

# THE STRUCTURE OF THE 2-SYLOW SUBGROUPS OF THE IDEAL CLASS GROUPS OF IMAGINARY BICYCLIC BIQUADRATIC FIELDS

CHARLES J. PARRY and RAMONA R. RANALLI

Department of Mathematics  
Virginia Tech  
Blacksburg, VA 24061, U. S. A.

Department of Mathematics  
University of Texas at Tyler  
3900 University Boulevard  
Tyler, TX 75799, U. S. A.

## Abstract

In this article a method for determining the structure of the 2-Sylow subgroup of the class group of an imaginary bicyclic biquadratic number field is described. As an application of our method, the structure of the 2-class group of all known imaginary bicyclic biquadratic extensions of  $\mathbb{Q}$  with class numbers 8 and 16 is determined.

## 1. Introduction

Given a bicyclic biquadratic field  $K$ , we wish to be able to determine the structure of the class group of  $K$  whenever the structure of the class groups of the three quadratic subfields is known. It is easy to show that the odd part of the class group of  $K$  is the direct product of the odd parts of the class groups of the quadratic subfields. However, the structure of

---

2000 Mathematics Subject Classification: 11R29, 11R16.

Keywords and phrases: class group, biquadratic fields.

Communicated by Jannis A. Antoniadis

Received October 25, 2006

the 2-Sylow subgroup,  $H$ , of the class group of  $K$  is much more difficult to determine. All notations are defined in Section 2. Section 3 details a method for determining  $H$  when the structure of the 2-class groups of the quadratic subfields is known. Various examples are presented in Section 4 where specific difficulties such as the need to normalize the characters of the real field, strong ambiguous and weak ambiguous classes are addressed. We conclude the section with a description of the algorithm. The final section contains a summary of tables of all known imaginary bicyclic extensions of  $Q$  with class numbers 8 and 16, as well as the specific structures of each. With one exception these tables are too long to be included here. All results in this section were obtained by applying the method given in Sections 3 and 4.

## 2. Notation

The following notations will be used throughout the remainder of this article.

$K$ : An imaginary bicyclic biquadratic extension of  $Q$ .

$k_1, k_2, k_3$ : The quadratic subfields of  $K$  with  $k_2$  real.

$d_1, d_2, d_3$ : Square free integers with  $k_i = Q(\sqrt{d_i})$  for  $i = 1, 2, 3$ .

$f$ : The conductor of  $K$ .

$H, H_1, H_2, H_3$ : The 2-Sylow subgroups of the ideal class groups of  $K, k_1, k_2$  and  $k_3$ , respectively.

$h, h_1, h_2, h_3$ : The 2-class numbers of  $K, k_1, k_2$  and  $k_3$ , respectively.

$\hat{H}_i$ : The group of quadratic characters on the group  $H_i$ . Each element of  $\hat{H}_i$  corresponds to a genus in  $H_i$  for  $i = 1, 2, 3$ .

$\tilde{A}$ : The ideal class determined by the ideal  $A$ .

$\hat{S}$ : The subgroup of  $\hat{H}_1 \times \hat{H}_2 \times \hat{H}_3$  consisting of all of those characters that are consistent on each pair of  $H_1, H_2$  and  $H_3$ .

$S$ : The subgroup of  $H_1 \times H_2 \times H_3$  with character group  $\hat{S}$ .

$\theta$ : The homomorphism of  $\hat{H}_1 \times \hat{H}_2 \times \hat{H}_3 \rightarrow H$  defined by  $\theta(C_1, C_2, C_3) = C_1 C_2 C_3$ .

$\ker$ : The kernel of  $\theta$ .

$H_0$ : The image of  $\theta$ .

$t$ : The positive integer determined such that  $2^t$  is the product of all the ramification indices of all the rational primes for the extension  $K/Q$ .

$t_i$ : The number of rational primes ramified in the extension  $k_i/Q$  for  $i = 1, 2, 3$ .

$r_a$ : The rank of  $H_1 \times H_2 \times H_3$ .

$r_H$ : The rank of  $H$ .

$l, q, r, s$ : Distinct prime numbers.

$(l, q, r)$ : An element of  $H_1 \times H_2 \times H_3$  determined by the ideal classes of prime divisors of  $l, q$  and  $r$  in  $k_1, k_2$  and  $k_3$ , respectively.

$\psi$ : The isomorphism from the multiplicative group  $\{\pm 1\}$  to the additive group  $Z_2$ .

$\left(\frac{a}{b}\right)$ : The Kronecker symbol using the convention  $\left(\frac{b}{2}\right) = \left(\frac{2}{b}\right)$  for all odd positive integers  $b$ .

$u, v, w, x, y, z$ :  $\psi\left(\frac{q}{s}\right), \psi\left(\frac{r}{s}\right), \psi\left(\frac{q}{r}\right), \psi\left(\frac{l}{q}\right), \psi\left(\frac{l}{r}\right), \psi\left(\frac{l}{s}\right)$  respectively.

$M$ : A  $Z_2$ -matrix determined by  $\hat{S} \cdot k \hat{e} r$ .

### 3. Class Group Structure of Imaginary Bicyclic Biquadratic Extensions

In this section we discuss a general method for determining the structure of the 2-class group,  $H$ , of any imaginary bicyclic biquadratic field.

**Lemma 1.** *Let  $(C_1, C_2, C_3) \in S$ . Then there is a prime  $p$  of  $Q$  which has a prime divisor  $P_0$  in  $K$  such that  $\mathfrak{p}_i = P_0 \cap k_i = P_0 P_i$  with  $\mathfrak{p}_i$  and  $C_i$  in the same genus of  $k_i$  where  $(p) = P_0 P_1 P_2 P_3$  in  $K$ .*

**Proof.** Since the characters on  $C_i$  in  $\hat{H}_i$  are consistent with one another for  $i = 1, 2, 3$ , there is a prime  $p$  of  $Q$  which satisfies these character values. Now  $p$  splits completely in  $K$  and so  $(p) = P_0 P_1 P_2 P_3$  in  $K$ . Since the Galois group of  $K/Q$  is transitive on the primes  $P_0, P_1, P_2$  and  $P_3$  there is a  $\sigma_i$  in  $G(K/Q)$  such that  $\sigma_i(P_0) = P_i$ . Number the primes  $P_1, P_2$  and  $P_3$  so that  $\sigma_i$  fixes the subfield  $k_i$  of  $K$ . Let  $\mathfrak{p}_i = P_0 \cap k_i$  for  $i = 1, 2, 3$ . Then  $\mathfrak{p}_i = P_0 P_j \cap k_i$  for some  $j$ . Since the Galois group of  $K/k_i$  is transitive on the factors of  $\mathfrak{p}_i$  and  $G(K/k_i) = \{1, \sigma_i\}$  we have  $\sigma_i(P_0) = P_i$  and so, by the definition of  $\sigma_i$ ,  $\mathfrak{p}_i = P_0 \cap k_i = P_0 P_i \cap k_i$ . Since  $\mathfrak{p}_i$  and  $C_i$  have the same character values they are in the same genus.

