On the Class Number of Relative Quadratic Fields

By Charles J. Parry

Abstract. We describe class number relations between certain pairs of algebraic number fields, both of the same degree over the rational numbers. This relationship is discussed in great detail when the common degree is equal to 4. Some numerical results are given in this case.

1. Introduction. We shall describe pairs of algebraic number fields $K_1$ and $K_2$ which satisfy the following properties:
   (1) Both $K_1$ and $K_2$ are quadratic extensions of a field $L$.
   (2) $K_1$ is totally real.
   (3) $K_2$ is totally imaginary.
   (4) There exists an odd prime $l$ such that $l$ divides the class number of $K_2$ whenever $l$ divides the class number of $K_1$.
   (5) If $l$ divides the class number of $K_2$, then $l$ divides the class number of $K_1$; or there exists a unit of $K_1$ which satisfies a certain congruence condition.

The results obtained here are extensions of earlier works of Herz [4] and Parry [7].

2. Notation.
   $l$: odd prime number.
   $\zeta = e^{2\pi il/l}$.
   $Q$: the field of rational numbers.
   $h(\cdot)$: class number of the field (\).
   $L$: a totally real algebraic number field.
   $K_3$: a totally imaginary extension of $L$ of degree 2 which contains $\zeta$. We assume $l$ does not divide $h(K_3)$.
   $K_2$: a totally imaginary quadratic extension of $L$ with $K_2 \neq K_3$.
   $K = K_2(\zeta)$: bicyclic biquadratic extension of $L$.
   $K_1$: maximal real subfield of $K$.
   $\delta = (-1)^{(l-1)/2}$.
   $k_3 = Q(\sqrt{\delta l})$: a quadratic subfield of $K_3$.
   $m$: a square free rational integer with $m > 0$ if $l \equiv 3 \pmod{4}$.
   $k_1 = Q(\sqrt{m})$.
   $k_2 = Q(\sqrt{\delta lm})$.
   $E_\cdot$: unit group of the field $\cdot$. 

Received August 4, 1977; revised February 16, 1978.
Copyright © 1978, American Mathematical Society
\[ W_\omega \text{: the group of roots of unity of the field } \omega. \]

\[ G(\omega) \text{: Galois group of the extension } (\omega). \]

3. **The Main Result.** Our primary goal is to prove the following theorem which establishes a relation between the congruences \( h(K_1) \equiv 0 \pmod{l} \) and \( h(K_2) \equiv 0 \pmod{l} \).

**Theorem 1.** The prime number \( l \) divides \( h(K_2) \) if and only if \( l \) divides \( h(K_1) \) or

\[ x^l \equiv e \pmod{(1 - \omega)^l} \]

is solvable in \( K \) for some unit \( e \) of \( K_1 \) which is not an \( l \)th power.

Taking \( l = 3 \) and \( L = \mathbb{Q} \) gives Theorem 6 of Herz [4]. Letting \( l = 5 \), \( L = \mathbb{Q}(\sqrt{5}) \) and \( K_1 = L(\sqrt{m}) \) gives Theorem 5 of Parry [7].

We now begin the proof of the main theorem.

**Proof of Theorem 1.** If \( l \) divides \( h(K_1) \), then there exists an abelian unramified extension \( M \) of \( K_1 \) of degree \( l \). We first show that \( M/L \) is normal.

Since \( (K_1 : L) = 2 \), either \( M/L \) is normal or there exists \( M' \subset M \) with \( M'/L \) normal and \( M'/K_1 \) is an unramified bicyclic extension of degree \( l^2 \). Let \( H = G(M/M') \) and let \( \tau \in G(M/L) \) with \( \tau \notin G(M/K_1) \). If \( \sigma \in H \), then there exists a prime ideal \( \mathfrak{p} \) of \( K_1 \) with \( (M/K_1)/\mathfrak{p} = \sigma \). Now \( \sigma \tau^{-1} = (M/K_1)/\tau(\mathfrak{p}) \) and \( \tau(\mathfrak{p}) = \mathfrak{q} \) is an ideal of \( L \). Since \( l \) does not divide \( h(L) \) (otherwise \( l|h(K_3) \) contrary to assumption), \( \mathfrak{q}^a \) is principal for some integer \( a \) with \( (a, l) = 1 \). Thus

\[ 1 = \left( \frac{M/K_1}{\mathfrak{q}^a} \right) = \left( \frac{M/K_1}{\mathfrak{p}} \right)^a \left( \frac{M/K_1}{\tau(\mathfrak{p})} \right)^a = a^a(\tau \sigma \tau^{-1})^a. \]

Hence \( (\tau \sigma \tau^{-1})^a = \sigma^{-a} \), and so \( \sigma \tau \tau^{-1} = \sigma^{-1} \), because \( (a, l) = 1 \). Thus, \( H \) is a normal subgroup of \( G(M/L) \), and so \( M/L \) is a normal extension.

