

5415  
110

# Problems Involving Relative Integral Bases For Quartic Number Fields

by

JOHN A. HYMO

Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY  
in  
Mathematics

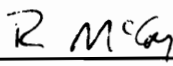
APPROVED:

  
C. J. Parry, Chairman

  
E. Brown

  
J. Rossi

  
R. Snider

  
R. McCoy

May, 1990  
Blacksburg, Virginia

# Problems Involving Relative Integral Bases For Quartic Number Fields

by

JOHN A. HYMO

Committee Chairman: Charles J. Parry

## (ABSTRACT)

In this dissertation the question of whether or not a relative extension of number fields has a relative integral basis is considered. In Chapters 2 and 3 we use a criteria of Mann to determine when a cyclic quartic field or a pure quartic field has an integral basis over its quadratic subfield. In the final chapter we study the question: if the relative discriminant of an extension  $K/k$  is principal, where  $[K : k] = l$  such that  $l$  is an odd prime and  $k$  is either a quadratic or a normal quartic number field, does  $K/k$  have an integral basis?

## DEDICATION

This work is dedicated to my parents — Lawrence and Keren Hymo.

## ACKNOWLEDGEMENTS

I am grateful to my advisor Charles Parry for his direction and support. The time and effort he has given me is greatly appreciated.

## TABLE OF CONTENTS

Abstract . . . . .	ii
Dedication . . . . .	iii
Acknowledgements . . . . .	iv
Chapter 1: Introduction . . . . .	1
Chapter 2: Relative integral bases for cyclic quartic fields . . . . .	2
Chapter 3: Relative integral bases for pure quartic fields . . . . .	10
Chapter 4: Steinitz classes of order 2 in quadratic and quartic fields . . . . .	27
References . . . . .	51
Vita . . . . .	53

## Introduction

The fundamental question considered in this dissertation is whether or not a relative extension of number fields has a relative integral basis. A number field is a finite extension of the rational number field  $Q$ . An algebraic integer is a root of a monic polynomial with coefficients in  $\mathbb{Z}$ . The set of all algebraic integers in a number field  $K$  forms a ring and is called the ring of algebraic integers of  $K$ . If  $K/k$  is an extension of number fields and  $R$  and  $S$  denote the rings of algebraic integers of  $K$  and  $k$  respectively, then an  $R$ -basis for  $S$  is called a *relative integral basis* for  $K$  over  $k$ . If  $k = Q$ , or more generally, if  $k$  has class number 1, then the extension  $K/k$  has an integral basis.

When  $K/k$  is a relative quadratic extension; i.e.  $[K/k] = 2$ , Mann [ ] has given a general criteria for a relative integral basis to exist. In Chapters 2 and 3 Mann's criteria is applied to obtain explicit results when  $K$  is either a cyclic quartic field or a pure quartic field. Moreover, a relative integral basis is determined whenever it exists.

If an extension  $K/k$  has a relative integral basis then the relative discriminant of  $K/k$  is principal. (See [21] for a definition of the relative discriminant.) However, this condition is not in general sufficient. Thus the question arises as to when this condition is sufficient. In the final chapter this question is studied when  $K/k$  is a normal extension of odd prime degree,  $l$ , and  $k$  is either a quadratic or a normal quartic number field. Pierce [20] had considered this problem for  $l \equiv 3 \pmod{4}$  only.

## Chapter II: ON RELATIVE INTEGRAL BASES FOR CYCLIC QUARTIC FIELDS

### §1. Introduction.

A necessary and sufficient condition is given for a cyclic quartic field to have an integral basis over its quadratic subfield. An explicit integral basis is given for this relative extension whenever it exists. For a fixed quadratic field  $k$ , it is shown that  $1/2^g$  of all cyclic quartic fields which contain  $k$  have a relative integral basis. Here  $g$  denotes the 2-rank of the ideal class group of  $k$ .

In [7], Edgar and Peterson give a criteria for a cyclic quartic field to have a relative integral basis over its quadratic subfield. However, their criteria is not explicit and they give no bases.

We use the description of cyclic quartic fields given in [10]. A criterion of Mann [17] is used to determine when the extension has an integral basis. In [3], Bird and Parry have obtained similar results for bicyclic biquadratic fields over their quadratic subfields.

### §2. Notation.

$L/M$ : An extension of number fields.

$\Delta_{L/M}$ : Discriminant of  $L/M$ .