**Theorem 2.** *The homomorphism  $\theta$  induces an isomorphism*  

$$\frac{S^{2^i}}{S^{2^i} \cap \ker} \simeq H^{2^{i+1}} \text{ for any integer } i \geq 0.$$

**Proof.** Let  $(C_1^{2^i}, C_2^{2^i}, C_3^{2^i})$  in  $S^{2^i}$  with  $(C_1, C_2, C_3) \in S$ . By Lemma 1 we have a prime  $p$  in  $Q$  which splits completely in  $K$  and has a prime divisor  $P_0$  such that  $\mathfrak{p}_i = P_0 \cap k_i = P_0 P_i \cap k_i$ , where  $(p) = P_0 P_1 P_2 P_3$  in  $K$  with  $\mathfrak{p}_i$  and  $C_i$  in the same genus. Note that  $(\mathfrak{p}_1^{2^i}, \mathfrak{p}_2^{2^i}, \mathfrak{p}_3^{2^i})$  in  $S^{2^i}$  with  $\mathfrak{p}_i$  and  $C_i$  being in the same genus of  $k_i$ . Now

$$\theta(\mathfrak{p}_1^{2^i}, \mathfrak{p}_2^{2^i}, \mathfrak{p}_3^{2^i}) = \mathfrak{p}_1^{2^i} \mathfrak{p}_2^{2^i} \mathfrak{p}_3^{2^i} = (\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3)^{2^i} = (P_0^2 p)^{2^i} \sim P_0^{2^{i+1}} \in H^{2^{i+1}}.$$

Here  $\sim$  denotes equivalent ideal classes. Since  $\mathfrak{p}_i C_i^{-1}$  is in the principal genus of  $k_i$ ,  $\mathfrak{p}_i C_i^{-1} \sim B_i^2$  for some class  $B_i$  of  $k_i$ . Hence

$$(\mathfrak{p}_1 C_1^{-1}, \mathfrak{p}_2 C_2^{-1}, \mathfrak{p}_3 C_3^{-1}) \sim (B_1^2, B_2^2, B_3^2),$$

so

$$B_1^2 B_2^2 B_3^2 \sim (\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3) (C_1 C_2 C_3)^{-1} \sim P_0^2 (C_1 C_2 C_3)^{-1}.$$

Therefore

$$(B_1 B_2 B_3)^{2^{i+1}} \sim P_0^{2^{i+1}} (C_1^{2^i} C_2^{2^i} C_3^{2^i})^{-1}$$

and  $C_1^{2^i} C_2^{2^i} C_3^{2^i} \in H^{2^{i+1}}$ .

Conversely, let  $C^{2^{i+1}} \in H^{2^{i+1}}$  and  $P_0 \in C$  be a prime ideal of degree 1 and index 1 over  $Q$ . Let  $\mathfrak{p}_i = P_0 \cap k_i$  for  $i = 1, 2, 3$ . Then  $\mathfrak{p}_1 = P_0 P_1$ ,  $\mathfrak{p}_2 = P_0 P_2$  and  $\mathfrak{p}_3 = P_0 P_3$ , where  $P_0 \cap Q = (p) = P_0 P_1 P_2 P_3$ . Now  $(\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3) \in S$  and  $\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \sim P_0^2 \sim C^2$ . Thus  $\mathfrak{p}_1^{2^i} \mathfrak{p}_2^{2^i} \mathfrak{p}_3^{2^i} \sim P_0^{2^{i+1}} \sim C^{2^{i+1}}$ . Therefore

$$\frac{S^{2^i}}{S^{2^i} \cap \ker} \simeq H^{2^{i+1}}.$$

**Theorem 3.** 
$$\frac{H^{2^{i+1}}}{H^{2^{i+2}}} \simeq \frac{S^{2^i} \cap \text{amb}}{S^{2^i} \cap \ker} \cdot (S^{2^{i+1}} \cap \ker).$$

**Proof.** Let  $S = \langle C_1, C_2, C_3, \dots, C_k \rangle$ , and  $o(C_{k+1}) = 1$ . Arrange the  $C_i$  so that  $o(C_1) \geq o(C_2) \geq o(C_3) \geq \dots \geq o(C_k)$ . Then, for any  $i$  where  $2^i < o(C_1)$ , there exists an  $m_i$  such that  $o(C_{m_i}) > 2^i$  and  $o(C_{m_i+1}) \leq 2^i$ .

Thus  $S^{2^i} = \langle C_1^{2^i}, C_2^{2^i}, C_3^{2^i}, \dots, C_{m_i}^{2^i} \rangle$ . Then we see that  $\frac{S^{2^i}}{S^{2^{i+1}}} \simeq Z_2 \times Z_2$

$\times \dots \times Z_2$ , where the rank of the right-hand side is  $m_i$  and  $S^{2^i} \cap \text{amb} \simeq Z_2 \times Z_2 \times \dots \times Z_2$  with the rank of the right side again being  $m_i$ . Now, by Theorem 1,

$$\frac{H^{2^{i+1}}}{H^{2^{i+2}}} \simeq \frac{\frac{S^{2^i}}{S^{2^{i+1}} \cap \ker}}{S^{2^{i+1}} \cap \ker}.$$

Using a simple order argument we now see that

$$\begin{aligned} \frac{|S^{2^i}|}{|S^{2^i} \cap \ker|} \cdot \frac{|S^{2^{i+1}} \cap \ker|}{|S^{2^{i+1}}|} &= \frac{\left| \frac{S^{2^i}}{S^{2^{i+1}}} \right|}{|S^{2^i} \cap \ker|} \cdot |S^{2^{i+1}} \cap \ker| \\ &= \left| \frac{S^{2^i} \cap \text{amb}}{S^{2^i} \cap \ker} \right| \cdot |S^{2^{i+1}} \cap \ker|. \end{aligned}$$

The isomorphism follows since both groups are elementary.

The rank of  $H$  can easily be computed using the following theorem which is proved in our earlier article [9].

**Theorem 4.** *Let  $m$  denote the rank of  $\hat{S} \cdot \hat{k}\hat{e}r$ . Then*

$$r_H = r_a + t - 2 - m = \begin{cases} 3t - 7 - m & \text{if } r_a = 2t - 5. \\ 3t - 6 - m & \text{if } r_a = 2t - 4. \\ 3t - 5 - m & \text{if } r_a = 2t - 3. \end{cases}$$

Below we give an example of how this theorem is applied. Lemma 1 of [9] shows the rank of  $\hat{S}$  is  $t - 2$  and Kubota [8] shows the rank of  $\hat{k}\hat{e}r$  is  $t - 1$  or  $t - 2$  according as the unit index of  $K$  is 1 or 2. Let  $n = \text{rank } \hat{S} + \text{rank } \hat{k}\hat{e}r$  and  $M$  be an  $n \times r_a$   $\mathbb{Z}_2$ -matrix whose rows correspond to generators of  $\hat{S} \cdot \hat{k}\hat{e}r$  by means of the isomorphism  $\psi$ . Then  $m$  is the rank of  $M$ .

