Real Quadratic Fields With Class Numbers Divisible by Five

By Charles J. Parry

Abstract. Conditions are given for a real quadratic field to have class number divisible by five. If 5 does not divide m, then a necessary condition for 5 to divide the class number of the real quadratic field with conductor m or 5m is that 5 divide the class number of a certain cyclic biquadratic field with conductor 5m. Conversely, if 5 divides the class number of the cyclic field, then either one of the quadratic fields has class number divisible by 5 or one of their fundamental units satisfies a certain congruence condition modulo 25.

1. Introduction. While a necessary and sufficient condition for 3 to divide the class number of a real quadratic field has been given by Herz [3], no similar condition seems to exist for 5. In this article, we will extend the methods of Herz to obtain such a result. Although Weinberger [9] and Yamatoto [10] have proved the existence of infinitely many real quadratic fields with class number divisible by any integer n, their results are quite different from those of Herz and those of this article.

Certainly 5 divides the class number of one of the quadratic fields $k_1 = Q(\sqrt{m})$ or $k_2 = Q(\sqrt{5m})$ if and only if 5 divides the class number of their biquadratic compositum $K_1$. We show if 5 divides the class number of $K_1$ then 5 divides the class number of a certain imaginary cyclic biquadratic field $K_2$ with conductor $5D$, where $D$ is the discriminant of $k_1$. Conversely, if 5 divides the class number of $K_2$, then either 5 divides the class number of $K_1$ or one of three congruence conditions holds modulo 5 or 25 on the fundamental units of $k_1$ or $k_2$.

2. Notation.

\[ \xi = e^{2\pi i / 5} \]

$m$: a square free positive rational integer with $(5, m) = 1$.

$Q$: the field of rational numbers.

$k_1 = Q(\sqrt{m})$.

$k_2 = Q(\sqrt{5m})$.

$k_3 = Q(\sqrt{5})$.

$L = Q(\xi, \sqrt{m})$.

$K_1 = Q(\sqrt{5}, \sqrt{m})$.

$K_2 = Q(\sqrt{-10m + 2m\sqrt{5}})$: cyclic biquadratic subfield of $L$.

$K_3 = Q(\xi)$.

$D$ = discriminant of the field $k_1$.

$h = \text{class number of } L$. 

Received August 5, 1976; revised December 16, 1976.


Copyright © 1977, American Mathematical Society
\( h_i \) \((i = 1, 2, 3)\): class number of \( K_i \).

\( h^*_i \) \((i = 1, 2, 3)\): class number of \( k_i \).

\( \hat{E} \): the group of units of \( L \).

\( \hat{e} \): the subgroup of \( \hat{E} \) generated by the units of fields \( K_i \) \((i = 1, 2, 3)\).

\( \hat{e} \): the subgroup of \( \hat{e} \) generated by the units of the fields \( k_i \) \((i = 1, 2, 3)\).

\( Q_0 = (\hat{E} : \hat{e}) \).

\( Q_1 = (\hat{e} : \hat{e}) \).

\( e_i \) \((i = 1, 2, 3)\): the fundamental unit of the field \( k_i \).

3. Class Number Relations.

**Theorem 1.** \( 2h = h_1 h_2 \).

**Proof.** Since the Galois group of \( L/k_3 \) is bicyclic of order 4, it follows from Theorem 5.5.1 of Walter [8] that \( 2h^*_3 = Q_0 h_1 h_2 h_3 \). However, it is well known that \( h_3 = h^*_3 = 1 \).

To complete the proof we need to show \( Q_0 = 1 \). If \( E \in \hat{E} \), Theorem 1 of Parry [7] shows

\[
E^2 = \pm \xi e = \pm \xi^6 e,
\]

where \( e \in K_1 \). Thus,

\[
(E/\xi^3)^2 = \pm e.
\]

If \( e_1 = E/\xi^3 \notin K_1 \), then \( L = K_1(e_1) = K_1(\sqrt{\pm e}) \) so only the prime divisors of 2 in \( K_1 \) could ramify in \( L \). However, the prime divisors of 5 in \( K_1 \) ramify in \( L \). Thus, \( e_1 \in K_1 \) and so \( E = \xi^3 e_1 \in \hat{e} \). Hence, \( \hat{E} \subset \hat{e} \) so \( Q_0 = 1 \).

**Theorem 2.** \( 4h_1 = Q_1 h^*_1 h^*_2 \) with \( Q_1 = 1 \) or 2.

**Proof.** Immediate from Satz 1 of Kubota [5] and Satz 11 of Kuroda [6] since \( h^*_3 = 1 \) and the fundamental unit of \( k_3 \) has norm \(-1 \).

