ON THE UNIT GROUP OF SOME MULTIQUADRATIC NUMBER FIELDS

Elliott Benjamin, Franz Lemmermeyer and Chip Snyder
ON THE UNIT GROUP OF SOME MULTIQUADRATIC NUMBER FIELDS

ELLIO T BENJAMIN, FRANZ L EmmERM EYER AND CHI PNYDER

We study the index of the group of units in the genus field of an imaginary quadratic number field modulo the subgroup generated by the units of the quadratic subfields (over \( \mathbb{Q} \)) of the genus field.

1. Introduction

One major problem in algebraic number theory is the computation of the class number \( h(K) \) for a number field \( K \). In the case of quadratic fields, this problem is easily solved by elementary methods. Once the field degree is larger than 2, the problem becomes more challenging. Historically, the oldest case after the quadratic fields seems to be when \( K \) runs through a particular family of quartic bicyclic fields over \( \mathbb{Q} \), meaning that \( \text{Gal}(K/\mathbb{Q}) \cong (2, 2) \) (here \( (a_1, \ldots, a_r) \) denotes the direct sum of cyclic groups of order \( a_i \), for \( i = 1, \ldots, r \)). Dirichlet [1842] in essence computed the class number \( h(K) \) for the family of quartic fields \( K = \mathbb{Q}(\sqrt{-1}, \sqrt{m}) \), \( m \) a positive nonsquare integer. Namely, let \( k_1 = \mathbb{Q}(\sqrt{-1}) \), \( k_2 = \mathbb{Q}(\sqrt{m}) \), and \( k_3 = \mathbb{Q}(\sqrt{-m}) \), and denote by \( E_F \) the group of units of a number field \( F \). Then Dirichlet discovered the class number formula

\[
h(K) = \frac{1}{2} q(K/\mathbb{Q}) h(k_2) h(k_3),
\]

where \( q = q(K/\mathbb{Q}) = (E_K : E_{k_1} E_{k_2} E_{k_3}) \). Dirichlet went on to show that the unit index \( q \) could be determined and was equal to 1 or 2.

Over time, Dirichlet’s formula has been generalized in several directions; see in particular [Herglotz 1922; Kubota 1953; 1956; Kuroda 1950; Lemmermeyer 1994b; Wada 1966], and references therein. One particularly striking formula is usually attributed to Kuroda [1950], but in fact goes back to Herglotz [1922] in an equivalent, if less convenient, form for \( q \). Let \( L = \prod_i k_i \) be the multiquadratic field generated as the composite of all its quadratic subfields \( k_i \), and suppose further that \( [L : \mathbb{Q}] = 2^m \). Then

\[
h(L) = \frac{1}{2^v} q(L/\mathbb{Q}) \prod_i h(k_i),
\]

\[\text{MSC2000: primary 11R11; secondary 11R27, 11R29.}\]

\[\text{Keywords: unit index, Kuroda’s class number formula, multiquadratic fields.}\]
where \( q = q(L/\mathbb{Q}) = (E_L : \prod_i E_{k_i}) \) and

\[
v = \begin{cases} 
  m(2^{m-1} - 1) & \text{if } L \text{ is real,} \\
  (m-1)(2^{m-2} - 1) + 2^{m-1} - 1 & \text{if } L \text{ is complex.}
\end{cases}
\]

Hence \( h(L) \) can be computed easily provided that the unit index \( q(L/\mathbb{Q}) \) can be computed. Herein lies the obstruction to an easy determination of the class number of multiquadratic number fields. For quartic bicyclic fields, Kubota [1956] gave a method for finding a system of fundamental units and thus for computing \( q \). Wada [1966], generalized Kubota’s method, creating an algorithm for computing fundamental units in any given multiquadratic field. However, in general there seems to be no explicit formula for \( q \), even when \( L \) is of degree 4 over \( \mathbb{Q} \).

This brings us to the purpose of this article. We try to glean some understanding of the difficulties in computing the unit index by giving explicit computations of \( q \) for special families of multiquadratic fields \( L \). We consider the special case of the genus field \( L = k_{\text{gen}} \) of a complex quadratic field \( k \) for which the 2-rank of the class group \( \text{Cl}(k) \) of \( k \) is \( \leq 3 \). (Recall that the 2\textsuperscript{-}rank of a finite abelian group \( G \) is the minimal number of generators of the factor group \( G^{2^\infty}/G^{2^\infty} \).) If the 2-rank of \( \text{Cl}(k) \) is 1, then \([L : \mathbb{Q}] = 4\), by genus theory, and in this case it is known that \( q = 1 \) (see [Lemmermeyer 1995], for instance; the proof is easy — see the next section).

Next, if the 2-rank is 2, then \([L : \mathbb{Q}] = 8\) by genus theory. In this case, we reduce the problem to that of computing \( q(K/\mathbb{Q}) \) where \( K \) is the maximal real subfield of \( L \). But then \( K \) is a totally real bicyclic field and we may apply the results of [Kubota 1956] to compute \( q(K/\mathbb{Q}) \). We find that \( q(L/\mathbb{Q}) = 8 \) or 2 according as the 2-class field tower of \( k \) is of length 1 or > 1. (Here \( k^1 \) is the Hilbert 2-class field of \( k \) and \( k^{n+1} = (k^n)^1 \); the length of the 2-class field tower of \( k \) is the cardinality of the set of \( k^n \).)

For the case where the 2-rank of \( \text{Cl}(k) \) is 3, we seem to be in new territory. We restrict to the case of elementary 2-class group. Specifically, we assume \( \text{Cl}_2(k) \simeq (2, 2, 2) \), so \( L = k_{\text{gen}} = k^1 \). If the rank of \( \text{Cl}_2(k^1) \) is 2 as a module over the integral group ring \( \Lambda = \mathbb{Z}[\text{Gal}(k^1/k)] \), then \( q(L/\mathbb{Q}) = 2^7 \). This condition on the \( \Lambda \text{-rank} \) is, by the way, a natural one; see [Benjamin et al. 2003]. We then obtain less complete information about \( q \) for the other case where \( \text{Cl}_2(k^1) \) is of \( \Lambda \text{-rank} \) 3. In the particular fields we consider, \( q = 2^4 \) or \( 2^5 \).