Note that the characters of the real field will often have to be normalized in order to ensure that  $-1$  lies in the principal genus. This is done by multiplying one column where  $-1$  has a negative character by each of the other columns where  $-1$  also has a negative character. The initial choice of column does not matter. The following example illustrates this as well as the technique for finding  $r_H$ .

**Example.** Let  $k_1 = Q(\sqrt{-lqrs})$ ,  $k_2 = Q(\sqrt{lq})$  and  $k_3 = Q(\sqrt{-rs})$  with  $l \equiv q \equiv r \equiv 3 \pmod{4}$  and  $s \equiv 1 \pmod{4}$ . Here the unit index is 1,  $t = 4$  and  $r_a = 4$ . Normalizing the character of the real field, the table of

consistent characters is

$l$	$q$	$r$	$s$	$lq$	$r$	$s$
+	+	+	+	+	+	+
-	-	+	+	+	+	+
+	+	-	-	+	-	-
-	-	-	-	+	-	-

Here  $\hat{S}$  is generated by  $(1, 1, 0, 0, 0, 0, 0)$  and by  $(0, 0, 1, 1, 0, 1, 1)$  representing a + by a 0 and a - by a 1. Moreover,  $\ker$  is generated by  $\{(l, 1, 1), (q, 1, 1), (r, 1, r)\}$ . Since in  $k_2$  the character  $lq$  is always + it will just generate a column of zeroes in our matrix and so can be deleted. Thus our columns will correspond to  $l, q$  and  $r$  in  $k_1$  and  $r$  in  $k_3$ . So our matrix is

$$\begin{aligned}
 M &= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ \psi\left(\left(\frac{l}{q}\right)\left(\frac{l}{r}\right)\left(\frac{l}{s}\right)\right) & \psi\left(\frac{l}{q}\right) & \psi\left(\frac{l}{r}\right) & 0 \\ 1 + \psi\left(\frac{l}{q}\right) & \psi\left(\left(\frac{q}{l}\right)\left(\frac{q}{r}\right)\left(\frac{q}{s}\right)\right) & \psi\left(\frac{q}{r}\right) & 0 \\ 1 + \psi\left(\frac{l}{r}\right) & 1 + \psi\left(\frac{q}{r}\right) & \psi\left(\left(\frac{l}{r}\right)\left(\frac{r}{s}\right)\left(\frac{q}{r}\right)\right) & \psi\left(\frac{r}{s}\right) \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ x + y + z & x & y & 0 \\ 1 + x & 1 + x + u + w & w & 0 \\ 1 + y & 1 + w & y + v + w & v \end{pmatrix} \\
 &\sim \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & y + z & y & 0 \\ 0 & u + w & w & 0 \\ 0 & w + y & w + y & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & z & y \\ 0 & 0 & u & w \\ 0 & 0 & 0 & w + y \end{pmatrix},
 \end{aligned}$$

where the first two rows correspond to the generators of  $\hat{S}$  and the last three rows correspond to generators of  $\ker$ . We have deleted one character from each subfield since the product of the characters for a quadratic field

is +1. The first three columns correspond to characters for  $k_1$ , determined by  $l$ ,  $q$  and  $r$ , and the last column to a character for  $k_3$ , determined by  $r$ . Elementary row and column operations lead us to the final two matrices from which we can conclude that

$$m = \begin{cases} 2 & \text{if } u = w = y = z = 0. \\ 3 & \text{if either } u \neq z \text{ and } w = y = 0 \text{ or } w \neq y \text{ and } u = z = 0 \\ & \text{or } u = z, w = y, \text{ not all zero.} \\ 4 & \text{if either } u \neq z, w = 1 \text{ or } y = 1 \text{ or } w \neq y, u = 1 \text{ or } z = 1. \end{cases}$$

Now  $r_a = 4$  and  $t = 4$  so  $r_H = 6 - m$ . Let

$$A = \begin{pmatrix} x + y + z & x & y \\ 1 + x & 1 + x + u + w & w \\ 1 + y & 1 + w & y + v + w \end{pmatrix}$$

and  $\gamma = \mathbb{Z}_2$ -rank of  $A$ . Then  $H_1$  has exactly  $3 - \gamma$  cyclic factors of order greater than 2. Also  $H_3$  has order 2 exactly when  $v = 1$ . When both  $H_1$  and  $H_3$  are elementary then  $h = 8$  and  $m = 3$  or 4, so  $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  or  $\mathbb{Z}_2 \times \mathbb{Z}_4$ . The following table gives the values of  $m$  in the cases when both  $H_1$  and  $H_3$  are elementary.

$u$	$w$	$x$	$y$	$z$	$m$
0	0	0	0	1	3
0	0	0	1	0	3
0	0	0	1	1	4
0	1	1	0	0	3
0	1	1	0	1	4
0	1	1	1	1	4
1	0	0	1	0	4
1	0	0	1	1	4
1	0	1	0	0	3
1	1	0	1	0	4
1	1	1	0	0	4
1	1	1	0	1	4



When  $m = 2$ , so  $r_H = 4$ ,  $H_1$  has either 1 or 2 cyclic factors of order greater than 2 according as  $v = 1$  or 0. Thus  $h = 16k$  or  $64k$ , where  $k \geq 1$  is a power of 2. When  $v = k = 1$ ,  $H$  is elementary of rank 4. When  $v = 0$  it is easily seen that

$$S \cap amb / S \cap ker$$

has order 2 and that  $S^2 \cap ker$  has order 4 or less. Thus  $H$  has between 1 and 3 cyclic factors of order 2.

Now we are ready to describe a method for computing the structure of  $H$  for any imaginary bicyclic biquadratic field  $K$ . The following proposition will be helpful.

**Proposition 1.** *Let  $b = 2^j$  for some  $j > 1$ , where  $b \mid h_i$  for some  $i = 1, 2, 3$ . Also, let  $T = S^2$ . If  $(C_1^{b/2}, C_2^{b/2}, C_3^{b/2})$  is in  $T^{b/2} \cap amb$ , then  $(C_1^{b/2}, 1, 1)$ ,  $(1, C_2^{b/2}, 1)$  and  $(1, 1, C_3^{b/2})$  are in  $T^{b/4} \cap amb$ .*

**Proof.** Let  $(C_1, C_2, C_3)^{b/2} = (C_1^{b/2}, C_2^{b/2}, C_3^{b/2})$  be in  $T^{b/2} \cap amb$ . Then  $C_i^{b/2}$  is ambiguous for each  $i$ . Since  $C_1^2$  is in the principal genus of  $k_1$ ,  $(C_1^2, 1, 1)$  is in  $T$ , so  $(C_1^{b/2}, 1, 1) = (C_1^2, 1, 1)^{b/4}$  is in  $T^{b/4} \cap amb$ . A similar argument is true for  $(1, C_2^{b/2}, 1)$  and  $(1, 1, C_3^{b/2})$ .