**Corollary 3.** \( 8h = Q_1 h^*_1 h^*_2 h_2 \).

4. Class Number Divisibility.

**Lemma 4.** If \( 5 \mid h_1 \), then \( 5 \mid h_2 \).

**Proof.** If \( M/K_1 \) is cyclic of degree 5, then \( M(\xi)/K_1 \) is cyclic of degree 10. A generator \( \sigma \) of the Galois group \( G(M/K_1) \) can be extended to an element of \( G(M(\xi)/K_1) \) by setting \( \xi^\sigma = \xi \). Hilbert’s Theorem 90 gives an element \( \alpha \in M(\xi) \) satisfying \( \alpha^{\sigma - 1} = \xi \). Moreover, \( \alpha \) is uniquely determined up to multiplication by \( \beta \in L \).

Let \( \rho \) be the unique element of \( G(M(\xi)/K_1) \) which has order 2 and define quantities \( \theta, a \) and \( e \) by \( \theta = \alpha + \alpha^2, a = \alpha^{1 + \rho} \) and \( e = \alpha^{4 - \rho} + \alpha^{4\rho - 1} \). Now \( a, e \in K_1 \), \( \theta \in M, M = K_1(\theta) \) and \( \theta^5 - 5a\theta^3 + 5a^2\theta - ae = 0 \). Since \( M/k_3 \) is dihedral, the non-trivial automorphism of \( K_1/k_3 \) can be extended to an automorphism \( \tau \) of \( M(\xi)/k_3 \) satisfying the following properties:

\[
\xi^\tau = \xi^4, \quad \tau^2 = 1, \quad \rho \tau = \tau \rho, \quad \tau \sigma = \sigma^4 \tau.
\]

If \( \beta = \alpha^{\tau - 1} \) then

\[
\beta^\sigma = (\alpha^{\tau - 1})^\sigma = \alpha^{\sigma^4 \tau - \sigma} = (\xi^4 \alpha)\tau/(\xi \alpha) = \xi \alpha^\tau / \xi a = \alpha^{\tau - 1} = \beta,
\]
so that \( \beta \in L \). Replace \( \alpha \) with \((1 + \beta)\alpha \) if \( \beta \neq -1 \) and with \((\xi - \xi^5)\) \( \alpha \) if \( \beta = -1 \). This gives \( \alpha = \alpha^5 \) so that \( \alpha^5 \in K_2 \) and \( \alpha \) is uniquely determined up to a factor \( \gamma \) of \( K_2 \). Thus we can take \( \alpha \) to be an integer of \( K_2 \) and so \( a \) and \( e \) will be integers of \( k_3 \). Theorem 1 of Parry [7] shows that the only units of \( K_2 \) are the units of \( k_3 \), so if \( \alpha^5 \) were a unit of \( K_2 \), then \( \alpha^5 \in K_1 \). This would mean that \( M = K_1(\alpha) = K_1(\sqrt[5]{\alpha^5}) \) and so \( M/K_1 \) would be a nonnormal extension. Thus, \( \alpha^5 \) is not a unit of \( K_2 \).

If \( 5 \mid h_1 \), then we may assume \( M/K_1 \) is unramified; and hence, \( M(\xi)/L \) is also unramified. Because \( M(\xi) = L(\xi^5) \), a prime ideal \( \mathfrak{p} \) of \( L \) can divide \((\alpha^5)\) if and only if \( \mathfrak{p}^5 \) divides \((\alpha^5)\). Since \( \alpha^5 \in K_2 \), a prime ideal \( \mathfrak{p} \) of \( K_2 \) will divide \((\alpha^5)\) if and only if \( \mathfrak{p}^5 \) divides \((\alpha^5)\). Since we may assume \( \alpha^5 \) is not divisible by a fifth power of another integer of \( K_2 \) (except units), it follows \((\alpha^5) = (\mathfrak{p}_1 \cdots \mathfrak{p}_t)^5 \) where \( \mathfrak{p}_1 \cdots \mathfrak{p}_t \) is a nonprincipal ideal of \( K_2 \) whose fifth power is principal. Thus, \( 5 \) divides \( h_2 \).

**Theorem 5 (Main Result).** If \( 5 \mid h_2 \), then either \( 5 \mid h_1 \) or the fundamental units \( e_1 = (a + b\sqrt{m})/2 \) of \( k_1 \) and \( e_2 = (c + d\sqrt{5m})/2 \) of \( k_2 \) satisfy one of the following conditions:

1. \( a \equiv 0 \) or \( b \equiv 0 \) (mod 25).
2. \( m \equiv \pm 2 \) (mod 5) and \( e_1 \equiv \pm e \) or \( \pm 7e \) (mod 25) where \( e = r \pm m^2\sqrt{m} \) with \( r = 9 \) or 12 according as \( m \equiv 2 \) or \(-2 \) (mod 5).
3. \( d \equiv 0 \) (mod 5).

Conversely, if \( 5 \mid h_1 \) or one of conditions (1)—(3) holds, then \( 5 \mid h_2 \).