$K$ : A cyclic quartic extension of  $Q$ .

$k = Q(\sqrt{D})$ : Quadratic subfield of  $K$ .

$\epsilon_0 = r + t\sqrt{D}$ : Fundamental unit of  $k$ .

$$\delta = \begin{cases} 0 & \text{if } r, t \in Z. \\ 2 & \text{if } r, t \notin Z. \end{cases}$$

In [10], it is shown that  $K = Q(\sqrt{A(D + B\sqrt{D})})$  where  $A$  is square free and odd,  $B > 0$  and  $C > 0$  with  $D = B^2 + C^2$  square free and  $A, B, C \in Z$ . Moreover,  $(A, D) = 1$ .

### §3. Existence of an integral basis.

We first determine the relative discriminant of  $K/k$ .

LEMMA 1. *The relative discriminant of  $K/k$  is given by  $\Delta_{K/k} = (\Delta)$  where*

$$\Delta = \begin{cases} 4A\sqrt{D} & \text{if } D \equiv 0 \pmod{2} \text{ or } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 3 \pmod{4} \\ A\sqrt{D} & \text{if } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 1 \pmod{4} \\ 8A\sqrt{D} & \text{if } D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}. \end{cases}$$

PROOF: By [3]

$$\Delta_{K/Q} = \begin{cases} 2^8 A^2 D^3 & \text{if } D \equiv 0 \pmod{2} \\ 2^4 A^2 D^3 & \text{if } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 3 \pmod{4} \\ A^2 D^3 & \text{if } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 1 \pmod{4} \\ 2^6 A^2 D^3 & \text{if } D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}. \end{cases}$$

Since

$$\Delta_{k/Q} = \begin{cases} D & \text{if } D \equiv 1 \pmod{4} \\ 4D & \text{if } D \not\equiv 1 \pmod{4} \end{cases}$$

and

$$\Delta_{K/Q} = N_{k/Q}(\Delta_{K/k})\Delta_{k/Q}^2 = \Delta_{K/k}^2 \Delta_{k/Q}^2,$$

the lemma follows.

LEMMA 2.  *$K/k$  has an integral basis if and only if  $K = k(\sqrt{A'\epsilon\sqrt{D}})$  where*

$$A' = \begin{cases} 2A & \text{if } D \equiv 1 \pmod{4} \text{ and } B \equiv 1 \pmod{2} \\ A & \text{otherwise} \end{cases}$$

and  $\epsilon$  is a unit of  $k$  with norm  $-1$ . In fact, we may choose  $\epsilon = \epsilon_0$ .

PROOF: Mann [17] shows that  $K/k$  has an integral basis if and only if  $K = k(\sqrt{\Delta})$  for some generator  $\Delta$  of  $\Delta_{K/k}$ . By Lemma 1, this is equivalent to  $K = k(\sqrt{A'\epsilon\sqrt{D}}) = k(\sqrt{2^a A\epsilon\sqrt{D}})$  for some unit  $\epsilon$  of  $k$ , where  $a = 1$  when  $B$  and  $D$  are both odd and  $a = 0$  otherwise.

But  $K = k(\sqrt{A(D + B\sqrt{D})}) = k(\sqrt{2^a A\epsilon\sqrt{D}})$  if and only if  $A(D + B\sqrt{D}) = 2^a A\epsilon\sqrt{D}s^2$  for some  $s \in k$ . Equivalently,  $B + \sqrt{D} = 2^a \epsilon s^2$ . Taking norms gives  $-C^2 = B^2 - D = (2^a)^2 N_{k/Q}(\epsilon)(s\bar{s})^2$ , so  $\epsilon$  has norm  $-1$ .



Since  $k(\sqrt{A(D + B\sqrt{D})}) = k(\sqrt{2^a A \epsilon \sqrt{D}})$ ,  $\epsilon > 0$ , so  $\epsilon = \epsilon_0^i$  for some integer  $i$ . Since  $\epsilon$  has norm  $-1$ ,  $i$  must be odd so  $k(\sqrt{2^a A \epsilon \sqrt{D}}) = k(\sqrt{2^a A \epsilon_0 \sqrt{D}})$ .

For the remainder of the article, we will assume, unless otherwise stated that  $N(\epsilon_0) = -1$ . Recall that  $\epsilon_0 = r + t\sqrt{D}$  and  $2^{\delta/2}r, 2^{\delta/2}t$  are integers with  $\delta = 0$  or  $2$ .