#### 4. Examples and Statement of Algorithm

Now we would like to compute  $H$  for a variety of cases in order to get a feel for the algorithm. The first is straight-forward, while the others will demonstrate some of the slightly more complicated scenarios.

**Example.** Let  $d_1 = -406$ ,  $d_2 = 182$  and  $d_3 = -377$ . Here  $H_1 \simeq H_3 \simeq Z_8 \times Z_2$  and  $H_2 \simeq Z_2$ . The  $ker$  is  $\{(1, 1, 1), (1, 1, 13), (1, 2, 2), (1, 2, 26), (2, 1, 2), (2, 1, 26), (2, 2, 1), (2, 2, 13), (7, 1, 2), (7, 1, 26), (7, 2, 1), (7, 2, 13), (14, 1, 1), (14, 1, 13), (14, 2, 2), (14, 2, 26)\}$ .

The table of consistent characters is

2	7	29	-2 · 7	13	-1	13	29
+	+	+	+	+	+	+	+
-	-	+	+	+	+	+	+
+	-	-	+	+	-	+	-
-	+	-	+	+	-	+	-
+	-	-	-	-	+	-	-
-	+	-	-	-	+	-	-
+	+	+	-	-	-	-	+
-	-	+	-	-	-	-	+

Note that we have normalized the characters of the real field and that in  $k_3$  the  $-1$  denotes the character  $\left(\frac{-1}{n}\right)$  determined by the ramified prime

2. In  $k_1$  we find that 2 has the character values  $- + -$  and that 7 is in the principal genus. Thus the character values  $- + -$  represent a genus with elements of order two and the other non-principal genera contain only classes with elements of order eight. In these latter genera, the fourth power of any element is in the principal genus and is ambiguous, so it can be represented by 7. In  $k_3$ , the character of 2 has values  $+ - -$  and 13 is in the principal genus. Thus  $+ - -$  represent a genus with elements of order two and the other non-principal genera contain only classes with elements of order eight. In these latter genera, the fourth power of any element in the principal genus and is ambiguous and so can be represented by 13. The following table reflects this information.

-2 · 7 · 29	2 · 7 · 13	-1 · 13 · 29
(1, 1)	(1, 1)	(1, 1)
(4, 7)	(1, 1)	(1, 1)
(4, 7)	(1, 1)	(4, 13)
(1, 1)	(1, 1)	(4, 13)
(4, 7)	(1, 1)	(1, 1)
(1, 1)	(1, 1)	(1, 1)
(1, 1)	(1, 1)	(4, 13)
(4, 7)	(1, 1)	(4, 13)

In this table each  $(a, b)$  with  $a > 1$  means that in the corresponding genus there is an element of order  $2a$  whose  $a$ th power is in the class represented by a divisor of  $b$ . This is also true when  $a = 1$  except in the case of the principal genus and the principal genus contains no class of order 2. In this exceptional case the principal genus has a class of order 1 whose square is the identity class. Thus, in this example, we see that  $S^4 \cap amb$  is given by  $\langle (7, 1, 1), (1, 1, 13) \rangle$  and that  $S^4 \cap \ker$  is  $\langle (1, 1, 13) \rangle$ .

Thus  $\frac{S^4 \cap amb}{S^4 \cap \ker} \simeq Z_2$  and  $\frac{H^8}{H^{16}} \simeq Z_2$ . Hence there is a factor of  $Z_{16}$  in  $H$ .

Now we see that for the square everything remains the same. So  $S^2 \cap amb = \langle (7, 1, 1), (1, 1, 13) \rangle$  and  $S^2 \cap \ker = \langle (1, 1, 13) \rangle$ . Thus,  $\frac{S^2 \cap amb}{S^2 \cap \ker} \simeq Z_2$ , so Theorem 3 shows  $\frac{H^4}{H^8} \simeq Z_2 \times Z_2$ . One  $Z_2$  is determined by the factor of  $Z_{16}$  that we already have, but the other one indicates there is a factor of  $Z_8$  in  $H$ .

Using the methods already described, we can determine that the rank of  $H$  is three and the order is  $2^8$ . Thus we have one more factor of order 2. Clearly then,  $H \simeq Z_{16} \times Z_8 \times Z_2$ .

Things worked out in a very straight-forward manner in this example because each  $H_i$  had at most one non-elementary factor. This meant that, once we identified the genera that contained the ambiguous classes, we knew the order of the classes of the other genera. If there are two or more non-elementary factors of unequal order in some  $H_i$ , then this will not be the case. To determine  $S^m \cap amb$  for any  $m = 2^j$ , where  $j$  is a whole number, we must know not only the minimum order of a class in each genus but also the ambiguous class in the principal genus which it generates.

Let  $q$  be an unramified prime whose character values place its prime divisors in a genus that does not contain ambiguous classes. Say  $\mathfrak{q}$ , a prime divisor of  $q$  in  $k_i$ , belongs to a class of order  $m$ . Then  $\mathfrak{q}^{m/2}$  belongs to an ambiguous class in the principal genus. Assume that  $\mathfrak{p}$  is an

ambiguous ideal in this class (this is always the case when  $k_i$  is imaginary). Then  $\mathfrak{q}^{m/2}\mathfrak{p} \sim (1)$  is a principal ideal of  $k_i$ . If  $\mathfrak{q}^{m/2}\mathfrak{p} = (x + \sqrt{d_i}y)$ , where  $x$  and  $y$  are both integers or half of integers then  $x^2 - d_i y^2 = q^{m/2}p$ . Conversely, assume  $x^2 - d_i y^2 = 2^l q^{m/2}p$ , where  $l = 0$ , unless  $d_i \equiv 1 \pmod{4}$  and then  $l = 0$  or  $2$  and  $\gcd(x, qp) = 1$ . If  $p$  ramifies in the field  $k_i$  and if the prime divisor  $\mathfrak{p}$  in  $k_i$  is not principal then the prime divisors of  $\mathfrak{q}$  in  $k_i$  belong to classes of order  $m$ .

For each ramified ( $p$ ) in the principal genus the key to solving such problems will be to find an  $x$  and  $y$  in  $Z$  and a prime  $\mathfrak{q}$  in a non-principal genus such that  $x^2 - d_i y^2 = pq^{m/2}$ . The genus which contains the divisors of  $\mathfrak{q}$  contains the classes of order  $m$ .

A slight complication occurs if the class group  $k_i$  contains one or more factors of odd order. In this case the right-hand side of the equation may be  $\mathfrak{q}^{gm}$ , where  $g$  is an odd divisor of the class number  $k_i$ .