**Proof.** We begin by reversing the roles of \( K_1 \) and \( K_2 \) in the proof of the preceding lemma. Thus, if \( 5 \mid h_2 \), then \( M/K_2 \) is an abelian unramified extension of degree 5 and \( M(\xi) = L(\alpha) \) with \( \alpha^5 \in K_1 \). If \( \alpha^5 \) is not a unit of \( K_1 \), then it follows as in Lemma 4 that \( 5 \mid h_1 \). If \( \alpha^5 = e \) is a unit of \( K_1 \), then \( \alpha \) may be replaced with \( \alpha^2 \) so that \( \alpha^5 = e = e_1 e_2 e_3 \) with \( e_i \in k_i \) \((i = 1, 2, 3)\) (see Theorems 1 and 2). Satz 119 of Hecke [2] shows that \( L(\sqrt[5]{\xi})/L \); and hence, \( M/K_2 \) will be an unramified extension if and only if

\[
(4) \quad x^5 \equiv e \mod (1 - \xi^5)
\]

is solvable in \( L \). By applying the relative norm function for \( L/K_1 \), it is seen that (4) is solvable if and only if

\[
(5) \quad x^5 \equiv e \mod (5\sqrt{5})
\]

is solvable in \( K_1 \). Applying the relative norm functions for \( K_1/k_i \) \((i = 1, 2, 3)\) to (5) shows that

\[
(6) \quad x^5 \equiv e_1 \mod (25),
\]

\[
(7) \quad x^5 \equiv e_2 \mod p_3^3,
\]

\[
(8) \quad x^5 \equiv e_3 \mod (5\sqrt{5})
\]

(where \( p_5 = (5, \sqrt{5m}) \)) must be solvable in \( k_1, k_2 \) and \( k_3 \), respectively. First of all, it is easy to see that (8) has no solution unless \( e_3 \) is the fifth power of a unit of \( k_3 \). Thus, we may take \( e_3 = 1 \) and \( \alpha^5 = e = e_1 e_2 \). Next observe (7) is solvable if and
only if \( e_2 \equiv u + v\sqrt{m} \) (mod 5) with \( v \equiv 0 \) (mod 5). Suppose \( e_2 = e_2' \) where \( e_2 \) is the fundamental unit of \( k_2 \). Certainly, we may assume that \( t \) is reduced modulo 5. Moreover, if \( t \not\equiv 0 \) (mod 5), then (7) has a solution if and only if

\[
x^5 \equiv e_2 \mod p_5^3
\]

has a solution; i.e. we may assume \( t = 0 \) or 1. If \( t = 1 \), then condition (3) of the theorem holds. If \( t = 0 \), then \( e_1 \not\equiv \pm 1 \), since otherwise \( \alpha \) would be a 10th root of unity. Hence, we may assume that (6) holds where \( e_1 = e_1 \) is the fundamental unit of \( k_1 \).

We need to determine exactly when

\[
(9) \quad x^5 \equiv e_1 \mod 25
\]

has a solution in \( k_1 \).

If \( m \equiv \pm 1 \) (mod 5), then (25) = \((p_1 p_2)^2\) in \( k_1 \) where \( p_1 \) and \( p_2 \) are distinct prime ideals. Now (9) has a solution if and only if

\[
(10) \quad x^5 \equiv e_1 \mod p_i^2
\]

has a solution for \( i = 1, 2 \). Also, the reduced residue system modulo 25 forms a reduced residue system modulo \( p_i^2 \); and the fifth powers modulo \( p_i^2 \) are precisely \( \pm 1 \) and \( \pm 7 \). If \( e_1 \equiv u + v\sqrt{m} \) (mod 25), then \( \pm 1 \equiv u^2 - m v^2 \) (mod 25); and since \( m \equiv \pm 1 \) (mod 5), either \( u \equiv 0 \) or \( v \equiv 0 \) (mod 5). It follows that \( u^2 \equiv \pm 1 \) or \( m v^2 \equiv \pm 1 \) (mod 25), and thus \( u \equiv \pm 1, \pm 7 \) or \( \sqrt{m v} \equiv \pm 1, \pm 7 \) (mod \( p_i^2 \)). Suppose

\[
e_1 \equiv u + v\sqrt{m} \mod p_i^2,
\]

where \( v \equiv 0 \) (mod 5). Thus, both \( e_1 \) and \( u \) are fifth power residues and \( v \equiv 0 \) (mod \( p_i \)). It follows that

\[
e_1 \equiv u \mod p_i^2,
\]

and so \( v\sqrt{m} \equiv 0 \mod p_i^2 \) which implies \( v \equiv 0 \) (mod 25). A similar argument shows that \( u \equiv 0 \) (mod 25) when \( u \equiv 0 \) (mod 5).