Now \( M(\xi)/K_1 \) is cyclic of degree \( 2l \), and 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 \( \xi' = \xi \). Hilbert’s Theorem 90 gives an element \( \alpha \in M(\xi) \) satisfying \( \alpha^o = \xi \). Moreover, \( \alpha \) is uniquely determined up to multiplication by \( \beta \in K \).

Since \( l^4 h(L) \), \( M/L \) must be dihedral. Thus, the nontrivial automorphism of \( K_1/L \) can be extended to an automorphism \( \tau \) of \( M(\xi)/L \) satisfying the following properties:

\[ \xi \tau = \xi^{-1}, \quad \tau^2 = 1, \quad \tau \sigma = \sigma^{-1} \tau, \quad \rho \tau = \tau \rho, \]

where \( \rho \) is the unique element of \( G(M(\xi)/K_1) \) of order 2. If \( \beta = \alpha^{-1} \), then

\[ \beta^o = (\alpha^{-1})^o = \alpha^{-1} \tau^{-\sigma} = (\xi^{-1} \alpha)^\tau/(\xi \alpha) = \xi \alpha^\tau/\xi \alpha = \alpha^{-1} = \beta, \]

so that \( \beta \in K \). Replace \( \alpha \) with \( (1 + \beta) \alpha \) if \( \beta \neq -1 \) and with \((\xi - \xi^{-1}) \alpha \) if \( \beta = -1 \). This gives \( \alpha = \alpha^\tau \) so that \( \alpha^l \in K_2 \), and \( \alpha \) is uniquely determined up to a factor \( \gamma \) of \( K_2 \).

If \( \alpha^l \) is a unit of \( K_2 \), then Theorem 1 of Parry [8] shows that \( \alpha^{2l} = \omega \mu \), where \( \omega \in K_2 \) is a root of unity and \( \mu \in L \) is a unit. Since \( K_2 \neq K_3 \), \( \omega^n = 1 \) where \( (n, l) = 1 \). Replacing \( \alpha \) with \( \alpha^{2\gamma}, \mu \) with \( \mu^n \) and \( \xi \) with \( \xi^{2\gamma} \) gives that \( \alpha^l = \mu \), a unit of \( L \) and...
hence of $K_1$. This means that $M = K_1(\alpha) = K_1(\sqrt{\mu})$ and so $M/K_1$ is a nonnormal extension, contrary to hypothesis. Thus, $\alpha^l$ is not a unit of $K_2$.

Because $M(\xi) = L(\sqrt[\ell]{\alpha^l})$ is an unramified extension of $K$, a prime ideal $\mathfrak{p}$ of $K$ can divide $(\alpha^l)$ if and only if $\mathfrak{p}^l$ divides $(\alpha^l)$. Since $\alpha^l \in K_2$, a prime ideal $\mathfrak{p}$ of $K_2$ will divide $(\alpha^l)$ if and only if $\mathfrak{p}^l$ divides $(\alpha^l)$. Since we may assume $\alpha^l$ is not divisible by an $l$th power of any integer of $K_2$ (except units), it follows that $(\alpha^l) = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^l$ where $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ is a nonprincipal ideal of $K_2$ whose $l$th power is principal. Thus, $l$ divides $h(K_2)$.

Assume now that $l$ divides $h(K_2)$. By reversing the roles of $K_1$ and $K_2$ in the first part of the proof we have that $M/K_2$ is an abelian unramified extension of degree $l$ and $M(\xi) = K(\alpha)$ with $\alpha^l \in K_1$. If $\alpha^l$ is not a unit of $K_1$, then it follows as above that $l$ divides $h(K_1)$. Assume $\alpha^l = e$ is a unit of $K_1$, and let $\mathfrak{p}$ in $K$ be a prime divisor of $(1 - \xi)$. If $\mathfrak{p}^a || (1 - \xi)$, then Satz 119 of Hecke [3] shows that $x^l \equiv e \pmod{\mathfrak{p}^a}$

has a solution $x \in K$. Since $\mathfrak{p}$ was an arbitrary prime divisor of $(1 - \xi)$, it follows by use of the Chinese Remainder Theorem that $x^l \equiv e \pmod{(1 - \xi)^l}$

has a solution $x \in K$.

The final portion of Theorem 1 will be proved as a corollary to the following theorem.