**LEMMA 3.** *If  $2^{\delta/2}(r + i) = (u + vi)^2(X + Yi)$  in  $Z[i]$  with  $X + Yi$  square free and  $X > 0$  then*

$$k(\sqrt{\epsilon_0 \sqrt{D}}) = \begin{cases} k(\sqrt{D + X\sqrt{D}}) & \text{if } \delta = 0 \\ k(\sqrt{D + |Y|\sqrt{D}}) & \text{if } \delta = 2. \end{cases}$$

Moreover, when  $D \equiv 1 \pmod{4}$ ,  $X \equiv \delta/2 \pmod{2}$  and  $Y \equiv \delta/2 + 1 \pmod{2}$ .

**PROOF:** Note that  $k(\sqrt{\epsilon_0 \sqrt{D}}) = k(\sqrt{tD + r\sqrt{D}}) = k(\sqrt{2^{\delta}t(2^{\delta/2}tD + 2^{\delta/2}r\sqrt{2^{\delta/2}tD})}) = k(\sqrt{A_1(D_1 + B_1\sqrt{D_1})})$  where  $A_1 = 2^{\delta}t, B_1 = 2^{\delta/2}r$  and  $D_1 = 2^{\delta}t^2D$ . Also,  $D_1 - B_1^2 = 2^{\delta}t^2D - 2^{\delta}r^2 = 2^{\delta} = C_1^2$  where  $C_1 = 2^{\delta/2}$ . Since  $B_1 + C_1i = 2^{\delta/2}(r + i) = (u + vi)^2(X + Yi)$ , it follows that  $2^{\delta}t^2D = D_1 = B_1^2 + C_1^2 = (u^2 + v^2)^2(X^2 + Y^2)$ . Since  $X + Yi$  is square free and has no rational factor (because  $2^{\delta/2}(r + i)$  has none), it follows that  $X^2 + Y^2$  is also square free. Thus  $2^{\delta/2}t = u^2 + v^2$  and  $X^2 + Y^2 = D$ . Moreover,  $B_1 = X(u^2 - v^2) - Y(2uv), C_1 = X(2uv) + Y(u^2 - v^2)$  and  $D_1 = (u^2 + v^2)^2D$ . It follows from [10, p. 5-6] that

$$\begin{aligned} k(\sqrt{\epsilon_0 \sqrt{D}}) &= k(\sqrt{A_1(D_1 + B_1\sqrt{D_1})}) = k(\sqrt{A_1(u^2 + v^2)(D + X\sqrt{D})}) \\ &= k(\sqrt{2^{\delta}t^22^{\delta/2}(D + X\sqrt{D})}) = k(\sqrt{2^{\delta/2}(D + X\sqrt{D})}) \\ &= \begin{cases} k(\sqrt{D + X\sqrt{D}}) & \text{if } \delta = 0 \\ k(\sqrt{D + |Y|\sqrt{D}}) & \text{if } \delta = 2. \end{cases} \end{aligned}$$

If  $D$  is odd, then  $-2^{\delta} = N(2^{\delta/2} \cdot \epsilon_0) = (2^{\delta/2}r)^2 - (2^{\delta/2}t)^2D$ . Thus  $2^{\delta/2}t = u^2 + v^2$  is odd, and hence  $u^2 - v^2$  is also odd. Since  $2^{\delta/2} = C_1 = X(2uv) + Y(u^2 - v^2)$ , we see that  $Y \equiv 2^{\delta/2} \equiv \delta/2 + 1 \pmod{2}$ . Thus  $X \equiv X^2 \equiv D - Y^2 \equiv 1 - Y \equiv \delta/2 \pmod{2}$ .

**THEOREM 1.** *If  $D$  is odd then  $K/k$  has an integral basis if and only if  $B \pm Ci$  divides  $2^{\delta/2}(r + i)$  in  $Z[i]$ . If  $D$  is even then  $K/k$  has an integral basis if and only if  $r + i = (u + vi)^2(B \pm Ci)$  for some  $u, v \in Z$ .*

PROOF: As in Lemma 3, write  $2^{\delta/2}(r+i) = (u+vi)^2(X+Yi)$ , where  $X > 0$ . Let  $Z = X$  or  $|Y|$  according as  $\delta = 0$  or  $\delta = 2$  and set  $Z' = \sqrt{D - Z^2}$ .