If \( m \equiv \pm 2 \) (mod 5), then 5 stays prime in \( k_1 \); and there are 600 reduced residues modulo 25, 24 of which are fifth powers. A complete set of fifth power residues may be obtained by taking all products from the sets

\[
S = \{ \pm 1, \pm 7, \pm m^2\sqrt{m}, \pm 7m^2\sqrt{m} \} \quad \text{and} \quad T = \{ \pm 1, r \pm m^2\sqrt{m} \},
\]

where \( r = 9 \) or 12 according as \( m \equiv 2 \) or \( m \equiv 3 \) (mod 5). Note that \( r^2 - m^4 \equiv 1 \) or \( -1 \) (mod 25) according as \( m \equiv 3 \) or \( m \equiv 2 \) (mod 5). Thus, only \( \pm 1 \) and \( \pm 7 \) times \( r \pm m^2\sqrt{m} \) can be units. It is now obvious that (9) has a solution if and only if (1) or (2) holds.

We have now proved that if \( 5 \mid h_2 \) and \( 5 \nmid h_1 \), then one of (1)–(3) must hold. Conversely, if one of (1)–(3) holds, set \( e = e_1 \) if (1) or (2) holds and \( e = e_2 \) if (3) holds. The above discussion shows that (4) has a solution for this choice of \( e \). Satz 119 of Hecke [2] shows that \( L(5\sqrt{e})/L \) is unramified so that \( 5 \mid h \). Theorem 1 shows \( 5 \mid h_1 \) or \( 5 \mid h_2 \). If \( 5 \mid h_1 \), then Lemma 4 shows \( 5 \mid h_2 \), also.
The following corollary gives a more convenient version of condition (2).

**Corollary 6.** The fundamental unit $e_1$ of $k_1$ satisfies condition (2) if and only if $\text{Tr}(e_1) \equiv \pm 1, \pm 7 \pmod{25}$ where $\text{Tr}$ denotes the trace function.

**Proof.** Certainly, if $e_1$ satisfies condition (2), then $\text{Tr}(e_1) \equiv \pm 1, \pm 7 \pmod{25}$. Conversely, suppose $e = e_1 \equiv a + b\sqrt{m} \pmod{25}$ with $\text{Tr}(e) \equiv 2a \equiv \pm 1, \pm 7 \pmod{25}$. Thus,

$$\pm 1 \equiv N(e) \equiv a^2 - b^2m \pmod{25},$$

so

$$\pm 4 \equiv 4a^2 - 4b^2m \equiv \text{Tr}(e)^2 - 4b^2m \equiv \pm 1 - 4b^2m \pmod{25}.$$ 

Since $m \not\equiv 0 \pmod{5}$, the choice of $\pm$ signs must be the same on both sides and, in fact, is the sign of $\text{Tr}(e)^2$. Thus,

$$4b^2m \equiv -3 \text{Tr}(e)^2 \pmod{25},$$

so

$$b^2m \equiv 18 \text{Tr}(e)^2 \equiv -7 \text{Tr}(e)^2 \pmod{25}.$$ 

Squaring gives

$$b^4m^2 \equiv -1 \pmod{25},$$

so

$$b \equiv -b^5m^2 \pmod{25}.$$ 

Now

$$b^2m \equiv -7 \text{Tr}(e)^2 \equiv -2 \text{Tr}(e)^2 \pmod{5},$$

so

$$b^2 \equiv \pm \text{Tr}(e)^2 \pmod{5},$$

where the sign is + if $m \equiv 3 \pmod{5}$ and − if $m \equiv 2 \pmod{5}$. If $m \equiv 3 \pmod{5}$, then

$$b \equiv \pm \text{Tr}(e) \pmod{5},$$

so

$$b \equiv -b^5m^2 \equiv \pm \text{Tr}(e)m^2 \pmod{25}.$$ 

Thus,

$$e \equiv a \pm \text{Tr}(e)m^2\sqrt{m} \pmod{25} \equiv -\text{Tr}(e)(12 \pm m^2\sqrt{m}) \pmod{25}.$$
If $m \equiv 2 \pmod{5}$, then
\[ b^2 \equiv -\text{Tr}(e)^2 \quad (\text{mod } 5), \]
so
\[ b \equiv \pm 7 \text{Tr}(e) \quad (\text{mod } 5). \]
Hence,
\[ b \equiv -b^5m^2 \equiv \pm 7 \text{Tr}(e)m^2 \quad (\text{mod } 25), \]
so
\[ e \equiv 13 \text{Tr}(e) \pm 7 \text{Tr}(e)m^2\sqrt{m} \quad (\text{mod } 25) \]
\[ \equiv -\text{Tr}(e)(12 \pm 7m^2\sqrt{m}) \quad (\text{mod } 25) \]
\[ \equiv \pm 7 \text{Tr}(e)(9 \pm m^2\sqrt{m}) \quad (\text{mod } 25). \]
Thus, in either case (2) is satisfied.

The distinction between conditions (1) and (2) of Theorem 5 is somewhat artificial as is seen by the following result.

