frac{14}{p}) = (\frac{p}{11}) = -1$. Again many other congruences are possible. We compute some of the values of the genus characters $\chi^{k_1}$ and $\chi^{k_2}$ below.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\chi^{k_1}(p)$</th>
<th>$\chi^{k_2}(p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p_3$</td>
<td>-1 11 19</td>
<td>3 11 19 p</td>
</tr>
<tr>
<td>$p_{11}$</td>
<td>1 -1 -1</td>
<td>q_3 1 -1 1 -1</td>
</tr>
<tr>
<td>$p_{19}$</td>
<td>-1 1 1</td>
<td>q_{19} -1 1 -1 1</td>
</tr>
<tr>
<td>$p_2$</td>
<td>1 1 1</td>
<td>q_2 1 1 1 1</td>
</tr>
<tr>
<td>$q_p$</td>
<td>-1 -1 1</td>
<td>p</td>
</tr>
</tbody>
</table>

Again, we see that $L_2 = E_2$, and that $q_2$ and $q_3$, $q_{11}$, $q_{19}$, $q_2$ are principal ideals of $k_2$. By Lemma 2.6, $\sqrt{e_2} = \frac{1}{2}(a\sqrt{2} + b\sqrt{1254p})$ for some $a, b \in \mathbb{Z}$. As in Case 1, $[O_K : O_{k_1}O_{k_2}^e] = 2$, so that $h' = 16$.

Let $l_1$ and $l_2$ be a prime which splits completely in $K$ such that $(\frac{q}{l_1}) = (\frac{q}{l_2}) = (\frac{q}{l_2})$ for $q = 3, 11, \text{ and } 19$. It follows that $p_{l_1} \approx k_1$, $p_3$ and $p_{l_2} \approx k_1$, $p_{19}$. Hence, $[p_{l_1}k_1]$ and $[p_{l_2}k_1]$ generate $G_1$. Since $(\frac{q}{l_1}) = (\frac{q}{l_2}) = 1$, we have $q_{l_1} \approx k_2$, $q_{3l_1}q_{19}$ and $q_{l_2} \approx k_2$, $q_{19}$. Let $[p_{l_1}]$ and $[p_{l_2}]$ be prime ideals of $K$ lying over $l_1$. By Lemmas 3.3 and 3.4 we have

$[p_{l_1}]_k \approx K p_{l_1}q_{l_1} \approx K p_{3l_1}q_{19} \approx K q_{19}\approx 1.$

Again, by Lemma 3.5, $q_{19}$ is not principal in $K$. Thus, $[p_{l_1}]_k$ has order 4 in $K$.

Now, let $l$ be any prime which splits completely in $K$. Since $[p_{l_1}]_k$ and $[p_{l_2}]_k$ generate $G_1$, we have $p_l \approx k_1$, $p_{l_1}^{e_1}p_{l_2}^{e_2}$ where $e_1$ and $e_2$ are integers. It follows that $(\frac{q}{l}) = (\frac{q}{l_1l_2})$ for $q = 3, 11, \text{ and } 19$. Also, since $l$ splits completely in $K$, $(\frac{q}{l}) = (\frac{q}{l_1l_2}) = 1$. Thus $q_l \approx k_2$, $q_{l_1}^{e_1}q_{l_2}^{e_2}$. Let $R_l$ be a prime ideal of $K$ lying above $l$. Then from above,

$[R_l]_k \approx K p_lq_l \approx K p_{l_1}^{e_1}p_{l_2}^{e_2}q_{l_1}^{e_1}q_{l_2}^{e_2} \approx K q_{19}$.

Thus, either $[R_l]_k$ has order less than or equal to 2, or $[R_l]_k^2 = [R_l]_k$. 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, \( \left( \frac{3}{p} \right) = \left( \frac{19}{p} \right) = \left( \frac{2}{p} \right) = 1 \) and \( \left( \frac{11}{p} \right) = -1 \). The values of the genus characters \( \chi^{k_1} \) and \( \chi^{k_2} \) are below.

\[
\begin{array}{cccc}
\chi^{k_1}(p_q) & \chi^{k_2}(q_q) \\
3 & 11 & 19 & p \\
p_3 & -1 & -1 & 1 \\
p_{11} & 1 & -1 & -1 \\
p_{19} & -1 & 1 & -1 \\
p_2 & 1 & 1 & 1 \\
q_\rho & 1 & -1 & -1 \\
\end{array}
\]

It follows that \( L_2 = E_2 \) again, and that \( q_2 \) and \( q_3 q_{11} q_{19} q_2 q_\rho \) are principal ideals of \( k_2 \). By Lemma 2.6, \( \sqrt{e_2} = \frac{1}{2}(a\sqrt{2} + b\sqrt{1254}) \) 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 \( \mathcal{P}_l \) be any prime ideal of \( K \) lying over \( l \). Since \( [p_3]_{k_1} \) and \( [p_{19}]_{k_1} \) generate \( G_1 \), then \( p_l \approx_{k_1} p^e_3 p^e_{11} p^e_{19} \), where \( e_i = 0, 1 \). Further, since \( \chi^{k_1}(p_l) = \chi^{k_2}(q_l) \), \( \chi^{k_1}(p_3) = \chi^{k_2}(q_3) \), and \( \chi^{k_1}(p_{19}) = \chi^{k_2}(q_{19}) \) for \( q = 3, 11, 19 \), and \( \chi^{k_2}(q_l) = \chi^{k_2}(q_{19}) = 1 \), it follows that \( q_l \approx_{k_2} q^e_3 q^e_{11} q_{19} \). Thus, by Lemmas 3.3 and 3.4,

\[
\mathcal{P}_l^2 \approx_K p^e_3 p^e_{11} p^e_{19} q^e_3 q^e_{11} q_{19} \approx_K (1) \text{.}
\]

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 \( \mathbb{Q}(\sqrt{p}) \), \( \mathbb{Q}(\sqrt{17}) \), and \( \mathbb{Q}(\sqrt{73}) \). 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 \( \mathbb{Q}(\sqrt{627}) \), \( \mathbb{Q}(\sqrt{627}\sqrt{p}) \) 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


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