**Example.** For our next problem let  $d_1 = -18761$ ,  $d_2 = 2482$  and  $d_3 = -8738$ . Here  $H_1 \simeq Z_{32} \times Z_4$ ,  $H_2 \simeq Z_4 \times Z_2$  and  $H_3 \simeq Z_{16} \times Z_4$ . First note that the *ker* is  $\{(1, 1, 1), (1, 2, 2), (1, 17, 17), (1, 34, 34), (2, 1, 2), (2, 2, 1), (2, 17, 34), (2, 34, 17), (73, 1, 34), (73, 2, 17), (73, 17, 2), (73, 34, 1), (146, 1, 34), (146, 2, 34), (146, 17, 1), (146, 34, 2)\}$ . The table of consistent characters is

-1	73	257	2	17	73	-2	17	257
+	+	+	+	+	+	+	+	+
-	+	-	+	+	+	-	+	-
+	-	-	+	-	-	+	-	-
-	-	+	+	-	-	-	-	+
+	-	-	-	+	-	-	+	-
-	-	+	-	+	-	+	+	+
+	+	+	-	-	+	-	-	+
-	+	-	-	-	+	+	-	-

Note that in this case the characters of the real field did not have to be normalized. Finding the ambiguous classes in the principal genus, we see

that in  $k_1$  the divisors of 2 and of 73 are both in the principal genus, in  $k_2$  it is the divisors of 2 and, in  $k_3$ , the divisors of 2 and of 17. In  $k_2$ , 17 is in the genus with character values  $+-$ .

It is necessary in this case, for both of the imaginary fields, to find the quadratic representations of a prime in the non-principal genera. It will be sufficient to find two such primes (perhaps even in the same genus) where some power of each is in the same ambiguous class as the divisors of 2, 73, or 146 in  $k_1$  and as 2, 17 or 34 in  $k_3$ . For  $k_1$  we get

$$(73 \cdot 4)^2 + 18761 \cdot 3^2 = 73 \cdot 59^2$$

$$141^2 + 18761 = 2 \cdot 139^2.$$

Since we find that both 59 and 139 have characters  $--+$ , we know this genus contains classes of order four which square to an ambiguous class containing divisors of 2 (and 73). The other non-principal genera must have classes of order thirty-two whose sixteenth power is an ambiguous class containing divisors of 146 (since 73 was also seen to be a square).

For  $k_3$  we get

$$108^2 + 8738 = 2 \cdot 101^2$$

$$51^2 + 8738 \cdot 2^2 = 17 \cdot 47^2.$$

Here 101 and 47 have characters  $-+-$  and so we know this genus contains classes of order four which square to an ambiguous class containing divisors of 2 (and 17). So the other non-principal genera must have classes of order sixteen whose eighth power is in an ambiguous class containing divisors of 34. Thus, using the quadratic representations, we get the following table

$-1 \cdot 73 \cdot 257$	$2 \cdot 17 \cdot 73$	$-2 \cdot 17 \cdot 257$
(1, 1)	(1, 1)	(1, 1)
(16, 146)	(1, 1)	(2, 2)
(16, 146)	(1, 1)	(8, 34)
(2, 2)	(1, 1)	(8, 34)
(16, 146)	(2, 2)	(2, 2)
(2, 2)	(2, 2)	(1, 1)
(1, 1)	(2, 2)	(8, 34)
(16, 146)	(2, 2)	(8, 34)

Again, in this table each  $(a, b)$  means that in that genus there is an element of order  $2a$  whose  $a$ th power is in the class represented by a divisor of  $b$ . Thus, in this example, we see that  $S^{16} \cap amb$  is given by

$\langle(146, 1, 1)\rangle$  and that  $S^{16} \cap ker$  is  $\langle(1, 1, 1)\rangle$ . Thus  $\frac{S^{16} \cap amb}{S^{16} \cap ker} \simeq Z_2$  and

$\frac{H^{32}}{H^{64}} \simeq Z_2$ . Hence there is a factor of  $Z_{64}$  in  $H$ . Now we see that for the

eighth power we have  $S^8 \cap amb = \langle(146, 1, 1), (1, 1, 34)\rangle$  and  $S^8 \cap ker$

$= \langle(1, 1, 1)\rangle$ . And so,  $\frac{S^8 \cap amb}{S^8 \cap ker} \simeq Z_2 \times Z_2$  making  $\frac{H^{16}}{H^{32}} \simeq Z_2 \times Z_2$ . One

$Z_2$  is determined by the factor of  $Z_{64}$  that we already have, but the other one indicates there is a factor of  $Z_{32}$  in  $H$ . Clearly, since there are

no terms  $(a, b)$  in the above table with  $a = 4$ ,  $S^4 \cap amb \simeq S^8 \cap amb$  so

we move on to  $S^2$ . Since  $S^2 \cap amb = \langle(146, 1, 1), (1, 1, 34), (2, 2, 1)\rangle$  and

$S^2 \cap ker = \langle(2, 2, 1)\rangle$  we have  $\frac{S^2 \cap amb'}{S^2 \cap ker} \simeq Z_2 \times Z_2$  and  $\frac{H^4}{H^8} \simeq Z_2 \times Z_2$ .

Both of these are accounted for by the factors of  $H$  already obtained. So all other factors of  $H$  are of order 2 or 4. Since it can be determined by previous methods that  $H$  has rank 5 and  $h = 2^{15}$  we see that  $H \simeq Z_{64} \times Z_{32} \times Z_4 \times Z_2 \times Z_2$ .

In our next example we will examine a special case for the real field: weak ambiguous classes. While these do not happen very often, they do occur and so must be dealt with. If in the real field the character values of  $-1$  are all positive and the norm of the fundamental unit is  $+1$ , then there exists at least one ambiguous class which does not contain an ambiguous ideal. Such a class is referred to as a weak ambiguous class. The number of such classes occurring is the same as the number of classes generated by taking the product of all strong ambiguous classes with any one of the weak ambiguous classes. In other words, half of the ambiguous classes will be weak. When this occurs we know that for some  $w_i$  in  $H_2$  the divisors of  $w_i^2$  are in the principal genus. It is not always necessary to know exactly what  $w_i$  is, only that it exists.

**Example.** For our next problem let  $d_1 = -1326$ ,  $d_2 = 14722$  and  $d_3 = -16887$ . Here  $H_1 \simeq Z_2 \times Z_2 \times Z_2$ ,  $H_2 \simeq Z_4 \times Z_4$  and  $H_3 \simeq Z_4 \times Z_8$ , where the class numbers of  $k_1$  and  $k_3$  have odd factors of 5 and 3, respectively. These can put a slight twist on the calculations for the quadratic representations. Next note that the *ker* is  $\{(1, 1, 1), (1, 17, 39), (2, 1, 1), (2, 17, 39), (3, 1, 3), (3, 17, 13), (6, 1, 3), (6, 17, 13), (13, 1, 13), (13, 17, 3), (17, 1, 39), (17, 17, 1), (26, 1, 13), (26, 17, 3), (34, 1, 39), (34, 17, 1)\}$ .