**Corollary 7.** If $e_1$ satisfies condition (2), then $e_1^3$ satisfies condition (1).

**Proof.** Simply cube $e = r \pm m^2\sqrt{m}$ and note that $m^5 \equiv 7$ or $-7$ and $r \equiv 9$ or $12 \pmod{25}$ according as $m \equiv 2$ or $-2 \pmod{5}$.

We now classify those fields $K_2$ which have class number divisible by 5 into three types:

**Type 1.** Condition (1) or (2) of Theorem 5 is satisfied.

**Type 2.** Condition (3) of Theorem 5 is satisfied.

**Type 3.** $5$ divides $h_1$.

Type 3 fields can be subdivided into two further types:

**Type 3a.** $5$ divides $h_2^*$.  

**Type 3b.** $5$ divides $h^*_2$.

The next corollary gives the sought after condition for 5 to divide $h_1$.

**Corollary 8.** If $5 | h_2$ and $K_2$ is not of Type 1 or 2, then $5 | h_1$.

**Corollary 9.** If $K_2$ is both Type 1 and Type 2, then $25 | h_2$ and the 5-class group of $K_2$ is noncyclic.

**Proof.** Under our assumptions $L(\sqrt{5}e_1)$ and $L(\sqrt{5}e_2)$ are distinct unramified abelian extensions of $L$ of degree 5. There exist corresponding unramified abelian extensions $M_i/K_2$ and $M_2/K_2$ of degree 5 with $M_i \subset L(\sqrt{5}e_i)$ for $i = 1, 2$. Since $L(\sqrt{5}e_1) \neq L(\sqrt{5}e_2)$ we see $M_1 \neq M_2$. Thus, $M_0 = M_1M_2$ is an unramified abelian extension of $K_2$ of degree 25 with noncyclic Galois group. Thus, $25 | h_2$ and the 5-class group of $K_2$ is noncyclic.

**Corollary 10.** If $K_2$ is of Type 1 and Type 3b or Type 2 and Type 3a, then $25 | h_2$ and the 5-class group of $K_2$ is noncyclic.

**Proof.** If $K_2$ satisfies both Type 1 and Type 2 conditions, then we are done by Corollary 9. When $K_2$ is of Type 3a (3b), there exists a nonprincipal prime ideal $\mathfrak{p}$ of
$k_1$ ($k_2$) such that $p^5 = (r + s\sqrt{m})$ is principal. (Here we temporarily change notation to allow $m \equiv 0 \pmod{5}$ when $K_2$ is Type 3b.) If we can choose $\alpha = r + s\sqrt{m}$ so that 5 does not ramify in $L(\sqrt[5]{\alpha})$, then we are done. This is so because $L(\sqrt[5]{\alpha})/L$ and $L(\sqrt[5]{\epsilon_i})/L$ ($i = 1$ or 2 according as $K_2$ is Type 3b or 3a) will be distinct unramified abelian extensions of degree 5. At this point, we can use the proof of Corollary 9.

In order to see that $\alpha$ can be chosen properly, it will be necessary to consider three cases:

Case 1. $K_2$ Type 2 and Type 3a, $m \equiv \pm 1 \pmod{5}$. Here $(25) = (p_1, p_2)^2$ where $p_1$ and $p_2$ are prime ideals of $k_1$. There are 20 reduced residues modulo $p_2$ and the fifth powers are precisely $\pm 1, \pm 7$. Since $\epsilon_1$ is not a fifth power residue, the powers $\epsilon_1^j$ ($j = 0, \ldots, 4$) form a complete set of coset representatives for the subgroup of fifth power residues in the whole group modulo $p_2$. Thus, $\epsilon_1^j(r + s\sqrt{m})$ is a fifth power residue modulo $p_2^2$ for some $j$. We need to observe that $j$ does not depend on $i$. If

$$\epsilon_1^j(r + s\sqrt{m}) \equiv u + v\sqrt{m} \pmod{25},$$

then as in the proof of Theorem 5 we must have $u \equiv 0$ or $v \equiv 0 \pmod{25}$. Thus, $\alpha = \epsilon_1^j(r + s\sqrt{m})$ is a fifth power modulo 25 and Satz 119 of Hecke [2] shows $L(\sqrt[5]{\alpha})/L$ is an unramified extension.