2. The Main Results

Let \( k \) be an imaginary quadratic field for which the 2-rank of \( \text{Cl}(k) \) is \( t - 1 \). Hence, by genus theory, \( k = \mathbb{Q} (\sqrt{d_1} \cdots \sqrt{d_t}) \), where \( \text{disc} \ k = d_1 \cdots d_t \) is a factorization of the discriminant of \( k \) into distinct prime discriminants \( d_i \) divisible by the rational prime \( p_i \) for \( i = 1, \ldots, t \). Then \( L = k_{\text{gen}} = \mathbb{Q} (\sqrt{d_1}, \ldots, \sqrt{d_t}) \) and hence multiquadratic
Let \( k \) be a complex quadratic number field and \( L \) the maximal real subfield of \( k \), \( d = \sqrt{\text{disc} k} \), \( t \) is odd for any prime discriminant \( d \). Moreover, since \( k \) is complex, \( \text{disc} k \) is contained in \( \mathbb{Q} \), and \( h(d) \) is odd for any prime discriminant \( d \). Thus, by the Artin map, \( \text{Gal}(k^1/k) \simeq \text{Cl}_2(k) \) where \( \text{Cl}_2(k) \) is the 2-class group of \( k \), the Sylow 2-subgroup of the class group, the order of which is \( h_2(k) \), the 2-class number of \( k \). Now consider \( G = \text{Gal}(k^2/k) \). Since the commutator subgroup \( G' = \text{Gal}(k^2/k^1) \), we see \( G/G' \simeq \text{Gal}(k^1/k) \simeq \text{Cl}_2(k) \). But in the present case, \( \text{Cl}_2(k) \) is cyclic, whence \( G' = \langle 1 \rangle \), and thus \( k^2 = k^1 \). But then since \( k^1 \subseteq L^1 \subseteq k^2 \), we have \( L^1 = k^1 \). Therefore, \( h_2(L) = [L^1 : L] = [k^1 : k]/2 = h_2(k)/2 \). Now by restricting to 2-class numbers and using the fact that \( q \) is a power of two, (see [Wada 1966], for instance) the Kuroda class number formula becomes

\[
h_2(L) = \frac{1}{2} q(L/\mathbb{Q}) h_2(k) h_2(d_1) h_2(d_2).
\]

From the preceding discussion we get \( \frac{1}{2} h_2(k) = \frac{1}{2} q h_2(k) \), as needed. \( \square \)

Next, we consider the case where the 2-rank of \( \text{Cl}(k) \) is 2, i.e. \( t = 3 \). Hence \( k = \mathbb{Q}(\sqrt{d_1d_2d_3}) \), with prime discriminants \( d_i \). Moreover, since \( k \) is complex, \( \text{disc} k < 0 \) so either all the \( d_i \) are negative or exactly two are positive, say \( d_1, d_2 > 0, d_3 < 0 \). Notice that we have \( L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}) \). Let \( K = L^+ \) be the maximal real subfield of \( L \), (so \( K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \) if \( d_1, d_2 > 0, d_3 < 0 \), and \( K = \mathbb{Q}(\sqrt{d_1d_2}, \sqrt{d_2d_3}) \) if \( d_i < 0 \), for \( i = 1, 2, 3 \)). But then it follows that \( q(L/\mathbb{Q}) = Q(L/K)q(K/\mathbb{Q}) \), where \( Q(L/K) = \langle E_L : W_L E_K \rangle \) with \( W_L \) the group of roots of unity of \( L \). To see this apply for example [Benjamin et al. 2003, Proposition 1], where we notice that any primitive eighth root \( \zeta_8 \) of unity is not contained in \( L \) since any ramification index of a prime in \( L/\mathbb{Q} \) must divide 2, whereas 2 is totally ramified in \( \mathbb{Q}(\zeta_8) \). Now suppose \( d_1, d_2 > 0, d_3 < 0 \). By [Lemmermeyer
Let $k$ be a complex quadratic field with field degrees in the above formula equal 1, and therefore the 2-class field tower of $k$ again for the details. Thus we have $q(L/Q) = q(K/Q)$. If however all the $d_i < 0$, then for any $i$, $L = K(\sqrt{d_i})$. In this case, it can be shown that $Q(L/K) = 2$ by [Lemmermeyer 1995], but we shall see that this is the case by another method. In either case, it is well known that $Q(L/K) = 1, 2$ (see [Hasse 1985, Satz 14]), and moreover, by Kubota [Kubota 1956], $q(K/Q)$ divides 4. Thus $q(L/Q)$ must divide 8.

**Theorem 2.** Let $k$ be a complex quadratic field with 2-rank $\text{Cl}(k) = 2$. Then for $L = k_{\text{gen}}$, $q(L/Q) = 8$ or 2 according as the 2-class field tower of $k$ is of length 1 or $> 1$.

**Proof.** By assumption, $k = Q(\sqrt{d_1d_2d_3})$ for prime discriminants $d_i$. Now notice that $K_i = k(\sqrt{d_i})$ for $i = 1, 2, 3$ are the three unramified quadratic extensions of $k$ in $L$. These fields are quartic bicyclic extensions of $Q$ and so Kuroda’s class number yields

$$h(K_1) = \frac{1}{2} q(K_1/Q)h(k)h(d_2d_3)h(d_1),$$

since $m = 2$, so $\nu = 1$, (analogously for $K_2$ and $K_3$). Now since the $K_i$ are unramified quadratic extensions of a complex quadratic field $k$, it is known that $q(K_i/Q) = 1$; see for example [Lemmermeyer 1995]. Hence by considering 2-class numbers so that we may use $h_2(d_i) = 1$, we have

$$h_2(L) = \frac{1}{32} q(L/Q)h_2(k)h_2(d_1d_2)h_2(d_1d_3)h_2(d_2d_3), \quad h_2(K_1) = \frac{1}{2} h_2(k)h_2(d_2d_3).$$