If  $K/k$  has an integral basis then Lemmas 2 and 3 show that

$$K = k(\sqrt{A(D + B\sqrt{D})}) = k(\sqrt{A'\epsilon_0\sqrt{D}}) = k(\sqrt{A'(D + Z\sqrt{D})}).$$

Unless both  $B$  and  $D$  are odd, Lemma 2 shows that  $A' = A$ . Theorem 1 of [10] shows that  $B + Ci = i^{\delta/2}(X \pm Yi)$ . Moreover, when  $D$  is even,  $\delta = 0$ , so  $B + Ci = X \pm Yi$ . If  $D$  and  $B$  are both odd then  $A' = 2A$ . It follows from Lemmas 2 and 3 and Theorem 2 of [10] that

$$k(\sqrt{A(D + B\sqrt{D})}) = K = k(\sqrt{2A(D + Z\sqrt{D})}) = k(\sqrt{A(D + Z'\sqrt{D})}).$$

Thus  $B + Ci = (i)^{1-\delta/2}(X \pm Yi)$ .

Conversely, assume  $D$  is odd and  $B \pm Ci$  divides  $2^{\delta/2}(r+i)$ , so  $2^{\delta/2}(r+i) = (x+yi)(B \pm Ci)$  for some  $x, y \in Z$ . Taking norms, we obtain  $2^{\delta}t^2D = 2^{\delta}(r^2+1) = (x^2+y^2)(B^2+C^2) = (x^2+y^2)D$  so  $x^2+y^2 = (2^{\delta/2}t)^2$ . Since  $2^{\delta/2}(r+i)$  is not divisible by a rational prime, neither is  $x+yi$ . Because its norm is a square,  $x+yi = i^b(w+zi)^2$  with  $b = 0$  or  $1$  and  $w, z \in Z$ . Thus

$$2^{\delta/2}(r+i) = i^b(w+zi)^2(B \pm Ci) = \begin{cases} (w+zi)^2(B \pm Ci) & \text{if } b = 0 \\ (w+zi)^2(\pm C + Bi) & \text{if } b = 1. \end{cases}$$

Hence

$$2^{\delta/2}(r+i) \equiv \begin{cases} B + Ci \pmod{2} & \text{when } b = 0 \\ C + Bi \pmod{2} & \text{when } b = 1. \end{cases}$$

Also, when  $\delta = 2$ , note that  $2^{\delta/2}(r+i) \equiv 1 \pmod{2}$ . If  $\delta/2 \not\equiv b \pmod{2}$  then  $B \equiv 1 \pmod{2}$ , so by Lemmas 1 and 3 and Theorem 2 of [10],

$$k(\sqrt{\Delta\epsilon_0}) = k(\sqrt{2A\epsilon_0\sqrt{D}}) = k(\sqrt{2A(D + C\sqrt{D})}) = k(\sqrt{A(D + B\sqrt{D})}) = K.$$

When  $\delta/2 \equiv b \pmod{2}$ ,  $B \equiv 0 \pmod{2}$ , so  $k(\sqrt{\Delta\epsilon_0}) = k(\sqrt{A\epsilon_0\sqrt{D}}) = k(\sqrt{A(D + B\sqrt{D})}) = K$ . Thus Lemma 2 applies to show  $K/k$  has an integral basis.

Finally, if  $D$  is even and  $r+i = (u+vi)^2(B \pm Ci)$  then by Lemmas 1 and 3,  $k(\sqrt{\Delta\epsilon_0}) = k(\sqrt{A\epsilon_0\sqrt{D}}) = k(\sqrt{A(D + B\sqrt{D})}) = K$ . Thus Lemma 2 again applies.

#### §4. An Integral Basis.

In this section an explicit integral basis is given for  $K/k$  whenever it exists. Let  $s = \frac{1}{2}(2r + 1)$ .

**THEOREM 2.** *If  $D$  is odd and  $K = k(\sqrt{2A\epsilon_0\sqrt{D}})$  then  $1, \sqrt{2A\epsilon_0\sqrt{D}}$  is an integral basis for  $K/k$ . If  $K = k(\sqrt{A\epsilon_0\sqrt{D}})$  then an integral basis for  $K/k$  is given by*

- i)  $1, \frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}$  if  $D \equiv 1 \pmod{4}$ ,  $A \equiv 3 \pmod{4}$  and  $\delta = 2$
- ii)  $1, \frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}$  if  $D \equiv A + r \equiv 1 \pmod{4}$  and  $\delta = 0$
- iii)  $1, \sqrt{A\epsilon_0\sqrt{D}}$  otherwise.