Case 2. $K_2$ Type 2 and Type 3a, $m \equiv \pm 2 \pmod{5}$. Here $L(\sqrt[5]{\alpha})/L$ will be unramified if $\alpha$ is a fifth power residue modulo 25. Since 5 remains prime in $k_1$, there are 600 reduced residues in $k_1$ modulo 25 and 24 of these are fifth power residues. If $\mathcal{A}$ denotes the ring of algebraic integers of $k_1$, then the norm function defines a surjective homomorphism

$$N: (\mathcal{A}/25\mathcal{A})^* \rightarrow (\mathbb{Z}/25\mathbb{Z})^*.$$ 

The kernel of $N$ must have order 30 and the preimage, $H$, of $\{ \pm 1, \pm 7 \}$ has order 120. Note that $\epsilon_1$, $\alpha$ and the subgroup, $F$, of fifth power residues all belong to $H$. Since $\epsilon_1$ is not in $F$, the powers $\epsilon_1^j$ ($j = 0, \ldots, 4$) give a complete set of coset representatives for $F$ in $H$. Thus, $\epsilon_1^j \alpha \in F$ for some choice of $j$. If $\alpha$ is replaced by $\epsilon_1^j \alpha$, then $L(\sqrt[5]{\alpha})/L$ will be unramified.

Case 3. $K_2$ Type 1 and Type 3b, $m \equiv 0 \pmod{5}$. We shall now return to our standard notation and write $\alpha = r + s\sqrt{5m}$ with $(m, 5) = 1$. Now $L(\sqrt[5]{\alpha})/L$ will be unramified if and only if $\alpha$ is a fifth power residue modulo $p_5^2$ where $p_5 = (5, \sqrt{5m})$. There are 100 reduced residues modulo $p_5^2$, and the subgroup of fifth power residues is $F = \{ \pm 1, \pm 7 \}$. If $\mathcal{A}$ denotes the ring of algebraic integers of $k_2$, then the norm function defines a homomorphism

$$N: (\mathcal{A}/p_5^2\mathcal{A})^* \rightarrow (\mathbb{Z}/25\mathbb{Z})^*.$$ 

Since only integers congruent to $\pm 1 \pmod{5}$ can be norms, the image of $N$ has order 10. The kernel of $N$ must also have order 10 and the preimage, $H$, of $\{ \pm 1 \}$ has order 20. Note that $\epsilon_2$, $\alpha$ and $F$ all belong to $H$. Since $\epsilon_2 \notin F$ we have, as in Case 2, $\epsilon_2^j \alpha \in F$ for some $j$. This completes the proof.
Table I \((m = p)\)