Now we rewrite the formula for $h_2(L)$ in terms of $h_2(K_i)$. From above, notice that for example $h_2(d_2d_3) = 2h_2(K_1)/h_2(k)$, etc. and so by class field theory,

$$h_2(d_2d_3) = \frac{2[K^1 : K]}{[k^1 : k]} = \frac{2[K_1^1 : k^1][K^1_1 : K_1]}{[k^1 : K_1][K_1^1 : k]} = [K_1^1 : k^1].$$

Substituting into the above formula yields

$$[L^1 : L] = \frac{1}{32} q(L/Q)[k^1 : k][K_1^1 : k^1][K_2^1 : k^1][K_3^1 : k^1]$$

and since $[L : k] = 4$, we have

$$[L^1 : k^1] = \frac{1}{8} q(L/Q)[K_1^1 : k^1][K_2^1 : k^1][K_3^1 : k^1].$$

Notice, in particular, that if the 2-class field tower of $k$ is of length 1, then all the field degrees in the above formula equal 1, and therefore $q = 8$. Now, the length of the 2-class field tower of $k$ is 1 precisely when $d_i < 0$ for $i = 1, 2, 3$; see for example [Benjamin et al. 1997]. From this we have $8 = q(L/Q) = Q(L/K)q(K/Q)$ from which it follows (by the comments before the proposition) that $Q(L/K) = 2$ and $q(K/Q) = 4$. 
Now suppose that $d_1, d_2 > 0, d_3 < 0$. In this case we have $q(L/Q) = q(K/Q)$, where $K = Q(\sqrt{d_1}, \sqrt{d_2})$. Kuroda’s class number formula implies

$$h_2(K) = \frac{1}{4}q(K/Q)h_2(F),$$

where $F = Q(\sqrt{d_1d_2})$. Then notice that $\text{Cl}_2(F)$ is cyclic and thus $F^1 = F^2$. Thus since $K/F$ is unramified so $K \subseteq F^1$, $h_2(K) = h_2(F)/2$. Plugging this into the formula above yields $q(K/Q) = 2$. Thus $q(L/Q) = 2$. □

**Proposition 3.** Let $k$ be a complex quadratic field with 2-rank $\text{Cl}(k) \leq 2$ and with 4-rank $\text{Cl}(k) \leq 1$. Then

$$\prod_i K_i^1 = \left( \prod_i K_i \right)^1,$$

where $K_i$ range over all the unramified quadratic extensions of $k$.

**Proof.** If $k^1 = k^2$, then the proposition is trivially true, since both fields are $k^1$. Thus, assume $k^1 \neq k^2$. Hence we know $k = Q(\sqrt{d_1d_2d_3})$ where $d_1, d_2 > 0, d_3 < 0$. From the proof of Theorem 2,

$$[L^1:k^1] = \frac{1}{4}[K_1^1 : k^1][K_2^1 : k^1][K_3^1 : k^1],$$

where $L = K_1K_2K_3$ with $K_i = k(\sqrt{d_i})$. But notice that

$$[K_1^1K_2^1K_3^1 : k^1] = \frac{[K_1^1 : k^1]}{[K_1^1 \cap K_2^1K_3^1 : k^1]} \frac{[K_2^1 : k^1]}{[K_2^1 \cap K_3^1 : k^1]} \frac{[K_3^1 : k^1]}{[K_3^1 \cap K_1^1 : k^1]}.$$ (Also notice this equation is true for any permutation of the indices.) Now since

$$[L^1:k^1] = [L^1 : K_1^1K_2^1K_3^1][K_1^1K_2^1K_3^1 : k^1],$$

we see by putting these equations together that

$$[L^1 : K_1^1K_2^1K_3^1] = \frac{1}{4}[K_1^1 \cap K_2^1K_3^1 : k^1][K_2^1 \cap K_3^1 : k^1][K_3^1 \cap K_1^1 : k^1].$$

To finish the proof, it suffices to show that

$$[K_1^1 \cap K_2^1K_3^1 : k^1] = [K_2^1 \cap K_3^1 : k^1] = 2.$$

Here is where some group theory comes in. Let $G = \text{Gal}(k^2/k)$, and further let $H_1, H_2, H_3$ be the three maximal subgroups of $G$ such that $\text{Gal}(k^2/K_i) = H_i$. Then we need to show that

$$(G' : H_2'H_3') = (G' : H_1'(H_2' \cap H_3')) = 2.$$ (Here is a sketch of the proof. If $G'$ is cyclic, say $G' = \langle c \rangle$, by the table of possible groups and their presentations at the end of [Benjamin et al. 1997], we have (without loss of generality) $H_3' = \langle c^3 \rangle$ and $H_1'H_2' = \langle c^2 \rangle$, from which our result follows.
Now suppose $G'$ is not cyclic. Then by our assumption on the class group of $k$, $G$ must be nonmetacyclic with $G/G' \simeq (2, 2^n)$ for some $n > 1$. Now we assume the notation before [Benjamin et al. 2001, Lemma 1]. Hence let $G = \langle a, b \rangle$ where $a^2 \equiv b^{2^n} \equiv 1 \mod G'$. Let $[a, b] = c$ and define inductively, $c_2 = c$ and $c_{j+1} = [b, c_j]$. We have $G' = \langle c_2, c_3, \ldots \rangle$, and $G_3 = \langle c_2^2, c_3, \ldots \rangle$, and $G_4 = \langle c_2^4, c_3^2, c_4, \ldots \rangle$; see [Benjamin et al. 1997, Lemma 2]. Now if $H_3 = \langle a, b^2, G' \rangle$, then it is easy to see that $H_1^2 G_4 = G_3$. Thus $H_2^2 = G_3$ by [Hall 1933, Theorem 2.49ii]. Hence $(G' : H_1^2) = (G' : G_3) = 2$. Similarly, if $H_1 = \langle b, G' \rangle$ and $H_2 = \langle ab, G' \rangle$, then $H_1^2 H_2 G_4 = G_3$ so once again $H_1^2 H_2^2 = G_3$. This shows the result and finishes the proof of the proposition.

Now we consider $\text{Cl}_2(k) \simeq (2, 2, 2)$, and thus in particular $k = d_1 d_2 d_3 d_4$ for distinct prime discriminants $d_i$. If we assume the $\Lambda$-rank of $\text{Cl}_2(k^1/k)$ is 2, then by [Benjamin et al. 2003, Theorem 2], exactly three of the $d_i$'s must be negative, say $d_1, d_2, d_3 < 0, d_4 > 0$.