**PROOF:** First assume that  $D$  is odd and  $K = k(\sqrt{2A\epsilon_0\sqrt{D}}) = k(\sqrt{2A(D + Z\sqrt{D})})$  where by Lemma 3,  $Z = X$  or  $|Y|$  according as  $\delta = 0$  or  $\delta = 2$ . By Theorem 2 of [10]  $K = k(\sqrt{A(D + Z'\sqrt{D})})$  where  $Z' = \sqrt{D - Z^2}$ . By Lemma 3,  $Z$  is even so  $Z'$  is odd. Hence, by Lemma 1,  $\Delta_{K/k} = (8A\sqrt{D})$ . Since the field basis  $1, \sqrt{2A\epsilon_0\sqrt{D}}$  has discriminant  $8A\epsilon_0\sqrt{D}$ , it is an integral basis for  $K/k$ .

For the remainder of this proof, we have  $K = k(\sqrt{A\epsilon_0\sqrt{D}})$ . In cases (i) and (ii), it is sufficient to show that the second element of the basis is an integer. In (i) this is equivalent to showing

$$\frac{1 + (-1)^s\sqrt{D}}{2} \equiv \sqrt{A\epsilon_0\sqrt{D}} \pmod{2}$$

or

$$\left( \frac{1 + (-1)^s\sqrt{D}}{2} \right)^2 \equiv A\epsilon_0\sqrt{D} \pmod{4}.$$

The last congruence can be restated in the form

$$\frac{1}{2} \left( \frac{1+D}{2} + (-1)^s\sqrt{D} \right) \equiv A(r + t\sqrt{D})\sqrt{D} \equiv \frac{A(2t)D + A(2r)\sqrt{D}}{2} \pmod{4}.$$

This can be proved by showing  $\frac{1+D}{2} \equiv A(2t)D \pmod{4}$ ,  $(-1)^s \equiv A(2r) \pmod{4}$ , and  $\frac{1+D}{2} - (-1)^s \equiv A(2t)D - A(2r) \pmod{8}$ . First note that since  $2r$  and  $2t$  are odd integers  $-4 = N(2\epsilon_0) = (2r)^2 - (2t)^2D \equiv 1 - D \pmod{8}$ , so  $D \equiv 5 \pmod{8}$ . Also, from the proof

of Lemma 3,  $2t$  is the sum of two squares, so  $2t \equiv 1 \pmod{4}$ . Therefore,

$$A(2t)D \equiv A \equiv 3 \equiv \frac{1+D}{2} \pmod{4}.$$

Also, since  $s = \frac{1}{2}(2r+1)$ ,  $(-1)^s \equiv -2r \equiv A(2r) \pmod{4}$ .

The congruence values of  $D \pmod{16}$  will be used to prove the final condition. If  $D \equiv 5 \pmod{16}$  then  $-4 = (2r)^2 - D(2t)^2 \equiv (2r)^2 - 5(2t)^2 \pmod{16}$ . Since  $2r$  and  $2t$  are odd, their squares are 1 or 9  $\pmod{16}$ . It follows that  $(2r)^2 \equiv (2t)^2 \pmod{16}$  and  $2r \equiv \pm 2t \pmod{8}$ . Hence,

$$A(2t)D - A(2r) \equiv A(10t - 2r) \equiv \begin{cases} 4 \pmod{8} & \text{if } 2r \equiv 2t \pmod{8} \\ 2 \pmod{8} & \text{if } 2r \equiv -2t \pmod{8}. \end{cases}$$

But  $\frac{1+D}{2} - (-1)^s \equiv 3 - (-1)^s \pmod{8}$  has the same value.

Similarly, when  $D \equiv 13 \pmod{16}$ ,  $-4 \equiv (2r)^2 - (2t)^2 D \equiv (2r)^2 + 3(2t)^2 \pmod{16}$ , so that  $(2r)^2 \equiv (2t)^2 + 8 \pmod{16}$ . Hence  $2t \pm 2r = 4z$  for some odd integer  $z$ . Thus

$$A(2t)D - A(2r) \equiv (10t - 2r)A \equiv \begin{cases} (8t + 4z)A \equiv 0 \pmod{8} & \text{if } 2r \equiv 2t \pmod{4} \\ (12t - 4z)A \equiv 6 \pmod{8} & \text{if } 2r \equiv -2t \pmod{4}. \end{cases}$$