**Theorem 2.** For some integer $t$ with $-1 \leq t \leq 3$,

$$2^t h(K)h(L)^2 = Q_0 h(K_1)h(K_2)h(K_3),$$

where $Q_0 = (E_K : W_K E_{K_1} E_{K_2} E_{K_3})$. Moreover, $Q_0$ divides $2^n$ where $n = (L : Q)$. If $\sqrt{-1} \notin K$, then $t = 2$ or $t = 1$ according as there exist positive units $e_1$ and $e_2$ of $L$, such that $K_1 = L(\sqrt{e_1})$ and $K_2 = L(\sqrt{-e_2})$ or not.

Before proving this theorem, we need some technical results. For more details and definitions, we refer the reader to Walter [9], [10]. Let $F_0 \subset F_1 \subset F_2$ be a tower of algebraic number fields. Define

$$U_{F_0}^* = \{e \in E_{F_2} | e^n \in E_{F_0} \text{ for some } n \in \mathbb{Z}, n \neq 0\}$$

and

$$I(F_1/F_0) = (E_{F_1} \cap U_{F_0}^* : W_{F_1} E_{F_0}).$$

**Lemma A.** $I(F_2/F_0) = I(F_2/F_1)I(F_1/F_0)$ and $I(F_2/F_1)$ divides $(F_2 : F_1)$.

**Proof.** See Section 4 of [10].

In the proof of Theorem 2 we need the value of $M = I(K/L)/\prod_{i=1}^3 I(K_i/L)$.

**Lemma B.** $M = 2^c$ with $-2 \leq c \leq 1$. If $\sqrt{-1} \notin K$, then $c = -1$ or 0, according as there exist units $\epsilon_1 > 0$ and $\epsilon_2 > 0$ of $L$ such that $K_1 = L(\sqrt{\epsilon_1})$ and $K_2 = L(\sqrt{-\epsilon_2})$ or not.
Proof. The first assertion is immediate from Lemma A. We divide the proof of the second assertion into three cases.

Case 1: \( I(K_i/L) = 2 \) for exactly one \( i, i = 1, 2 \) or 3. It follows from Lemma A that \( I(K/L) = 2 \) and so \( M = 1 \).

Case 2: \( I(K_i/L) = 2 \) for two or more \( i \)'s. Say \( I(K_1/L) = I(K_2/L) = 2 \). Lemma 4.2 of [10] tells us that this can happen if and only if there exist positive units \( e_1 \) and \( e_2 \) of \( L \) such that \( K_1 = L(\sqrt{e_1}) \) and \( K_2 = L(\sqrt{-e_2}) \). Thus, \( K_3 = L(\sqrt{-e_1e_2}) \); and the same lemma tells us that \( I(K_3/L) = 2 \). Set \( e_1 = \sqrt{e_1} \) and \( e_2 = \sqrt{-e_2} \), and suppose that \( e_1e_2 = \sqrt{-e_1e_2} \in WKE_L \). Then \( e_1e_2 = \omega e \) with \( \omega \in W_K \) and \( e \in E_L \). Now \( -\omega^2 = e_1e_2/e^2 \) is a positive root of unity of \( L \). Thus, \( \omega^2 = -1 \), contradicting the hypothesis that \( \sqrt{1} \notin K \). Hence, \( e_1e_2 \notin WKE_L \) and so \( e_1 \) and \( e_2 \) determine distinct cosets of \( WKE_L \) in \( U_L^* \). Thus, \( 4 \leq I(K/L) \leq 4 \), and so \( M = 1/2 \) as desired.

Case 3: \( I(K_i/L) = 1 \) for \( i = 1, 2, 3 \). If \( e \notin K_i \), then \( e^4/nK/L(e) \in W_K \) so that \( e^4 \in WKE_L \). Suppose \( \omega = \omega e \) with \( \omega \in W_K \) and \( e \in E_L \). By hypothesis, we can choose \( \omega \) to have odd order, say \( \omega' = 1 \) with \( r \) odd. Choose \( s \) so that \( 4s \equiv -1 \pmod{r} \). Now \( (\omega e)^4 = e \in E_L \). Thus, \( L(e \omega^4) \) is a subfield of \( K \) which is not \( K \), because \( K/L \) is a normal extension of degree 4 and \( \sqrt{1} \notin K \). Moreover, \( L(e \omega^4) \neq K_i \) for \( i = 1, 2, 3 \), because \( I(K_i/L) = 1 \). Thus, \( L(e \omega^4) = L \), and so \( e \in WKE_L \). Thus, \( I(K/L) = 1 = M \).

Proof of Theorem 2. Since \( G(K/L) \) is bicyclic of order 4, it follows from Theorem 5.5.1 of [9] that

\[
h(K)h(L)^2/h(K_1)h(K_2)h(K_3) = 2^{b - 1}Q_0M,
\]

where \( b = 0 \) unless \( \sqrt{-1} \in K \). If \( \sqrt{-1} \in K \), then \( b = 0 \) or 1. Thus

\[
2^t h(K)h(L)^2 = Q_0 h(K_1)h(K_2)h(K_3)
\]

with \( t = 1 - (b + c) \) where \( M = 2^c \). The restrictions on \( t \) are now immediate from Lemmas A and B. The bounds on \( Q_0 \) are immediate from Lemma 5.4.1 of [9].