**Theorem 4.** Let $k$ be a complex quadratic field with $\text{Cl}_2(k) \simeq (2, 2, 2)$. If the $\Lambda$-rank of $\text{Cl}_2(k^1)$ equals 2, the unit index $q(k^1/Q)$ equals $2^7$.

**Proof.** If $\text{Cl}_2(k) \simeq (2, 2, 2)$, then $\text{Cl}_2(k^1/k)$ has $\Lambda$-rank 2 if and only if $G/G' \simeq (2, 2, 2)$ and $G'/G_3 \simeq (2, 2)$, where $G = \text{Gal}(k^2/k)$. Thus $(G : G_3) = 32$ and $G'/G_3 \simeq (2, 2)$, and by [Hall and Senior 1964], $G/G_3$ must be one of the seven groups $32.033, 32.035, 32.036, 32.037, 32.038, 32.040, 32.041$, in the notation of that same reference.

Let $L = k^1 = k_{\text{gen}}$. Kuroda’s class number formula (with $t = 4$, so $v = 16$) gives

$$h_2(L) = \frac{1}{2^{16}} q(L/Q) h_2(k) \prod_i h_2(k_i),$$

where the $k_i$ are the quadratic subfields of $L$ excluding $k$.

The following table lists the 2-class numbers $h_2(k_i)$ and $h_2(L)$:

<table>
<thead>
<tr>
<th>$G/G_3$</th>
<th>$h_2(k_i)$</th>
<th>$h_2(L)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.041, 32.040</td>
<td>1 (7), 2 (6), 4</td>
<td>4</td>
</tr>
<tr>
<td>32.035, 32.037, 32.038</td>
<td>1 (7), 2 (5), 4, $2^n$</td>
<td>$2^{n+1}$</td>
</tr>
<tr>
<td>32.036</td>
<td>1 (7), 2 (5), $2^{m+1}$, $2^n$</td>
<td>$2^{m+n}$</td>
</tr>
<tr>
<td>32.033</td>
<td>1 (7), 2 (3), 4, $2^l$, $2^m$, $2^n$</td>
<td>$2^{l+m+n-1}$</td>
</tr>
</tbody>
</table>

Here “1 (7)” means that 7 quadratic subfields have 2-class number equal to 1. Plugging these data into (1) we immediately find the values of the unit index $q(L/Q)$ in each of the cases.

The 2-class numbers of the quadratic subfields $k_i$ of $L$ are easily determined using genus theory (see [Kaplan 1976], for instance). The 2-class numbers of $L$
were computed in [Benjamin et al. 2003], except for the group $G/G_3 = 32.033$
(for the first five groups, we have given the structure of $G'$ explicitly; in the case $G/G_3 = 32.036$, we computed the 2-class number and actually showed that $q(L/\mathbb{Q}) = 2^7$).

We will now study the case $G/G_3 \simeq 32.033$ in detail. By Proposition 16 in the same reference, we have $k = \mathbb{Q}(\sqrt{d_1d_2d_3d_4})$ with $d_i < 0$, $(i = 1, 2, 3)$, $d_4 > 0$ and such that

$$
\begin{align*}
\left( \frac{d_1}{p_2} \right) &= \left( \frac{d_2}{p_3} \right) = \left( \frac{d_3}{p_1} \right) = \left( \frac{d_4}{p_4} \right) = -1, \quad \left( \frac{d_4}{p_3} \right) = +1.
\end{align*}
$$

Here is a list of the 2-class numbers of the quadratic subfields of $L = k^1$. Along with $h_2(k) = 8$, we have

$$
\begin{align*}
h_2(d_j) &= h_2(d_1d_2) = h_2(d_2d_3) = h_2(d_1d_3) = 1, \quad (j = 1, 2, 3, 4) \\
h_2(d_1d_4) &= h_2(d_1d_2d_4) = h_2(d_1d_3d_4) = 2, \quad h_2(d_2d_3d_4) = 4, \\
h_2(d_3d_4) &= 2l, \quad h_2(d_2d_3d_4) = 2m, \quad h_2(d_2d_4) = 2^l (l, m, n \geq 2).
\end{align*}
$$

Let $K = L^+ = \mathbb{Q}(\sqrt{d_1d_2}, \sqrt{d_1d_3}, \sqrt{d_4})$, the maximal real subfield of $L$. Then $q(L/\mathbb{Q}) = Q(L/K)q(K/\mathbb{Q})$ by [Benjamin et al. 2003, Proposition 1]. But by [Lemmermeyer 1995], $Q(L/K) = 2$. In fact, if $w_L(= \# W_L) \equiv 2$ mod 4, then $L = K(\sqrt{d_1})$ and $(p_1) = (\pi)^2$ in $Q(\sqrt{d_1d_2})$ since $p_1$ ramifies and the field has odd class number. But then $d_1 \mathcal{O}_K = (\pi \mathcal{O}_K)^2$, and part (i)2(a) of [Lemmermeyer 1995, Theorem 1] implies $Q(L/K) = 2$. If instead $w_L \equiv 4$ mod 8, then $2 \mathcal{O}_K = (1+i)^2 \mathcal{O}_K$, whence part (ii)2(a) of the same theorem shows again that $Q(L/K) = 2$.

Now we compute $q(K/\mathbb{Q})$. To this end, consider the quadratic number field $k_0 = \mathbb{Q}(\sqrt{d_2d_3d_4})$ with 2-class group $Cl_2(k_0) = (2^m)$ and fundamental unit $\varepsilon_{234}$. Then $K/k_0$ is a $V_4$-extension with the quadratic subextensions $K_1 = k_0(\sqrt{d_1d_2})$, $K_2 = k_0(\sqrt{d_1d_3})$, $K_3 = k_0(\sqrt{d_2d_3})$. Let $\varepsilon_{ij}$ denote the fundamental unit of $Q(\sqrt{d_id_j})$ for $1 \leq i < j \leq 3$. We shall determine $Cl_2(K_1)$ and $q(K_1/\mathbb{Q})$. Since $k_0$ has cyclic 2-class group of type $(2^m)$ and since $K_1/k_0$ is ramified, its class group contains $(2^m)$ as a subgroup. If we can show that $h_2(K_1) = 2^m$, then $Cl_2(K_1) \simeq (2^m)$; since $K/K_1$ is unramified, it would then follow that $Cl_2(K) \simeq (2^m)$. Applying Kuroda’s class number formula to $K/\mathbb{Q}$ would then give $q(K/\mathbb{Q}) = 2^6$, and this in turn implies $q(L/\mathbb{Q}) = 2^7$ and $h_2(L) = 2^{l+m+n-1}$.