The table of consistent characters is

2	3	13	17	2	17	433	3	13	433
+	+	+	+	+	+	+	+	+	+
+	-	-	+	+	+	+	-	-	+
+	+	-	-	+	-	-	+	-	-
+	-	+	-	+	-	-	-	+	-
-	+	-	+	-	+	-	+	-	-
-	-	+	+	-	+	-	-	+	-
-	+	+	-	-	-	+	+	+	+
-	-	-	-	-	-	+	-	-	+

Observe that again in this case the characters of the real field did not have to be normalized. Finding the ambiguous classes in the principal genus, we see that in  $k_1$  all genera contain ambiguous classes, and in  $k_2$  all discriminantal divisors are in the principal genus. However,

$$364^2 - 3^2 \cdot 14722 = -2,$$

so the divisors of 2 and  $17 \cdot 433$  are in the principal class. Hence the divisor of 17 is the only nonprincipal strong ambiguous divisor. Since the norm of the fundamental unit here is +1 and the characters of -1 are all positive, there are two weak ambiguous classes. We find that  $1517^2 - 14722 \cdot 2^2 = 17 \cdot 19^2$ . The characters for 19 in  $k_2$  are  $- + -$ . Thus the divisor of (17) is a square of a class in this genus. Now there must be two weak ambiguous classes. Let  $w_1$  and  $w_2$  be their representatives whose divisors are in the principal genus. Then  $17w_1 \sim w_2$ . Now, in  $k_3$

the all ambiguous divisors are in the principal genus. Using the quadratic representations for  $k_3$  we get

$$186^2 + 16887 = 3 \cdot 131^2$$

$$377^2 + 16887 \cdot 2^2 = 13 \cdot 127^2.$$

Here 131 and 127 give the character values  $- + -$  and  $+ + +$ . Hence we get the following table

$-2 \cdot 3 \cdot 13 \cdot 17$	$2 \cdot 17 \cdot 433$	$-3 \cdot 13 \cdot 433$
(1, 1)	(1, 1)	(1, 1)
(1, 1)	(1, 1)	(4, 13)
(1, 1)	(2, $17w_1$ )	(4, 13)
(1, 1)	(2, $17w_1$ )	(2, 3)
(1, 1)	(2, 17)	(4, 13)
(1, 1)	(2, 17)	(2, 3)
(1, 1)	(2, $w_1$ )	(1, 1)
(1, 1)	(2, $w_1$ )	(4, 13)

Again, in this table each  $(a, b)$  means that in that class there is an element of order  $2a$  whose  $a$ th power is in the class represented by a divisor of  $b$ . Thus, in this example, we see that  $S^4 \cap amb$  is given by  $\langle(1, 1, 13)\rangle$  and that  $S^4 \cap \ker$  is  $\langle(1, 1, 1)\rangle$ . Thus  $\frac{S^4 \cap amb}{S^4 \cap \ker} \simeq Z_2$  and

$\frac{H^8}{H^{16}} \simeq Z_2$ . Hence there is a factor of  $Z_{16}$  in  $H$ . Now we see that for

the second power we have  $S^2 \cap amb = \langle(1, 1, 13), (1, w_1, 1), (1, 17w_1, 3), (1, 17, 3)\rangle = \langle(1, 1, 13), (1, w_1, 1), (1, 17, 3)\rangle$  and  $S^2 \cap \ker = \langle(1, 17, 39)\rangle$ . And

so,  $\frac{S^2 \cap amb}{S^2 \cap \ker} \simeq Z_2 \times Z_2$  making  $\frac{H^4}{H^8} \simeq Z_2 \times Z_2$ . One  $Z_2$  is determined

by the factor of  $Z_{16}$  that we already have, but the other one indicates there is one factor of  $Z_8$  in  $H$ . So all other factors of  $H$  are of order 2 or 4.

Since it can be determined by previous methods that  $H$  has rank 4 and

$h = 2^{11}$ , we see that  $H \simeq Z_{16} \times Z_8 \times Z_4 \times Z_4$ .



**Example.** For our final problem let  $d_1 = -388841$ ,  $d_2 = 31897$  and  $d_3 = -6497$ . Here  $H_1 \simeq Z_4 \times Z_4 \times Z_{16}$  (the class group also has an odd factor of order 3),  $H_2 \simeq Z_2 \times Z_4$  and  $H_3 \simeq Z_8 \times Z_8$ . Next note that the *ker* is  $\{(1, 1, 1), (1, 17, 73), (2, 1, 2), (2, 17, 146), (17, 1, 73), (17, 17, 1), (34, 1, 146), (34, 17, 2), (89, 1, 73), (89, 17, 1), (178, 1, 146), (178, 17, 2), (257, 1, 1), (257, 17, 73), (514, 1, 2), (514, 17, 146)\}$ .

The table of consistent characters is

-1	17	89	257	17	73	257	-1	73	89
+	+	+	+	+	+	+	+	+	+
+	+	-	-	+	-	-	+	-	-
+	-	+	-	-	+	-	+	+	+
+	-	-	+	-	-	+	+	-	-
-	+	+	-	+	-	-	-	-	+
-	-	+	+	-	-	+	-	-	+
-	+	-	+	+	+	+	-	+	-
-	-	-	-	-	+	-	-	+	-

Note that again in this case the characters of the real field did not have to be normalized. Finding the ambiguous classes in the principal genus, we see that in  $k_1$  and  $k_3$  all ambiguous classes are in the principal genus. In  $k_2$  the divisors of 17 are in the genus with character values  $- - +$  and the divisors of 257 are principal. Since the norm of the fundamental unit here is  $+1$  and the characters of  $-1$  are all positive, there must be a weak ambiguous class in the principal genus. We find that  $55301^2 + 38841 \cdot 4^2 = 17 \cdot 13629^2$ . The characters for 13629 in  $k_1$  are  $+ - - +$ . Also  $6230^2 + 38841 \cdot 8^2 = 89 \cdot 846^2$ . The characters for 846 in  $k_1$  are  $- + + -$ . Finally,  $11^2 + 38841 = 2 \cdot 21^4$ . Since the divisors of 21 are in the principal genus, we get  $4870^2 + 38841 \cdot 4^2 = 21 \cdot 1194^2$ . The characters for 1194 in  $k_1$  are  $+ + - -$ . Thus (2) is a eighth power of elements in this genus. In  $k_2$  there is a weak ambiguous class that is a square of elements from each of the two genera with character values  $+ - -$  and  $- + -$ . Using the quadratic

representations for  $k_3$  we get:

$$97820^2 + 6497 \cdot 3^2 = 73 \cdot 107^4, 1^2 + 6497 = 2 \cdot 57^2$$

and

$$2219^2 + 6497 \cdot 4^2 = 57 \cdot 297^2.$$

Here 107 and 297 give the character values  $--+$  and  $+--$ . Hence we get the following table

$-17 \cdot 89 \cdot 257$	$2 \cdot 73 \cdot 257$	$-73 \cdot 89$
(1, 1)	(1, $w$ )	(1, 1)
(8, 2)	(2, $w$ )	(4, 2)
(8, 2)	(2, $w$ )	(1, 1)
(2, 17)	(1, $w$ )	(4, 2)
(2, 89)	(2, $w$ )	(4, 73)
(8, 2)	(1, $w$ )	(4, 73)
(8, 2)	(1, $w$ )	(4, 146)
(2, 1513)	(2, $w$ )	(4, 146)