Also,

$$\frac{1+D}{2} - (-1)^s \equiv 7 - (-1)^s \equiv \begin{cases} 0 \pmod{8} & \text{if } 2r \equiv 2t \pmod{4} \\ 6 \pmod{8} & \text{if } 2r \equiv -2t \pmod{4}. \end{cases}$$

In (ii), we first note that  $-1 = -r^2 - t^2 D$  implies  $r$  is even and  $t$  is odd. Since  $t$  is the sum of two squares,  $t \equiv D \equiv 1 \pmod{4}$ . Thus  $A\epsilon_0\sqrt{D} = AtD + Ar\sqrt{D} \equiv A + r \equiv 1 \pmod{4}$ , so  $\sqrt{A\epsilon_0\sqrt{D}} \equiv 1 \pmod{2}$  and hence  $\frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}$  is an integer. In (iii) we only need to show that  $\Delta_{K/k} = (4A\sqrt{D})$ . First, assume  $D$  is odd,  $A + r \equiv 3 \pmod{4}$  and  $r, t \in Z$ . From the proof of Lemma 3,  $r = (u^2 - v^2)X - 2uvY$  with  $r, X$  and exactly one of  $u$  or  $v$  even, so  $r \equiv X \pmod{4}$ . Thus,  $A + X \equiv A + r \equiv 3 \pmod{4}$ , so Lemmas 3 and 1 show  $\Delta_{K/k} = (4A\sqrt{D})$ . When  $D$  is odd with  $A \equiv 1 \pmod{4}$  and  $r, t \notin Z$  then  $Y$  is even by Lemma 3. Since  $-4 = (2r)^2 - (2t)^2 D = (2r)^2 - (2t)^2(X^2 + Y^2) \equiv 1 - (Y^2 + 1) \equiv -Y^2 \pmod{8}$ , we have  $Y \equiv 2 \pmod{4}$ . Thus  $A + |Y| \equiv 3 \pmod{4}$ , so Lemmas 3 and 1 again show  $\Delta_{K/k} = (4A\sqrt{D})$ .

When  $D$  is even, Lemma 1 shows that  $\Delta_{K/k} = (4A\sqrt{D})$ .

### §5. Class Number Considerations.

In this section a connection is established between the existence of an integral basis for  $K/k$  and the class number of  $k$ . In Theorem 3, a new proof of Theorem 1 of [7] is given, while Theorem 4 strengthens the results of Theorem 2 of [7].

**THEOREM 3.** *If  $k$  has odd class number then  $K/k$  always has an integral basis.*

**PROOF:** If  $h(k)$  is odd then  $D = 2$  or  $D = p \equiv 1 \pmod{4}$  with  $p$  prime. Thus  $N(\epsilon_0) = -1$  and  $D$  can be expressed as a sum of two squares in a unique way. When  $D = 2, B = 1$  and  $\epsilon_0 = 1 + \sqrt{2}$ , so  $k(\sqrt{A\epsilon_0\sqrt{2}}) = k(\sqrt{A(2 + \sqrt{2})}) = K$ . Hence by Lemma 2,  $K/k$  has an integral basis.

Assume now  $D = p = B^2 + C^2$ . Since  $X^2 + Y^2 = D$ , and the representation of  $D$  as a sum of two squares is unique,  $B \pm Ci$  and  $X + Yi$  are associates. It follows from Lemma 3 and Theorem 1 that  $K/k$  has an integral basis.

**THEOREM 4.** *Assume  $h(k)$  is even and that  $D = p_1 \dots p_n (n \geq 2)$  with  $p_1, \dots, p_n$  distinct primes,  $p_i \equiv 1$  or  $2 \pmod{4}$ . If  $N(\epsilon_0) = +1$  then  $K/k$  never has an integral basis. If  $N(\epsilon_0) = -1$  then the ratio  $\rho$  of cyclic quartic extensions  $K/Q$  such that  $K/k$  has an integral basis to all cyclic quartic extensions  $K/Q$  which contain  $k$  is  $\frac{1}{2^{n-1}} = \frac{1}{2^g}$  where  $g$  is the 2-rank of the ideal class group of  $k$ .*