Corollary 1. If \( l \) divides \( h(K_1) \) or \( x^l \equiv e \pmod{(1 - \zeta)^l} \) is solvable in \( K \) for some unit \( e \) of \( K_1 \), which is not an \( l \)th power, then \( l \) divides \( h(K_2) \).

Proof. If \( l \) divides \( h(K_1) \), then Theorem 1 applies to give the desired result. Assume \( l \) does not divide \( h(K_1) \) and that \( x^l \equiv e \pmod{(1 - \zeta)^l} \) is solvable for some unit \( e \) of \( K_1 \) which is not an \( l \)th power in \( K_1 \). Satz 119 of Hecke [3] shows that \( K(\sqrt{e}) \) is an abelian unramified extension of \( K \) of degree \( l \). Thus, \( l|h(K) \). By assumption \( l \) divides neither \( h(K_1) \) nor \( h(K_3) \). Theorem 2 shows \( l|h(K_2) \).

From now on we shall take \( K_3 = Q(\zeta) \) where \( l \) is a regular prime. If \( l \equiv 3 \pmod{4} \), set \( K_1 = L(\sqrt{m}) \) and \( K_2 = L(\sqrt{-lm}) \).

Corollary 2. Let \( l \equiv 3 \pmod{4} \) be a regular prime. If \( l \) divides \( h(k_1) \), then \( l \) divides \( h(k_2) \). If \( l \) divides \( h(k_2) \), either \( l \) divides \( h(k_1) \) or the congruence

\[
x^l \equiv e \pmod{(1 - \zeta)^l}
\]

has a solution for some unit \( e \) of \( K_1 \) (\( e \) not an \( l \)th power in \( K_1 \)).

Proof. If \( l \) divides \( h(k_1) \) \((i = 1 \text{ or } 2) \), then class field theory shows \( l \) divides \( h(k_1) \).
CLASS NUMBER OF RELATIVE QUADRATIC FIELDS 1265

(i = 1 or 2); because \( K_i/k_i \) is an extension of degree \( (l-1)/2 \). The desired results are now immediate from Theorem 1.

If \( l \equiv 1 \) (mod 4), there are two cases to consider according as \( m \) is positive or negative. First, assume \( m > 0 \) and set \( K_1 = L(\sqrt{m}) \) and \( K_2 = L((\xi - \xi^{-1})\sqrt{m}) \).

**COROLLARY 3.** If \( l \) divides \( h(k_1) \) or \( h(k_2) \), then \( l \) divides \( h(K_2) \).

**Proof.** Here both \( k_1 \) and \( k_2 \) are subfields of \( K_1 \) of index \( (l-1)/2 \). The result follows as in Corollary 2.

Next if \( m < 0 \), set \( K_2 = L(\sqrt{-m}) \) and \( K_1 = L((\xi - \xi^{-1})\sqrt{m}) \).

**COROLLARY 4.** If \( l \) divides \( h(k_1) \) or \( h(k_2) \), then either \( l \) divides \( h(K_1) \) or the congruence

\[
x^l \equiv e \mod (1 - \xi)^l
\]

has a solution for some unit \( e \) of \( K_1 \) which is not an \( l \)th power.

**Remark.** If \( l \equiv 5 \) (mod 8), then

\[
L((\xi - \xi^{-1})\sqrt{m}) = L(\sqrt{-e}\sqrt{lm}),
\]

where \( e \) is the fundamental unit of \( k_3 \).

4. \( l = 5 \). When \( m > 0 \), this case has been discussed in great detail by Parry [7]. Here we shall only consider the case \( m < 0 \). It will be convenient to replace \( m \) with \(-m\) so that \( m > 0 \). Thus, \( k_1 = Q(\sqrt{-m}) \) and \( k_2 = Q(\sqrt{-5m}) \). Without loss of generality, we shall assume \((5, m) = 1 \).

Here \( K_2 = Q(\sqrt{5}, \sqrt{-m}) \) and \( K_1 = Q(\sqrt{e}\sqrt{5m}) \), where \( e = (1 + \sqrt{5})/2 \). Set \( G = m \) or \( 4m \) according as \( m \equiv 3 \) (mod 4) or not.

**THEOREM 3.** If \( 5 \) divides \( h(K_1) \), then \( 5 \) divides \( h(k_1) \) or \( h(k_2) \). Conversely, if \( 5 \) divides \( h(k_1) \) or \( h(k_2) \), then either \( 5 \) divides \( h(K_1) \) or the congruence

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

has a solution for some unit \( e \) of \( K_1 \) which is not a fifth power.