For computing the 2-class number of $K_1$ we use Kuroda’s formula

$$h_2(K_1) = \frac{1}{2}q(K_1/\mathbb{Q})h_2(d_1d_2)d_2(d_1d_2d_4)h_2(d_2d_3d_4) = q(K_1/\mathbb{Q})2^{m-1}.$$

It suffices to show that $q(K_1/\mathbb{Q}) \leq 2$ (which implies $q(K_1/\mathbb{Q}) = 2$ by the argument above).

We consider two cases: $d_k := \text{disc } k \not\equiv 4$ mod 8 and $d_k \equiv 4$ mod 8. Assume $d_k \not\equiv 4$ mod 8. The prime ideal above $d_1$ in $\mathbb{Q}(\sqrt{d_1d_2})$ is principal; hence $X^2 - d_1d_2y^2 =$
\[ \pm 4d_1 \text{ is solvable, and so is } d_1 x^2 - d_2 y^2 = -4 \text{ (the minus sign must occur since } (d_1/p_2) = -1). \] Then \( \eta = \frac{1}{2}(x + y \sqrt{d_2}) \) is a unit in \( F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \); note that \( \eta^2 < 0 \) in \( \mathbb{Q}(\sqrt{d_1d_2}) \) since otherwise \( \eta \in \mathbb{R} \) and \( F = \mathbb{Q}(\sqrt{d_1d_2}) \). Therefore \( \eta^2 = -\varepsilon_1^2 \); notice that \( u \) is odd since otherwise \( \sqrt{-1} \in \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \), a contradiction. Thus \(-d_1\varepsilon_{12} = (\sqrt{d_1}\varepsilon_{12}^{(1-u)/2})^2 \) is a square in \( \mathbb{Q}(\sqrt{d_1d_2}) \).

Next consider \( \mathbb{Q}(\sqrt{d_1d_2d_4}) \), along with the diophantine equations

\[
\begin{align*}
d_1 x^2 - d_3 d_4 y^2 &= \pm 4, \\
d_3 x^2 - d_1 d_4 y^2 &= \pm 4, \\
d_4 x^2 - d_1 d_3 y^2 &= \pm 4,
\end{align*}
\]

which are solvable if the prime above \( d_1, d_3, d_4 \), respectively, is principal. The first implies \( (d_1/p_3) = +1 \), which contradicts the assumptions. The last implies \( (d_4/p_1) = (d_4/p_3) \), which also leads to a contradiction. Thus the second equation must have a solution, and reduction mod \( p_3 \) shows that we must have \( d_3 x^2 - d_1 d_4 y^2 = -4 \). Thus \(-d_3\varepsilon_{134} \) is a square in \( \mathbb{Q}(\sqrt{d_1d_2d_4}) \). Hence none of \( \varepsilon_{12}, \varepsilon_{134}, \varepsilon_{12}\varepsilon_{134} \) can be squares in \( K_1 \). Therefore \( q(K_1/\mathbb{Q}) \leq 2 \), as desired.

Now suppose \( d_k \equiv 4 \mod 8 \). Then our assumptions imply that \( d_3 = -4 \) or \( d_2 = -4 \). First assume that \( d_3 = -4 \). Then the argument above shows that \( \varepsilon_{12} = p_1\kappa^2 \) for some \( \kappa \in \mathbb{Q}(\sqrt{d_1d_2}) \). Now consider \( \mathbb{Q}(\sqrt{d_1d_2d_4}) = \mathbb{Q}(\sqrt{p_1p_4}) \). Then by genus theory ([Lemmermeyer 2000, page 76]) there is a principal ideal (\( \alpha \)) in \( \mathbb{Q}(\sqrt{p_1p_4}) \) different from (1) and \( (\sqrt{p_1p_4}) \) which is a product of distinct ramified prime ideals. We now consider the possibilities. First notice that the prime ideals above \( p_1 \) and \( p_4 \) are not principal, since otherwise \( p_1 x^2 - p_4 y^2 = \pm 1 \) is solvable which cannot happen. Now assume that the prime ideal above 2 is principal, equal to say \( (\pi) \) with \( \pi = x + y\sqrt{p_1p_4} \), for some \( x, y \in \mathbb{N} \). Then \( \pi^2/2 = \mu \) a positive unit in \( \mathbb{Q}(\sqrt{p_1p_4}) \). Clearly \( \mu \) is not a square in \( \mathbb{Q}(\sqrt{p_1p_4}) \) since otherwise \( \sqrt{2} \in \mathbb{Q}(\sqrt{p_1p_4}) \), a contradiction. Hence \( \varepsilon_{134} = 2\kappa^2 \), for some \( \kappa \in \mathbb{Q}(\sqrt{p_1p_4}) \). Similarly \( \varepsilon_{134} \) could be of the form \( 2p_1\kappa^2 \) or \( 2p_4\kappa^2 \). But in all of these cases we see that none of \( \varepsilon_{12}, \varepsilon_{134}, \varepsilon_{12}\varepsilon_{134} \) can be squares in \( K_1 \). Once again we have \( q(K_1/\mathbb{Q}) \leq 2 \).\]
Finally, suppose \( d_2 = -4 \). The argument above shows \( \epsilon_{134} = p_3 \kappa^2 \), for some \( \kappa \in \mathbb{Q}(\sqrt{d_1d_3d_4}) \). Now consider \( \mathbb{Q}(\sqrt{d_1d_2}) = \mathbb{Q}(\sqrt{d_1^2}) \). Then arguing as above we see \( \epsilon_{12} = 2\kappa^2 \) or \( \epsilon_{12} = 2p_1 \kappa^2 \) for some \( \kappa \in \mathbb{Q}(\sqrt{d_1}) \). But again this implies \( q(K_1/\mathbb{Q}) \leq 2 \); whence the result is established. \( \square \)