**PROOF:** If  $N(\epsilon_0) = +1$  then Lemma 2 shows  $K/k$  never has an integral basis.

Assume next that  $N(\epsilon_0) = -1$  and  $D$  is odd. Then  $D = B^2 + C^2$ , with  $B \neq C$ , can be expressed as the sum of two squares in  $2^{n-1}$  ways, so there are  $2^n$  distinct fields of the form  $k(\sqrt{A(D + B\sqrt{D})})$  for any fixed odd integer  $A$ . If  $X + Yi$  is determined as in Lemma 3, then by Theorem 1, only  $k(\sqrt{A(D + X\sqrt{D})})$  and  $k(\sqrt{A(D + |Y|\sqrt{D})})$  have integral basis over  $k$ . Thus  $\rho = \frac{2}{2^n} = \frac{1}{2^{n-1}}$ . Since  $N(\epsilon_0) = -1, n - 1 = g$  is the 2-rank of the ideal class group of  $k$  (see Satz 106 and 107 of [12].)

Assume now that  $N(\epsilon_0) = -1$  and  $D$  is even. Since  $h(k)$  is even,  $D \neq 2$ . Here

$D = B^2 + C^2$ , with  $B \neq C$ , can be expressed as the sum of two squares in  $2^{n-2}$  ways. Hence for any fixed odd integer  $A$ , there are  $2^{n-1}$  fields of the form  $k(\sqrt{A(D + B\sqrt{D})})$ . By Theorem 1, there is only one field  $K$  such that  $K/k$  has an integral basis. Thus  $\rho = \frac{1}{2^{n-1}}$  and as above  $g = n - 1$ .

### §6. Examples.

1.  $D = 1105 = 5 \cdot 13 \cdot 17$      $\epsilon_0 = 28488 + 857\sqrt{1105}$      $r + i = 28488 + i = (29 - 4i)^2(32 + 9i)$ .

By Theorem 1  $K = k(\sqrt{A(1105 + B\sqrt{1105})})$  has an integral basis over  $k$  for  $B = 9$  and 32, but does not have a basis for  $B = 4, 12, 23, 24, 31$  and 33. For  $B = 32, K = k(\sqrt{A\epsilon_0\sqrt{D}})$  by Lemma 2, so by Theorem 2, a basis is

$$\begin{cases} 1, \frac{1 + \sqrt{A\epsilon_0\sqrt{D}}}{2} & \text{if } A \equiv 1 \pmod{4} \\ 1, \sqrt{A\epsilon_0\sqrt{D}} & \text{if } A \equiv 3 \pmod{4}. \end{cases}$$

For  $B = 9, K = k(\sqrt{2A\epsilon_0\sqrt{D}})$  by Lemma 2, so by Theorem 2, a basis is  $1, \sqrt{2A\epsilon_0\sqrt{D}}$ .

2.  $D = 1189 = 29 \cdot 41$      $\epsilon_0 = \frac{1}{2}(25689 + 745\sqrt{1189})$      $2^{\delta/2}(r + i) = 25689 + 2i = (27 - 4i)^2(33 + 10i)$ . By Theorem 1,  $K = k(\sqrt{A(1189 + B\sqrt{1189})})$  has an integral basis over  $k$  for  $B = 10$  and 33, but not for  $B = 17$  and 30. For  $B = 10, K = k(\sqrt{A\epsilon_0\sqrt{D}})$  by Lemma 2, so by Theorem 2 a basis is

$$\begin{cases} 1, \frac{1 - \sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}} & \text{if } A \equiv 3 \pmod{4} \\ 1, \sqrt{A\epsilon_0\sqrt{D}} & \text{if } A \equiv 1 \pmod{4}. \end{cases}$$

For  $B = 33, K = k(\sqrt{2A\epsilon_0\sqrt{D}})$  by Lemma 2, so by Theorem 2, a basis is  $1, \sqrt{2A\epsilon_0\sqrt{D}}$ .

3.  $D = 2210 = 2 \cdot 5 \cdot 13 \cdot 17$      $\epsilon_0 = 47 + \sqrt{2210}$      $r + i = 47 + i$ . By Theorem 1,  $K = k(\sqrt{A(2210 + B\sqrt{2210})})$  has an integral basis over  $k$  for  $B = 47$ , but not for  $B = 1, 19, 23, 29, 37, 41$  and 43. For  $B = 47, K = k(\sqrt{A\epsilon_0\sqrt{D}})$  by Lemma 2, so by Theorem 2, a basis is  $1, \sqrt{A\epsilon_0\sqrt{D}}$ .
4.  $D = 221 = 13 \cdot 17$      $\epsilon_0 = \frac{1}{2}(15 + \sqrt{221})$  has norm  $+1$ , so no cyclic quartic field containing  $k = Q(\sqrt{221})$  has an integral basis over  $k$ .