**Proof.** If \( 5 \) divides \( h(K_1) \), then Theorem 1 gives \( 5 \) divides \( h(K_2) \). Satz 1 of Kubota [6] shows \( h(K_2) = \frac{1}{2}Q^*h(k_1)h(k_2) \) where \( Q^* = 1 \) or 2. Thus, \( 5 \) divides \( h(k_1) \) or \( h(k_2) \). The converse is immediate from Corollary 4.

Our primary goal of this section is to characterize those units \( e \) of \( K_1 \), for which the congruence of Theorem 3 has a solution. Since \( K_1/Q \) is cyclic (see Kaplansky [5, Exercise 4, p. 53]), \( K_1 \) has three fundamental units. It follows from Hasse [1] that there exists a relative fundamental unit \( E \) of \( K_1 \) with relative norm equal to \( \pm 1 \), such that either \(-1, E, E' \) and \( e \) generate the whole group of units of \( K_1 \) or they generate a subgroup of index 2 in the whole group of units of \( K_1 \). Here \( E' \) is obtained by applying an automorphism of order 4 to \( E \). Since the unit \( e \) of Theorem 3 may be replaced by \( e^2 \), we may always assume that \( e \) is in the subgroup generated by \( E, E' \) and \( e \). (In all of our examples, this set of units is actually fundamental.) Set \( \Omega = \sqrt{e}\sqrt{5G} \) and \( \Omega' = \sqrt{-e'}\sqrt{5G} \), where \( e' = (1 - \sqrt{5})/2 \). Also, let \( \eta = (\sqrt{5}, \Omega) \) be the prime divisor of \( 5 \) in \( K_1 \). Let \( E \equiv a + b\sqrt{5} + c\Omega + d\Omega' \mod(5\eta) \).

**THEOREM 4.** There exists a unit \( e \) of \( K_1 \) (e not a fifth power in \( K_1 \)) such that
has a solution $x \in K$ if and only if $E$ satisfies one of the following conditions:

(1) $b \equiv c \equiv d \equiv 0 \pmod{5}$.

(2) $a \equiv \pm 1, \pm 7 \pmod{25}$ and $b \equiv 0, 2c \equiv d \pmod{5}$.

(3) $G \equiv \pm 1 \pmod{5}$ and

$$E \equiv \pm a(1 + \sqrt{5} \pm g\Omega) \text{ or }$$

$$E \equiv \pm a(1 - \sqrt{5} \pm g\Omega) \pmod{(5\mathfrak{p}_5)},$$

where $a \equiv 6$ or $8 \pmod{25}$ and $g = 1$ or $2$ according as $G \equiv 1$ or $-1 \pmod{5}$.

(4) $G \equiv \pm 2 \pmod{25}$ and

$$E \equiv \pm a(1 + 2\sqrt{5} \pm g(\Omega + \Omega')) \text{ or }$$

$$E \equiv \pm a(1 - 2\sqrt{5} \pm g(\Omega - \Omega')) \pmod{(5\mathfrak{p}_5)},$$

with $a \equiv 3$ or $4 \pmod{25}$ and $g = 1$ or $2$ according as $G \equiv 2$ or $-2 \pmod{5}$.

**Proof.** Assume the congruence

(5) $x^5 \equiv e \pmod{(1 - \xi)^5}$

has a solution in $K$. By applying the relative norm function for $K/K_1$, it is seen that (5) has a solution if and only if

(6) $x^5 \equiv e \pmod{5\mathfrak{p}_5}$

has a solution in $K_1$. Suppose $e = E^rE'^s$. Applying the norm function for $K_1/k_3$, we see

$$x^5 \equiv e^{2t} \pmod{5\sqrt{5}}$$

must have a solution in $k_3$. This is only possible if $t \equiv 0 \pmod{5}$. Hence, we may take $t = 0$. First, suppose that exactly one of $r$ or $s$ is congruent to $0$ modulo $5$. By taking conjugates, we may assume $s = 0$; and by replacing $e$ with $e^i$ ($i = 1, 2, 3$ or $4$), we may assume $r = 1$. Thus