Now we come to the case where \( \text{Cl}_2(k) \simeq (2, 2, 2) \) but with \( \text{disc} \ k \) divisible by three positive prime discriminants, say \( \text{disc} \ k = d_1d_2d_3d_4 \) with \( d_i > 0 \) for \( i = 1, 2, 3 \) and \( d_4 < 0 \). Our results in this case will be far less complete since our knowledge of \( \text{Gal}(k^2/k) \) is much more spotty. But we now simplify things somewhat by reducing to the maximal real subfield of \( k^1 \). To this end, from now on, let \( L = k^1 \) and \( K = L^+ \) the maximal real subfield of \( L \). But then

\[
q(L/\mathbb{Q}) = q(K/\mathbb{Q}),
\]

because \( q(L/\mathbb{Q}) = Q(L/K)q(K/\mathbb{Q}) \) (by [Benjamin et al. 2003, Proposition 1], for example). By [Lemmermeyer 1995, Theorem 1] we get \( Q(L/K) = 1 \) since \( L = K(\sqrt{d_4}) \) is essentially ramified if \( d_4 \neq -4 \) and \( 2 \mathcal{O}_K \) is not an ideal square when \( d_4 = -4 \).

Now we need only consider \( K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) \) where \( p_i \) are the rational primes dividing \( d_i \). We set up the following notation. Let \( k_0 = \mathbb{Q}(\sqrt{p_1 p_2 p_3}) \). Let \( K_i = k_0(\sqrt{p_i}) \) for \( i = 1, 2, 3 \) and let \( k_i \) be the quadratic subfield of \( K_i \) not equal to \( k_0 \) and \( \mathbb{Q}(\sqrt{p_i}) \). (Notice that \( k_i = \mathbb{Q}(\sqrt{\text{disc} k_0/p_i}) \).) We now let \( \epsilon_i \) for \( i = 0, 1, 2, 3 \) be the fundamental unit \( > 1 \) in \( k_i \) and \( N \epsilon_i \) the norm from \( k_i \) to \( \mathbb{Q} \); also let \( \epsilon_{p_i} \) be the fundamental unit in \( \mathbb{Q}(\sqrt{p_i}) \). Finally let \( H_i = \text{Gal}(k_0^2/K_i) \).

Now we assume that \( k_0 \) is a particular type of field. Namely, assume that \( \text{Cl}_2(k_0) \simeq (2, 2) \). This assumption implies that \( G = \text{Gal}(k_0^2/k_0) \) is one of the following types: abelian, quaternion, dihedral, semidihedral. Moreover notice that in this case \( k_0^1 = K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) \) since \( K/k_0 \) is unramified and \( h_2(k_0) = 4 \). Without loss of generality we now pick \( K_1 \) above so that \( H_1 \) is cyclic. We are in a position to state and prove the following (rather technical) theorem.

**Theorem 5.** Let \( k \) be a complex quadratic field with \( \text{Cl}_2(k) \simeq (2, 2, 2) \) and with \( \text{disc} \ k = d_1d_2d_3d_4 \) where \( d_i \) are distinct prime discriminants divisible by primes \( p_i \) and \( d_1, d_2, d_3 \) are positive. With the notation above, assume that \( \text{Cl}_2(k_0) \simeq (2, 2) \). Then \( q = q(k^1/\mathbb{Q}) \) takes on the two values \( 2^4 \) and \( 2^5 \) as follows:

- If \( G \) is abelian, then \( q = 2^4 \).
- If \( G \) is nonabelian, then \( N \epsilon_0 = +1 \) implies \( q = \left\{ \begin{array}{ll} 2^4 \text{ if } N \epsilon_1 = -1; \\
2^5 \text{ otherwise,} \end{array} \right. \)

\[
N \epsilon_0 = -1 \text{ implies } q = \left\{ \begin{array}{ll} 2^4 \text{ if } \left( N \epsilon_1 = 1 \text{ or } (N \epsilon_1 = -1 \text{ and } \sqrt{p_1 \epsilon_0 \epsilon_1} \not\in K_1) \right) \\
2^5 \text{ otherwise.} \end{array} \right.
\]

With the notation above, let

\[
\left( \frac{p_1}{p_2} \right) = \left( \frac{p_1}{p_3} \right) = -\left( \frac{p_2}{p_3} \right) = -1,
\]

then

\[
N \epsilon_0 = -1 \text{ implies } q = \left\{ \begin{array}{ll} 2^4 \text{ if } \left( N \epsilon_1 = 1 \text{ or } (N \epsilon_1 = -1 \text{ and } \sqrt{p_1 \epsilon_0 \epsilon_1} \not\in K_1) \right) \\
2^5 \text{ otherwise.} \end{array} \right.
\]
Proof. Since \( H_1 \) is cyclic (and so in particular abelian), we have \( k_0^2 = K_1^1 \). Thus \( h_2(K_1) = [k_0^2 : k_0^1][k_1^1 : K_1] = 2h_2(k_0^1) \), and hence

\[
(*) \quad h_2(k_0^1) = \frac{1}{2} h_2(K_1).
\]

Next notice by Kuroda’s class number formula that

\[
(**) \quad h_2(k_0^1) = \frac{1}{2^7} q h_2(k_1)h_2(k_2)h_2(k_3),
\]

where we have used \( \nu = 9 \) and \( h_2(k_0) = 4 \). Now Kuroda’s class number formula for \( K_i \) yields

\[
(***) \quad h_2(K_i) = \frac{1}{4} q_i h_2(p_i)h_2(k_i)h_2(k_0) = q_i h_2(k_i).
\]

But then \((*)\), \((**)*\), \((**\ast)*\) imply

\[
\frac{1}{2} q_1 h_2(k_1) = \frac{1}{2^7} q h_2(k_1) \frac{h_2(K_2)}{q_2} \frac{h_2(K_3)}{q_3},
\]

and therefore

\[
q = \frac{2^6 q_1 q_2 q_3}{h_2(K_2) h_2(K_3)}.
\]

Suppose first of all that \( G \) is abelian. Then \( k_0^2 = k_0^1 \) and so \( h_2(K_i) = 2 \). Thus \( q = 2^4 q_1 q_2 q_3 \). But \( h_2(k_i) \equiv 0 \mod 2 \), since the \( d_j \) is odd for \( j = 1, 2, 3 \). So \((**\ast)\) implies that \( h_2(K_i) = 2 = q_i h_2(k_i) \) and this in turn yields \( h_2(k_i) = 2 \) and \( q_i = 1 \), for \( i = 1, 2, 3 \). Thus when \( G \) is abelian, \( q = 2^4 \).