Thus, in this example, we see that  $S^8 \cap \text{amb}$  is given by  $\langle (2, 1, 1) \rangle$  and that  $S^8 \cap \text{ker}$  is  $\langle (1, 1, 1) \rangle$ . Thus  $\frac{S^8 \cap \text{amb}}{S^8 \cap \text{ker}} \simeq Z_2$  and  $\frac{H^{16}}{H^{32}} \simeq Z_2$ . Hence there is a factor of  $Z_{32}$  in  $H$ . Now we see that for the fourth power we have  $S^4 \cap \text{amb} = \langle (2, 1, 1), (1, 1, 2), (1, 1, 73) \rangle$  and  $S^4 \cap \text{ker} = \langle (2, 1, 2) \rangle$ . And so,  $\frac{S^4 \cap \text{amb}}{S^4 \cap \text{ker}} \simeq Z_2 \times Z_2$  making  $\frac{H^8}{H^{16}} \simeq Z_2 \times Z_2$ . One  $Z_2$  is determined by the factor of  $Z_{32}$  that we already have, but the other one indicate there is a factor of  $Z_{16}$  in  $H$ . For the squares there is no change, but Theorem 3 shows  $H$  has a factor of  $Z_8$ . Now all other factors of  $H$  are of order 2 or 4. Since it can be determined by previous methods that  $H$  has rank 6 and  $h = 2^{16}$ , we see that

$$H \simeq Z_{32} \times Z_{16} \times Z_8 \times Z_4 \times Z_2 \times Z_2.$$

In certain cases it may be necessary to determine which genera of the real quadratic field contain the weak ambiguous classes. To do this one needs to know an ideal that is contained in a weak ambiguous class. A simple method for doing this is described in [10, p. 19]. Let  $\Delta$  denote the discriminant of this field and write  $\Delta = 4a^2 + b^2$ . Then the ideal  $I$  with  $Z$  basis  $[a, (b + \sqrt{\Delta})/2]$  generates a weak ambiguous class and has norm  $a$ .

We now state our algorithm:

1. Compute  $\ker$ . The generators of  $\ker$  are of the form  $(l, l, 1)$ ,  $(l, 1, l)$ ,  $(1, l, l)$  and  $(m, 1, 1)$ ,  $(1, 1, m)$ , where  $l$  is a common prime divisor of the discriminants of the two quadratic fields with subscripts corresponding to the position of the  $l$ 's. The terms involving  $m$  (not necessarily prime) are defined similarly, but it is a principal divisor of  $k_2$ . Set  $H = (1)$ .

2. Make a table of the consistent characters for  $K$ . This will be referred to as the genus table for  $K$ . In our examples we made a separate  $(a, b)$  table corresponding to the genus table. Here it will be easier to describe if we instead think of this as a labeling of the genus table. Label the principal genus of each field as  $(1, 1)$ .

3. For each of the three quadratic subfields, determine in which genus each ambiguous class is contained. For the real quadratic this may include weak ambiguous classes denoted by  $w$ . Label the corresponding entry in the genus table as  $(1, 1)$ .

4. If none of the  $H_i$ 's has more than one cyclic factor of order greater than 2, label the remaining entries (if any) for the field  $k_i$  as  $(2^j, p)$ , where the largest cyclic factor of  $H_i$  has order  $2^{j+1}$  and  $p$  is in the nonprincipal ambiguous class that is the principal genus. If this is a weak ambiguous class set  $p = w$ . Let  $2^j$  be the maximum first coordinate of any entry in the table. Go to step 8. Otherwise set  $j = 1$ .

5. For each  $H_i$  with two or more cyclic factors of order greater than 2, determine a basis for the ambiguous classes that are in the principal

genus. Here, if necessary, a weak ambiguous class will be denoted by  $c$ , where  $c$  is the norm of the ideal described above. The other weak classes by  $p \cdot c$ , where a divisor of  $p$  is a strong ambiguous class in the principal genus. For each such ambiguous class let  $m$  denote the norm of an ideal in this class. Solve the equation  $x^2 \pm d_i \cdot y^2 = \pm m \cdot z^2$ , where the first sign is negative exactly when  $i = 2$  and the second sign is always positive when  $i = 1$  or  $i = 3$ . A method of Lagrange as explained by Hasse in [6] can be used for this purpose.

6. Determine the generic characters for each  $z$ . If this is not all  $+1$ 's label the corresponding genus of the quadratic subfield as  $(2^j, m)$ , where  $m$  appears in the equation giving  $z$  or  $m = m_0$  when  $j > 1$ . If a product of some  $z$ 's for a particular field belongs to the principal genus, let  $z_0$  denote the product of these  $z$ 's and  $m_0$  denote the product of the corresponding  $m$ 's solve the equation  $x^2 \pm d_i \cdot y^2 = \pm z_0 \cdot z^2$ . Do this for all such products and all three fields. Increase  $j$  by 1.

7. Repeat step 6 until no product of  $z$ 's are in the principal genus for any of the three quadratic subfields. There may still be unlabeled genera. In this case there should be labeled genera whose product is this genus. Let  $2^j$  denote the maximum of the first coordinates in this product and  $m$  the product of the second coordinates of all terms where this maximum value of the first coordinate occurs with square factors deleted. Label the genus as  $(2^j, m)$ . A short cut is possible when an  $H_i$  has a unique cyclic factor of maximum order  $2^s$ . When half of the genera of  $k_i$  have been labeled, the other half can be labeled as  $(2^{(s-1)}, b)$ , where  $b$  has a divisor that is ambiguous and does not correspond to a genera containing classes of smaller order. This can substantially reduce the number of quadratic equations that must be solved. When all ramified primes divide the discriminant of one of the quadratic subfields  $k_i$  and 2 is not totally ramified only half of the genera for  $k_i$  occur in  $\hat{S}$ . If a genus for  $k_i$  that would normally be labeled  $(2^j, m)$  with  $j \geq 2$  does not occur in  $\hat{S}$ , then

the principal genus of  $k_i$  needs to be labeled as  $(2^{j-1}, m)$ . Set  $2^J$  equal to the maximum of all the first coordinates of all labels in the genus table.

8. Use the genus table to compute  $S^{2^J} \cap amb$  and  $S^{2^J} \cap ker$ . Let the quotient of the groups have order  $2^{f_1}$ . Then  $\frac{H^{2^{J+1}}}{H^{J+2}}$  has  $f_1 + f_2$  cyclic factors of  $Z_2$ , where  $2^{f_2}$  is the order of  $S^{2^{J+1}} \cap ker$ . Let  $f_3$  denote the number of cyclic factors already in  $H$  (Initially both  $f_2$  and  $f_3$  will be 0). Then  $f_1 + f_2 - f_3$  will be the number of cyclic factors of order  $2^{J+2}$  that are now added to  $H$ . Decrease  $J$  by 1.

9. While  $J > 0$  repeat step 8.

10. Compute the rank and order of  $H$ . The remaining factors all have order 4 or 2 and the number of each is now easily determined.