(7) $x^5 \equiv E \pmod{5\mathfrak{p}_3}$

has a solution. Since the only fifth powers ($mod \ 5\mathfrak{p}_3$) are $\pm 1, \pm 7$, it follows that $b \equiv c \equiv d \equiv 0 \pmod{5}$. This gives condition (1) of the theorem. Conversely, if (1) holds, then taking the relative norms, we get

$$a^2 \equiv N(E) \equiv \pm 1 \pmod{25}$$

so that $a \equiv \pm 1, \pm 7 \pmod{25}$, and hence (7) has a solution. Suppose now that $rs \not\equiv 0 \pmod{5}$. By replacing $e$ with $e^i$ where $i = 1, 2, 3$ or $4$, we may assume $r = 1$ and $s = \pm 1$ or $\pm 2$. First, suppose that $s = \pm 1$. Since

$$x^5 \equiv EE'^s \pmod{5\mathfrak{p}_3}$$

is solvable, so is

$$x^5 \equiv E'E'^s \equiv \pm E'^sE' \pmod{5\mathfrak{p}_3}.$$
CLASS NUMBER OF RELATIVE QUADRATIC FIELDS

\[ x^5 \equiv E^{1-s}E'^{1+s} \pmod{5p_5} \]

is solvable. Since \( s = \pm 1 \), this leads us back to (7). Finally, assume \( s = \pm 2 \) or equivalently \( s = 2 \) or \( s = 3 \). A computer analysis shows that \( EE'^3 \equiv \pm 1 \) or \( \equiv \pm 7 \pmod{5p_5} \) exactly when condition (2) is satisfied and that \( EE'^2 \equiv \pm 1 \) or \( \equiv \pm 7 \pmod{5p_5} \) exactly when conditions (3) or (4) are satisfied.

**Corollary 1.** If condition (1) of Theorem 4 is satisfied, then 25 divides the class number of \( K_2 \). Moreover, the 5-class group of \( K_2 \) is noncyclic.

**Proof.** From the proof of Theorem 4 it follows that the congruence \( x^5 \equiv E \pmod{5p_5} \) (where \( E \) is the relative fundamental unit of \( K_1 \)) has a solution if and only if condition (1) holds. But then \( x^5 \equiv E' \pmod{5p_5} \) also has a solution. It follows from Satz 119 of Hecke [3] that \( K(\sqrt[5]{E}) \) and \( K(\sqrt[5]{E'}) \) are unramified abelian extensions of \( K \). Since \( E \) and \( E' \) are independent, they must be distinct. There exist corresponding unramified abelian extensions \( M/K_2 \) and \( M'/K_2 \) of degree 5 with \( M \subset K(\sqrt[5]{E}) \) and \( M' \subset K(\sqrt[5]{E'}) \). Note that \( M = M' \) implies \( K(\sqrt[5]{E}) = K(\sqrt[5]{E'}) \). Thus, \( M_0 = MM' \) is an abelian unramified extension of \( K_2 \) of degree 25 with noncyclic Galois group. Thus, 25\( h(K_2) \) and the 5-class group of \( K_2 \) is noncyclic.

**Corollary 2.** Suppose 25 divides \( h(K_2) \) and the 5-class group of \( K_2 \) is noncyclic. Then either 5 divides \( h(K_1) \) or condition (1) of Theorem 4 is satisfied.

**Proof.** Using the method of proof of Theorem 1, there exist distinct unramified abelian extensions \( M/K_2 \) and \( M'/K_2 \) of degree 5 such that \( M(\sqrt[5]{a}) = K(\sqrt[5]{a}) \) and \( M'(\sqrt[5]{b}) = K(\sqrt[5]{b}) \) for some \( a, b \in K_1 \). If one of \( a \) or \( b \) is not a unit, then, as in the proof of Theorem 1, 5 divides \( h(K_1) \). If \( a = e_1 \) and \( b = e_2 \) are units, as in the proof of Theorem 4, we may suppose \( e_1 = EE'^r \) and \( e_2 = EE'^s \). Note that \( r \neq s \pmod{5} \) since otherwise \( M = M' \). Hence, \( K(\sqrt[5]{e_1/e_2}) = K(\sqrt[5]{E'^r}) \subset MM'(\xi) \), and so \( K(\sqrt[5]{E'})/K \) is an abelian unramified extension of \( K \) of degree 5. As seen in the proof of Theorem 4, this can happen if and only if (1) holds.

We now obtain a simpler criterion for conditions (1)-(4) of Theorem 4 to hold.

**Theorem 5.**

(i) If (1) holds, then (2) also holds.

(ii) If \( b \equiv 0 \pmod{5} \), then (2) holds.

(iii) If \( b \not\equiv 0, G \equiv \pm 1 \pmod{5} \) and \( a \equiv \pm 6 \) or \( \equiv \pm 8 \pmod{25} \), then (3) holds.

(iv) If \( b \not\equiv 0, G \equiv \pm 2 \pmod{5} \) and \( a \equiv \pm 3 \) or \( \equiv \pm 4 \pmod{25} \), then (4) holds.