Now assume that \( G \) is not abelian. Then for \( G \simeq H_8 \), the quaternion group of order 8, or \( G \simeq D_4 \), the dihedral group of order 8, \( H_1 \) has order 4 for \( i = 1, 2, 3 \) and so in particular \( h_2(K_i) = 4 \). If \( G \not\simeq H_8 \) or \( D_4 \), then \( H_2, H_3 \) are either dihedral, semidihedral, or quaternion, whence in particular the abelianizations \( H_2^{ab} \simeq H_3^{ab} \simeq (2, 2) \) and thus \( h_2(K_2) = h_2(K_3) = 4 \). Then

\[
q = 2^2 q_1 q_2 q_3.
\]

Case 1. Assume \( N \epsilon_0 = 1 \). We now compute the \( q_i \)’s. First consider \( q_2 \). By [Couture and Derham 1992, Theorem 1], \( (p_1/p_3) = -1 \), whence \( h_2(k_2)(= h_2(p_1 p_3)) = 2 \). But \( 4 = h_2(K_2) = q_2 h_2(k_2) = 2q_2 \), so thus

\[
q_2 = 2.
\]

Next consider \( q_3 \). Again by [Couture and Derham 1992, Theorem 1], \( (p_2/p_1) = 1 \) and \( (p_1/p_2)_4 = -(p_2/p_1)_4 \). Since \( 4 = h_2(K_3) = q_3 h_2(p_1 p_2) \), then either \( (h_2(p_1 p_2) = 2 \& q_3 = 2) \) or \( (h_2(p_1 p_2) = 4 \& q_3 = 1) \). We claim the latter does not hold. For, first by \((\alpha)\) on page 318 of [Kaplan 1976], \( Cl_2^+(k_3) \simeq (4) \).
Hence if the latter holds, then \( N_\varepsilon_1 = -1 \), which is not possible by [Kaplan 1976, Corollary 1]. Hence
\[
q_3 = 2.
\]
Finally consider \( q_1 \). First assume \( N_\varepsilon_1 = -1 \). Then by [Kubota 1956] the only possible square root of a nonsquare unit in \( K_1 \) would be \( \sqrt{\varepsilon_0} \) since the others have negative norm. Now applying [Benjamin et al. 1998, Proposition 3], for example, we see \( k_0(\sqrt{\varepsilon_0}) = k_0(\sqrt{3}) \), where by genus theory \( \delta | p_1 p_2 p_3 \) (but \( \neq \)) and \( \chi_j(\delta) = 1 \) for all genus characters of \( k_0 \). But then since \( (p_1 / p_2) = (p_3 / p_2) = 1 \), \( p_2 \) is trivial for all the genus characters and no other \( p_i \) has this property. Thus we may assume \( \delta = p_2 \) which is not a square in \( K_1 \). Thus
\[
N_\varepsilon_1 = -1 \implies q_1 = 1.
\]
Now assume \( N_\varepsilon_1 = +1 \). Then \( \delta_k = p_2 \) again and \( \delta_k = p_2 \) so that \( \varepsilon_0 \varepsilon_1 \) is a square in \( K_1 \) this time; again see [Kubota 1956]. Hence
\[
N_\varepsilon_1 = +1 \implies q_1 = 2.
\]
Therefore, for \( N \varepsilon_0 = 0 \), \( q = 2^4 \) if \( N_\varepsilon_1 = -1 \) and \( q = 2^5 \) if \( N_\varepsilon_1 = +1 \).

Case 2. Assume \( N \varepsilon_0 = -1 \). Since \( \text{Cl}_2(k_0) = \text{Cl}_2^+(k_0) \) is elementary, the Rédei–Reichardt conditions [1933] imply that
\[
a) \quad \left( \frac{p_i}{p_j} \right) = -1, \quad \text{for all } i \neq j, \quad \text{or} \quad b) \quad \left( \frac{p_1}{p_2} \right) = \left( \frac{p_1}{p_3} \right) = -\left( \frac{p_2}{p_3} \right) = -1.
\]
First consider \( a) \). Then \( (p_i p_j / p_\ell) = 1 \) for all distinct \( i, j, \ell = 1, 2, 3 \). By [Couture and Derhem 1992, Theorem 2], \( G \cong (2, 2) \) or \( H_8 \). Hence in the present situation \( G \cong H_8 \). Thus as noted above the order of \( H_i \) is 4 whence \( h_2(K_i) = 4 \) so that \( 4 = h_2(K_i) = q_i h_2(k_i) \), for \( i = 1, 2, 3 \). But \( (p_i / p_j) = -1 \) implies \( h_2(k_i) = 2 \). Therefore, \( q_i = 2 \) for \( i = 1, 2, 3 \) so \( q = 2^5 \).

Next consider \( b) \). As immediately above, \( q_2 = q_3 = 2 \). Now consider \( q_1 \). If \( N \varepsilon_1 = +1 \), then arguing as above shows \( q_1 = 1 \). If \( N \varepsilon_1 = -1 \), so that the norms of \( \varepsilon_1, \varepsilon_0 \) are negative, then \( q_1 = 1 \) if \( \sqrt{\varepsilon_0} \varepsilon_1 \varepsilon_0 \not\in K_1 \), and \( q_1 = 2 \) otherwise.

This establishes the theorem.