<table>
<thead>
<tr>
<th>(h_2)</th>
<th>(h_2^*)</th>
<th>Type</th>
<th>(D)</th>
<th>(h_2)</th>
<th>(h_2^*)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>10</td>
<td>2</td>
<td>1429</td>
<td>180</td>
<td>2</td>
<td>3a</td>
</tr>
<tr>
<td>53</td>
<td>10</td>
<td>1</td>
<td>1493</td>
<td>250</td>
<td>18</td>
<td>1, 2</td>
</tr>
<tr>
<td>73</td>
<td>10</td>
<td>1</td>
<td>1597</td>
<td>250</td>
<td>2</td>
<td>1, 2</td>
</tr>
<tr>
<td>89</td>
<td>20</td>
<td>1</td>
<td>1621</td>
<td>320</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>20</td>
<td>2</td>
<td>1637</td>
<td>450</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>109</td>
<td>20</td>
<td>1</td>
<td>1721</td>
<td>400</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>124</td>
<td>40</td>
<td>2</td>
<td>1741</td>
<td>400</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>169</td>
<td>20</td>
<td>2</td>
<td>1756</td>
<td>320</td>
<td>2</td>
<td>3a</td>
</tr>
<tr>
<td>236</td>
<td>80</td>
<td>2</td>
<td>1777</td>
<td>370</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>241</td>
<td>40</td>
<td>1</td>
<td>1861</td>
<td>320</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>257</td>
<td>50</td>
<td>1, 2</td>
<td>1868</td>
<td>500</td>
<td>10</td>
<td>1, 3b</td>
</tr>
<tr>
<td>281</td>
<td>40</td>
<td>2</td>
<td>1913</td>
<td>250</td>
<td>2</td>
<td>1, 2</td>
</tr>
<tr>
<td>293</td>
<td>50</td>
<td>2</td>
<td>1916</td>
<td>320</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>313</td>
<td>50</td>
<td>2</td>
<td>1949</td>
<td>260</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>401</td>
<td>80</td>
<td>3a</td>
<td>1973</td>
<td>370</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>428</td>
<td>100</td>
<td>1</td>
<td>1996</td>
<td>400</td>
<td>6</td>
<td>2, 3a</td>
</tr>
<tr>
<td>433</td>
<td>90</td>
<td>1</td>
<td>2092</td>
<td>340</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>457</td>
<td>50</td>
<td>2</td>
<td>2348</td>
<td>500</td>
<td>2</td>
<td>1, 2</td>
</tr>
<tr>
<td>508</td>
<td>100</td>
<td>1, 2</td>
<td>2524</td>
<td>520</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>509</td>
<td>100</td>
<td>4</td>
<td>2572</td>
<td>500</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>541</td>
<td>80</td>
<td>1</td>
<td>2732</td>
<td>740</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>556</td>
<td>80</td>
<td>1</td>
<td>2876</td>
<td>640</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>557</td>
<td>130</td>
<td>2</td>
<td>2908</td>
<td>740</td>
<td>2</td>
<td>3a</td>
</tr>
<tr>
<td>617</td>
<td>130</td>
<td>1</td>
<td>2972</td>
<td>580</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>673</td>
<td>90</td>
<td>1</td>
<td>3336</td>
<td>1280</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>761</td>
<td>80</td>
<td>4</td>
<td>3548</td>
<td>740</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>764</td>
<td>200</td>
<td>1, 2</td>
<td>3644</td>
<td>1000</td>
<td>10</td>
<td>3b</td>
</tr>
<tr>
<td>796</td>
<td>160</td>
<td>2</td>
<td>3788</td>
<td>900</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>809</td>
<td>100</td>
<td>4</td>
<td>3932</td>
<td>1220</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>844</td>
<td>200</td>
<td>1</td>
<td>4124</td>
<td>680</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>857</td>
<td>170</td>
<td>1</td>
<td>4204</td>
<td>680</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>881</td>
<td>200</td>
<td>2</td>
<td>4252</td>
<td>820</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>892</td>
<td>260</td>
<td>2</td>
<td>4348</td>
<td>1220</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>908</td>
<td>180</td>
<td>2</td>
<td>4492</td>
<td>1780</td>
<td>10</td>
<td>2, 3b</td>
</tr>
<tr>
<td>937</td>
<td>130</td>
<td>2</td>
<td>4748</td>
<td>900</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>997</td>
<td>130</td>
<td>2</td>
<td>4924</td>
<td>1000</td>
<td>2</td>
<td>1, 2</td>
</tr>
<tr>
<td>1069</td>
<td>100</td>
<td>2</td>
<td>5116</td>
<td>1600</td>
<td>10</td>
<td>1, 3b</td>
</tr>
<tr>
<td>1084</td>
<td>200</td>
<td>1</td>
<td>5164</td>
<td>1960</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1093</td>
<td>250</td>
<td>2</td>
<td>5308</td>
<td>900</td>
<td>2</td>
<td>2, 3a</td>
</tr>
<tr>
<td>1097</td>
<td>170</td>
<td>2</td>
<td>5708</td>
<td>1220</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1129</td>
<td>180</td>
<td>2</td>
<td>5804</td>
<td>1000</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1193</td>
<td>290</td>
<td>2</td>
<td>5932</td>
<td>1220</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>1213</td>
<td>250</td>
<td>2</td>
<td>6044</td>
<td>1640</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1217</td>
<td>170</td>
<td>10</td>
<td>6124</td>
<td>1000</td>
<td>6</td>
<td>1, 2</td>
</tr>
<tr>
<td>1228</td>
<td>260</td>
<td>2</td>
<td>6284</td>
<td>1640</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1289</td>
<td>180</td>
<td>1</td>
<td>6316</td>
<td>1360</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1301</td>
<td>200</td>
<td>2</td>
<td>6652</td>
<td>1940</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1321</td>
<td>360</td>
<td>1</td>
<td>6796</td>
<td>2320</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1388</td>
<td>180</td>
<td>2</td>
<td>6892</td>
<td>1780</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1428</td>
<td>180</td>
<td>2</td>
<td>7132</td>
<td>2340</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7388</td>
<td>1300</td>
<td>10</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7628</td>
<td>1700</td>
<td>2</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7916</td>
<td>1360</td>
<td>10</td>
<td>3b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7996</td>
<td>1600</td>
<td>6</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8012</td>
<td>2900</td>
<td>2</td>
<td>1, 2</td>
</tr>
</tbody>
</table>
It is interesting to note that when \( m = 982 \), \( K_2 \) is of Types 1 and 3a and when \( m = 1123 \), \( K_2 \) is of Types 2 and 3b. However, 25 does not divide \( h_2 \) in either case!

**Corollary 11.** If \( K_2 \) is of both Type 3a and Type 3b, then \( 25 | h_2 \) and the 5-class group of \( K_2 \) is noncyclic.

**Proof.** Corollary 10 shows that we may assume that \( K_2 \) is of neither Type 1 nor Type 2. Thus, as in the proof of that corollary, we may choose \( \alpha_i \in K_i \) such that \( L(\sqrt[5]{\alpha_i})/L \) \((i = 1, 2)\) is an unramified abelian extension of degree 5. Moreover, we
may assume \((\alpha_i) = \psi_i^5\) where \(\psi_i\) is a nonprincipal prime ideal of \(k_i\) \((i = 1, 2)\). If \(L(\sqrt[5]{\alpha_1}) = L(\sqrt[5]{\alpha_2})\), then \(\alpha_1 = \beta^5\alpha_1^t\) for some \(\beta \in K_1\) and \(t = 1, 2, 3\) or \(4\). Applying the norm function for \(K_1/k_1\) gives \(\alpha_1^2 = (N(\beta)p_1^5)^5\), where \(p_1\) is a prime integer. Since \(L(\sqrt[5]{\alpha_1})/L\) is of degree 5, we must have \(L(\sqrt[5]{\alpha_1}) \neq L(\sqrt[5]{\alpha_2})\). The proof of Corollary 9 now applies.