**Proof.** If (1) holds, then \( \alpha \equiv \pm 1 \pmod{25} \) since \( E \) has relative norm \( \pm 1 \). Thus, (2) holds. If \( E = a + b\sqrt{5} + c\Omega + d\Omega' \pmod{5p_5} \), then

\[ E'' \equiv (a + b\sqrt{5}) - (c\Omega + d\Omega') \pmod{5p_5}, \]

where \( E'' \) is obtained from \( E \) by applying the automorphism of \( K_1 \) of order 2. Now

\[ \pm 1 = EE'' = (a + b\sqrt{5})^2 - (c\Omega + d\Omega')^2 \]

\[ \equiv a^2 + 5b^2 + 10(c^2 + d^2)G + 2(ab - (2c - d)^2G)\sqrt{5} \pmod{5p_5}. \]

Thus, we obtain

\[ ab \equiv (2c - d)^2G \pmod{5} \]
and
\[(9)\quad a^2 + 5b^2 + 10(c^2 + d^2)G \equiv \pm 1 \pmod{25}.
\]

If \(b \equiv 0 \pmod{5}\), then \(2c \equiv d \pmod{5}\) and
\[
\pm 1 \equiv a^2 + 10(c^2 + 4c^2)G \equiv a^2 \pmod{25}.
\]

Thus, \(a \equiv \pm 1, \pm 7 \pmod{25}\) and (2) holds. If \(c \equiv 0 \pmod{5}\), then (1) also holds.

The remaining parts of Theorem 5 follow from an easy, but lengthy, analysis of congruences. The proofs will be omitted.

5. Numerical Results. We employ methods developed by Hasse [1], [2] to compute the units and class number of \(K_1 = \mathbb{Q}(\sqrt{5}e_m)\) where \(e = (1 + \sqrt{5})/2\).

Using the notation of the previous section, Satz 24 of [1] shows that \(u^2 + v^2\) is minimal when \(E = \frac{1}{2}([s + t\sqrt{5})/2 + (u\Omega + v\Omega')]\) is a relative fundamental unit of \(K_1\). As the amount of time required to compute \(E\) increases with the magnitude of \(u^2 + v^2\), we only compute \(E\) when \(|u|, |v| \leq 50\). If \(t\) is not divisible by \(G\) then \(E, E'\) and \(e\) form a system of fundamental units for \(K_1\) (see p. 49 of [1]). In this case the regulator \(R\) of \(K_1\) is given by

\[
R = \begin{vmatrix}
\log |e| & -\log |e| & \log |e| \\
\log |E| & \log |E'| & -\log |E| \\
\log |E'| & -\log |E| & -\log |E'| \\
\end{vmatrix}
= \log |e| (\log^2 |E| + \log^2 |E'|)
= R_1 R_2,
\]

where \(R_1 = \log |e|\) is the regulator of \(\mathbb{Q}(\sqrt{5})\). If \(E, E'\) and \(e\) are not a fundamental set of units for \(K_1\), then Satz 16 of [1] shows that \(R\) is half of the above value. It follows from Hasse [2, p. 11], that \(h = h(K_1)\) is determined by

\[
h R_2 = \left| \sum_{x \pmod{F/2}} \chi(x) \log |1 - \xi_F^x| \right|^2,
\]

where \(F = 5G\) is the conductor of \(K_1\), the summation is over all integers \(x\) with \(0 \leq x \leq F/2\), \(\xi_F = e^{2\pi i/F}\) and \(\chi\) is a character of \(K_1\) of order 4. More precisely, \(\chi(x) = 0\) if \((x, F) \neq 1\) and \(\chi(x) = \chi_5(x)\chi_1(x)(x/m)\) if \((x, F) = 1\). Here \(\chi_5(x)\) is a character modulo 5 determined by \(\chi_5(2) = \sqrt{-1}\),

\[
\chi_1(x) = \begin{cases} 
(-1/x) & \text{if } m \equiv 1 \pmod{4}, \\
(2/x) & \text{if } m \equiv 2 \pmod{4}, \\
1 & \text{if } m \equiv 3 \pmod{4}
\end{cases}
\]

and \((x/m)\) is the Jacobi symbol for the modulus \(m\). Certainly,

\[
\chi(-1) = 1 \quad \text{and} \quad \sum_{x \pmod{F}} \chi(x) = 0.
\]
Units and Class Numbers