As a corollary to this theorem, we see that the structure \( G = \text{Gal}(k_0^2 / k_0) \) determines \( q(k^1 / \mathbb{Q}) \):

**Corollary 6.** Let \( k_0 \) satisfy all the conditions in Theorem 5. For \( G = \text{Gal}(k_0^2 / k_0) \),
\[
q(k^1 / \mathbb{Q}) = \begin{cases} 
2^4 & \text{if } G \text{ is abelian or dihedral}, \\
2^5 & \text{if } G \text{ is semidihedral or quaternion}.
\end{cases}
\]
Proof. This follows immediately by Theorem 1 of [Couture and Derhem 1992] and a stronger form of part of Theorem 2 of the same paper, as found in [Lemmermeyer 1994a]. The main change in Theorem 2 is the following: with the notation above Theorem 5 suppose \( N \varepsilon_0 = N \varepsilon_1 = -1 \). If \( \sqrt{p_1 \varepsilon_1 \varepsilon_0} \in K_1 \), then \( G \) is quaternion (of order 8 or larger). If \( \sqrt{p_1 \varepsilon_1 \varepsilon_0} \notin K_1 \), then \( G \) is dihedral. \( \square \)

The previous theorem is a special case of the following proposition:

**Proposition 7.** Let \( k \) be a complex quadratic field with \( \text{Cl}_2(k) \cong (2, 2, 2) \) and with \( \text{disc} \ k = d_1 d_2 d_3 d_4 \) where \( d_i \) are distinct prime discriminants divisible by primes \( p_i \) and \( d_1, d_2, d_3 \) are positive. With the notation above, assume that \( k_0^1 = k_0^2 \). Then \( q = q(k^1/\mathbb{Q}) = 2^4 \).

Proof. Recall that \( k_0 = \mathbb{Q}(\sqrt{p_1 p_2 p_3}) \), \( K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) \), and that \( q = q(K/\mathbb{Q}) \). Then Kuroda’s class number formula yields

\[
h_2(K) = \frac{1}{2^9} q h_2(k_0) h_2(k_1) h_2(k_2) h_2(k_3);
\]

(again, refer to the notation before the previous theorem). Now since \( k_0 \subseteq K \subseteq k^1_0 \), we see \( k^1_0 \subseteq K^1 \subseteq k^2_0 \), but since by assumption \( k^1_0 = k^2_0 \), we have \( K^1 = k^1_0 \). Hence

\[
h_2(K) = [K^1 : K] = [k^1_0 : K] = \frac{1}{4} [k^1_0 : k_0] = \frac{1}{4} h_2(k_0).
\]

Similarly \( K^1_i = k^1_0 \), for \( i = 1, 2, 3 \), whence

\[
h_2(K_i) = \frac{1}{2} h_2(k_0).
\]

On the other hand Kuroda’s class number formula again yields

\[
h_2(K_i) = \frac{1}{4} q_i h_2(k_0) h_2(k_i).
\]

All this implies

\[
\frac{1}{2} h_2(k_0) = \frac{1}{4} q_i h_2(k_0) h_2(k_i)
\]

so that \( 2 = q_i h_2(k_i) \). But then since \( 2 | h_2(k_i) \), we must have \( h_2(k_i) = 2 \). But then from above we have

\[
\frac{1}{4} h_2(k_0) = h_2(K) = \frac{1}{2^9} q h_2(k_0) h_2(k_1) h_2(k_2) h_2(k_3) = \frac{1}{2^6} q h_2(k_0).
\]

Therefore by solving for \( q \), we obtain

\[
q = 2^4.
\] \( \square \)
3. Examples

We now give numerical examples illustrating Theorem 5 with \( q = 2^4 \) and \( q = 2^5 \).

Example 1. Let \( k_0 = \mathbb{Q}(\sqrt{2405}) = \mathbb{Q}(\sqrt{5 \cdot 13 \cdot 37}) \) and \( K = \mathbb{Q}(\sqrt{5}, \sqrt{13}, \sqrt{37}) \).

By [Rédei and Reichardt 1933] or [Kaplan 1976] we see that \( \text{Cl}_2(k_0) \simeq (2, 2) \).

Moreover, we have \( N_{\epsilon_0} = -1 \) and \((13/5) = (37/5) = (37/13) = -1 \). Thus by [Couture and Derhem 1992, Theorem 2], \( \text{Gal}(k_0^5/k_0) \simeq H_8 \) or \( (2, 2) \); but [Benjamin et al. 1998, Theorem 1] then shows that \( \text{Gal}(k_0^2/k_0) \simeq H_8 \). Finally Theorem 4 above shows \( q = 2^5 \).

Example 2. Consider \( k_0 = \mathbb{Q}(\sqrt{290}) = \mathbb{Q}(\sqrt{2 \cdot 5 \cdot 29}) \); see the examples in [Couture and Derhem 1992]. Let \( K = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{29}) \).

By [Rédei and Reichardt 1933] or [Kaplan 1976] or even [Couture and Derhem 1992], we see that \( \text{Cl}_2(k_0) \simeq (2, 2) \).

Moreover, we have \( N_{\epsilon_0} = -1 \), where \( \epsilon_0 = 17 + \sqrt{290} \) is the fundamental unit of \( k_0 \); and \((2/5) = (2/29) = -(29/5) = -1 \). Now by genus theory \( K_1 = \mathbb{Q}(\sqrt{5 \cdot 29}, \sqrt{2}) \) (notation as in above). Also \( N_{\epsilon_1} = -1 \) where \( \epsilon_1 = 12 + \sqrt{145} \) is the fundamental unit of \( \mathbb{Q}(\sqrt{5 \cdot 29}) \). Finally, \( \epsilon_2 = 1 + \sqrt{2} \).

By the techniques described in [Kubota 1956] we see that \( \epsilon_0\epsilon_1\epsilon_2 \) is not a square in \( K_1 \). Theorem 5 above then shows \( q = 2^4 \). Furthermore, [Couture and Derhem 1992, Theorem 2] and PARI show \( \text{Gal}(k_0^5/k_0) \simeq D_4 \).

References


[Hall and Senior 1964] M. Hall, Jr. and J. K. Senior, \textit{The groups of order \( 2^n \) (n \leq 6)}, Macmillan, New York, 1964. MR 29 #5889 Zbl 0192.11701


Received August 14, 2005.