**Corollary 12.** Let \(K_2\) be of Type \(i\) \((i = 1\) or \(2)\), \(\epsilon = \epsilon_i\) and \(\epsilon = e_i\) and both fifth roots are real. Then \(M = K_2(\theta)\) is an unramified abelian extension of \(K_2\) of degree 5 and \(\theta\) is a root of

\[f(x) = x^5 - 5N(\epsilon)x^3 + 5x - Tr(\epsilon),\]

where \(N(\epsilon)\) and \(Tr(\epsilon)\) denote the norm and trace of \(\epsilon\).

**Proof.** Merely reverse the roles of \(K_1\) and \(K_2\) in the proof of Lemma 4. Under our assumptions we can take \(\alpha = \sqrt[5]{\epsilon}\) and \(\alpha^2 = \sqrt[5]{\epsilon^2}\). It is easy to see \(a = N(\epsilon)\) and \(ae = Tr(\epsilon)\).

5. **Numerical Results.** Since \(K_2\) is an imaginary cyclic biquadratic field, its class number can be readily computed using a result of Hasse [1]. The formula is

\[h_2 = \frac{1}{2\ell^2} \left| \sum_{n \mod \ell} \chi(n)n \right|^2,
\]

where \(\ell\) is the conductor of \(K_2\), the summation is over the smallest reduced residue system modulo \(\ell\) and \(\chi(n) = (m/n)\chi_1(n)\). Here \((m/n)\) is the Jacobi symbol and \(\chi_1(n)\) is a primitive character modulo 5 defined by \(\chi_1(2) = i = \sqrt{-1}\). The conductor \(\ell = 5D\) where \(D\) is the discriminant of \(k_1\). When \(\ell\) is even, we can make the following simplification:

**Theorem 13.** If \(\ell\) is even, then

\[h_2 = \frac{1}{8} \left| \sum_{n \mod \ell/2} \chi(n) \right|^2.
\]

**Proof.** Note that

\[\chi(n + \ell/2) = \left(\frac{m}{n + \ell/2}\right)\chi_1(n + \ell/2) = \left(\frac{m}{n + \ell/2}\right)\chi_1(n),
\]

since \(\ell/2 = 10m\). Now either \(m\) is odd or \(m = 2r\) with \(r\) odd. In the first case \(m \equiv 3 \mod 4\) and in both cases \(n\) is odd. In the former case

\[\left(\frac{m}{10m + n}\right) = (-1)((m-1)/2)(10m+n-1)/2 \left(\frac{10m + n}{m}\right)
\]

\[= (-1)^{(n+1)/2} \left(\frac{n}{m}\right) = (-1)^{(n+1)/2}(-1)^{(n-1)/2} \left(\frac{m}{n}\right)
\]

\[= - \left(\frac{m}{n}\right).
\]
In the second case
\[
\left(\frac{m}{10m + n}\right) = \left(\frac{2r}{20r + n}\right) = \left(\frac{2}{20r + n}\right) \left(\frac{r}{20r + n}\right)
\]
\[
= \left(\frac{2}{n + 4}\right) \left(\frac{r}{n}\right) = -\left(\frac{2}{n}\right) \left(\frac{r}{n}\right) = -\left(\frac{m}{n}\right).
\]

In either case \(\chi(n + \lfloor/2) = -\chi(n)\) so
\[
\sum_{n \pmod{\lfloor}} \chi(n)n = \sum_{n \pmod{\lfloor/2}} \chi(n)n + \chi(n + \lfloor/2)(n + \lfloor/2)
\]
\[
= \sum_{n \pmod{\lfloor/2}} \chi(n)n - \chi(n)(n + \lfloor/2) = -\lfloor/2 \sum_{n \pmod{\lfloor/2}} \chi(n).
\]

The desired result is now immediate.

Using FORTRAN programs, we have computed \(h_2\) for all values of \(m < 2000\) where \(m = p^i 2^j\) with \(p\) prime. In the tables above we list all such values of \(m\) with 5 dividing \(h_2\). The type (or types) of each field was determined using the table of Ince [4] and a program to compute \(e_2\) (or \(e_2\) modulo 100 when overflow occurred in double precision) when \(5m > 2025\). If Corollary 10 did not show \((h_2^2, 5) = 1\) and \(m > 405\), then \(h_2^2\) was computed. This value appears in the tables whenever we computed it.

Department of Mathematics
Virginia Polytechnic Institute & State University
Blacksburg, Virginia 24061