<table>
<thead>
<tr>
<th>G</th>
<th>m</th>
<th>s</th>
<th>t</th>
<th>u</th>
<th>v</th>
<th>N(E)</th>
<th>h(k₁)</th>
<th>h(k₂)</th>
<th>R₂</th>
<th>h(K₁)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>47</td>
<td>47</td>
<td>47</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>-1</td>
<td>5</td>
<td>2</td>
<td>39.4242184</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>79</td>
<td>79</td>
<td>79</td>
<td>95</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>84.9155464</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>83</td>
<td>83</td>
<td>913</td>
<td>401</td>
<td>38</td>
<td>23</td>
<td>-1</td>
<td>3</td>
<td>10</td>
<td>101.63678571</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>103</td>
<td>103</td>
<td>103</td>
<td>55</td>
<td>4</td>
<td>3</td>
<td>-1</td>
<td>5</td>
<td>6</td>
<td>55.38387765</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>119</td>
<td>119</td>
<td>203</td>
<td>85</td>
<td>7</td>
<td>4</td>
<td>-1</td>
<td>10</td>
<td>4</td>
<td>62.91774917</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>127</td>
<td>127</td>
<td>1397</td>
<td>475</td>
<td>45</td>
<td>20</td>
<td>-1</td>
<td>5</td>
<td>10</td>
<td>153.67144889</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>143</td>
<td>143</td>
<td>121</td>
<td>65</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>4</td>
<td>60.27872559</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>159</td>
<td>159</td>
<td>597</td>
<td>265</td>
<td>18</td>
<td>11</td>
<td>-1</td>
<td>10</td>
<td>4</td>
<td>83.45102140</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>179</td>
<td>179</td>
<td>179</td>
<td>155</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>16</td>
<td>101.29863674</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>232</td>
<td>58</td>
<td>116</td>
<td>32</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>20</td>
<td>60.4469988</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>303</td>
<td>303</td>
<td>303</td>
<td>145</td>
<td>7</td>
<td>4</td>
<td>-1</td>
<td>10</td>
<td>12</td>
<td>77.32653170</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>319</td>
<td>29</td>
<td>55</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>10</td>
<td>16</td>
<td>67.14327939</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>344</td>
<td>86</td>
<td>172</td>
<td>440</td>
<td>17</td>
<td>-1</td>
<td>-1</td>
<td>10</td>
<td>12</td>
<td>152.38387765</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>347</td>
<td>347</td>
<td>165</td>
<td>7</td>
<td>4</td>
<td>-1</td>
<td>5</td>
<td>26</td>
<td>79.55760924</td>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>488</td>
<td>122</td>
<td>2728</td>
<td>1220</td>
<td>47</td>
<td>29</td>
<td>-1</td>
<td>10</td>
<td>12</td>
<td>125.17811780</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>664</td>
<td>166</td>
<td>332</td>
<td>152</td>
<td>5</td>
<td>3</td>
<td>-1</td>
<td>10</td>
<td>20</td>
<td>71.76579538</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>724</td>
<td>181</td>
<td>2896</td>
<td>1180</td>
<td>38</td>
<td>26</td>
<td>1</td>
<td>10</td>
<td>24</td>
<td>172.82304130</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>836</td>
<td>209</td>
<td>304</td>
<td>220</td>
<td>6</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>20</td>
<td>112.94781541</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>872</td>
<td>218</td>
<td>872</td>
<td>380</td>
<td>11</td>
<td>7</td>
<td>-1</td>
<td>10</td>
<td>12</td>
<td>103.04348388</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>1604</td>
<td>401</td>
<td>1604</td>
<td>820</td>
<td>17</td>
<td>9</td>
<td>1</td>
<td>20</td>
<td>32</td>
<td>155.97863984</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>

Thus, $\sum_{x \pmod{F/2}} \chi(x) = 0$. Now

$$hR₂ = \left| \sum_{x \pmod{F/2}} \chi(x) \log |1 - \xi F x| \right|^2$$

$$= \frac{1}{2} \left| \sum_{x \pmod{F/2}} \chi(x) \log |1 - \xi F x| + \chi(-x) \log |1 - \xi F \bar{x}| \right|^2$$

$$= \frac{1}{2} \left| \sum_{x \pmod{F/2}} \chi(x) \log |2(1 - \cos 2\pi x/F)| \right|^2$$

$$= \frac{1}{2} \left| \sum_{x \pmod{F/2}} \chi(x) \log |4 \sin^2 \pi x/F| \right|^2$$

$$= \frac{1}{2} \log 4 \sum_{x \pmod{F/2}} \chi(x) + 2 \sum_{x \pmod{F/2}} \chi(x) \log |\sin \pi x/F| \right|^2$$

$$= \sum_{x \pmod{F/2}} \chi(x) \log |\sin \pi x/F| \right|^2.$$
Using this procedure, we have computed $E$, $R_2$ and $h(K_1)$ for some small values of $m$ where 5 divides $h(k_1)$ or $h(k_2)$. The results of our computations appear in the table above. In the table $E$ is determined by

$$E = \frac{1}{2} \left[ (s + t\sqrt{5})/2 + u\Omega + v\Omega' \right]$$

and $N(E)$ gives the relative norm of $E$. The “type” refers to the statement number of Theorem 4 which is satisfied by the particular field.

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

10. C. WALTER, "Kuroda’s class number relation,” Acta Arith. (To appear.)