We would like to close this section with two examples with much larger class groups that have been done both by hand and by computer. If  $d_1 = -6411481$ ,  $d_2 = 14722$ ,  $d_3 = -94389823282$ , then

$$H_1 \simeq Z_4 \times Z_{512},$$

$$H_2 \simeq Z_4 \times Z_4,$$

$$H_3 \simeq Z_2 \times Z_2 \times Z_4 \times Z_{64}$$

and

$$H \simeq Z_{512} \times Z_{128} \times Z_8 \times Z_8 \times Z_2 \times Z_2.$$

If

$$d_1 = -5776272669249131925508687$$

$$= -179424673 \cdot 17942911 \cdot 179424929,$$

$$d_2 = 14722,$$

$$d_3 = -85038286236685720207338890014,$$

then

$$H_1 \simeq Z_4 \times Z_{256},$$

$$H_2 \simeq Z_4 \times Z_4,$$

$$H_3 \simeq Z_2 \times Z_2 \times Z_2 \times Z_4 \times Z_{16}$$

and

$$H \simeq Z_{512} \times Z_{32} \times Z_8 \times Z_8 \times Z_2 \times Z_2.$$

### 5. Fields With Class Numbers 8 and 16

Complete lists of all imaginary, bicyclic, biquadratic fields of class numbers 1 and 2 have already been given in [2] and [5]. Moreover, in our recent article [9] we gave an essentially complete list of all such fields with class number 4 and determined the structure of the 2-class group of each field. Here, we give an essentially complete list of all such fields with class numbers 8 and 16 as well as determine the structure of the 2-class group of each field. In order to determine all such fields of class number  $2^n$ , we use the well-known class number formula

$$h = \frac{q_0}{2} h_1 h_2 h_3,$$

where  $q_0 = 1$  or  $2$  is a unit index. Hence if  $h = 2^n$ , then  $h_1 \leq 2^{n+1}$ . To accomplish our goal here we need complete lists of all imaginary quadratic fields of class number  $2^n$  for  $n \leq 5$ . Stark [12, 13] has given such lists for  $n = 0$  and  $1$  and Arno [1] a list for  $n = 2$ . While complete lists of imaginary quadratic fields of class numbers 8, 16 and 32 are unknown, Buell [3, 4] has computed the class number of all such fields with discriminant greater than 2.2 million. Moreover, Hoffstein's [7] bounds on the  $L$ -series show that there is at most one more imaginary quadratic field of class numbers 8, 16 or 32 with discriminant less than 2.2 million. Therefore, Buell's lists are essentially complete.

When  $h = 8$ , the rank of the 2-class group determines its structure. But when  $h = 16$  there are two possible structures of rank 2. Here we

apply the methods of this article to distinguish between the two possibilities. The structure of the class group of the quadratic subfields was usually obtained from Oriat's [11] tables. A summary of these results appear in the following table.

structure	no.	least conductor	greatest conductor
$Z_2 \times Z_2 \times Z_2$	132	168, 21, 2, 42	233905, 163, 233905, 1435
$Z_2 \times Z_4$	469	120, 6, 15, 10	297005, 955, 59401, 1555
$Z_8$	585	195, 15, 65, 39	930241, 163, 930241, 5707
$Z_2 \times Z_2 \times Z_2 \times Z_2$	26	1320, 2, 330, 165	18204, 37, 4551, 123
$Z_2 \times Z_2 \times Z_4$	423	552, 46, 3, 138	626665, 403, 626665, 1555
$Z_4 \times Z_4$	281	420, 5, 105, 21	602497, 427, 602497, 1411
$Z_2 \times Z_8$	1152	264, 33, 2, 66	1304645, 1555, 260929, 4195
$Z_{16}$	719	555, 555, 5, 111	3844681, 163, 3844681, 23587

Since there are only 26 fields with class number 16 and class group of rank 4, the complete table is given below.

Fields where  $H \simeq Z_2 \times Z_2 \times Z_2 \times Z_2$

$f$	$-d_1$	$d_2$	$-d_3$	$f$	$-d_1$	$d_2$	$-d_3$
1320	2	330	165	5187	3	1729	5187
1848	42	11	462	5208	6	217	1302
1848	21	22	462	5304	13	1326	102
1848	2	231	462	6105	11	6105	555

2652	13	663	51	6460	19	1615	85
2760	30	46	345	7315	19	385	7315
2856	2	714	357	7755	11	705	7755
3080	70	22	385	8835	15	589	8835
3795	11	345	3795	8932	7	319	2233
4420	13	1105	85	11305	19	11305	595
4488	2	561	1122	11715	11	1065	11715
5016	2	1254	627	14763	3	4921	14763
5115	11	465	5115	18204	37	4551	123

### References

- [1] S. Arno, The imaginary quadratic fields of class number 4, *Acta Arith.* 60(4) (1992), 321-334.
- [2] E. Brown and C. J. Parry, The imaginary bicyclic biquadratic fields with class number 1, *Reine Angew. Math.* 266 (1974), 118-120.
- [3] D. A. Buell, Small class numbers and extreme values of  $L$ -functions of quadratic fields, *Math. Comp.* 31 (1977), 786-796.
- [4] D. A. Buell, The last exhaustive computation of class groups of complex quadratic number fields. *Number theory* (Ottawa, ON, 1996), 35-53, CRM Proc. Lecture Notes, 19, Amer. Math. Soc., Providence, RI, 1999.
- [5] D. A. Buell, H. C. Williams and K. S. Williams, On the imaginary bicyclic biquadratic fields with class number 2, *Math. Comp.* 31 (1977), 1034-1042.
- [6] H. Hasse, An algorithm for determining the structure of the 2-Sylow subgroup of the divisor group of a quadratic number field, *Symposia Mathematica* 15 (1975), 341-352.
- [7] J. Hoffstein, On the Siegel-Tatuzawa theorem, *Acta Arith.* 38(2) (1980-81), 167-174.
- [8] T. Kubota, Über den bizyklischen biquadratischen Zahlkörper, *Nagoya Math. J.* 10 (1956), 65-85.
- [9] T. M. McCall, C. J. Parry and R. R. Ranalli, The 2-rank of the class group of imaginary bicyclic biquadratic fields, *Can. J. Math.* 49(2) (1997), 283-300.



- [10] R. A. Mollin, *Quadratics*, CRC Press, 1996.
- [11] B. Oriat, Groupes des classes d'idéaux des quadratiques imaginaires  $Q(d^{1/2})$ ,  $-24572 < d < 0$ , *Theorie des nombres*, Années, 1986/87-1987/88, Fasc. 2, pp. 63, Publ. Math. Fac. Sci. Besancon, Univ., Franhe-Compté, Besancon, 1988.
- [12] H. M. Stark, A complete determination of the complex quadratic fields of class number one, *Michigan Math. J.* 14 (1967), 1-27.
- [13] H. M. Stark, On complex quadratic fields with class number two, *Math. Comp.* 29 (1975), 289-302.