# Chapter III: ON RELATIVE INTEGRAL BASES FOR PURE QUARTIC FIELDS

## §1. Introduction.

A relative extension of number fields may or may not have an integral basis. Let  $L$  denote the Galois closure of a pure quartic field and  $K, k$  be subfields of  $L$  such that  $[K : k] = 2$ . Explicit necessary and sufficient conditions are given for  $K/k$  to have an integral basis and a basis is determined whenever it exists.

## §2. Notation.

$\Delta_{M/K}$ : discriminant of  $M/K$ .

$\Delta_{M/K}(x_1, x_2, \dots, x_n)$ : relative discriminant of  $x_1, x_2, \dots, x_n$ .

$f, g, h$ : positive, squarefree, relatively prime integers such that  $f > 1$  and  $h$  is odd.

$$\eta = \sqrt[4]{fg^2h^3}, \bar{\eta} = \sqrt{fh}, \bar{\bar{\eta}} = \sqrt[4]{f^3g^2h}$$

$$\alpha = \begin{cases} (1+i)\eta & g - \text{odd} \\ (\frac{1+i}{2})\eta & g - \text{even} \end{cases}$$

$$\bar{\alpha} = i\bar{\eta}$$

$$\bar{\bar{\alpha}} = \begin{cases} (i-1)\bar{\bar{\eta}} & f, g - \text{odd} \\ (\frac{i-1}{2})\bar{\bar{\eta}} & f \text{ or } g - \text{even} \end{cases}$$

$$k_1 = Q(\sqrt{fh})$$

$$k_2 = Q(\sqrt{-fh})$$

$$k_3 = Q(\sqrt{-1})$$

$$K_1 = Q(\eta)$$

$$K_2 = Q((1+i)\eta)$$

$$K_3 = Q(\sqrt{fh}, \sqrt{-1})$$

$$L = Q(\eta, \sqrt{-1})$$

$B_i, b_i$  ( $i = 1, 2$ ): ideals of  $K_i$  and  $k_i$  respectively, whose square is 2, if they exist.

$I$ : the ideal of  $k_1$  with  $I^2 = (h)$ .

$\mathfrak{p}_1 \cdot \mathfrak{p}_2 = (2)$ : prime ideals of  $k_1$  when  $fh \equiv 1 \pmod{8}$  such that  $\mathfrak{p}_1$  ramifies in  $K_1$  when  $g$  is odd.

$\hat{\mathfrak{p}}_1 \cdot \hat{\mathfrak{p}}_2 = (2)$ : prime ideals of  $k_2$  when  $fh \equiv 7 \pmod{8}$  such that  $\hat{\mathfrak{p}}_1$  ramifies in  $K_2$  when  $g$  is even.

$\mathfrak{p} = \mathfrak{p}_1, \hat{\mathfrak{p}} = \hat{\mathfrak{p}}_1$ .

$P_1 \cdot P_2 = \mathfrak{p}_2$ : prime ideals of  $K_1$  which ramify in  $L$  when  $fh \equiv 1 \pmod{8}$  and  $g$  is odd.

$\hat{P}_1 \cdot \hat{P}_2 = \hat{\mathfrak{p}}_2$ : prime ideals of  $K_2$  which ramify in  $L$  when  $fh \equiv 7 \pmod{8}$  and  $g$  is even.

$P, \hat{P}$ : prime ideals of  $K_1$  and  $K_2$  lying over 2.

$\epsilon_0 = a + b\sqrt{fh}$ : fundamental unit of  $k_1$ .

$$\theta = \begin{cases} \sqrt[4]{fg^2} & h = 1. \\ \sqrt[4]{fg^2 h \epsilon_0^2} & h \neq 1 \text{ and } \pm h \text{ is a principal divisor of } k_1. \\ \sqrt[4]{-fg^2 h \epsilon_0^2} & h \neq 1 \text{ and } \pm 2h \text{ is a principal divisor of } k_1. \end{cases}$$

$$\gamma = \begin{cases} \frac{(g/2 - \bar{\eta})(1-i) + 2\sqrt[4]{-f(g/2)^2}}{4} & h = 1 \text{ and } \pm 2 \text{ is not a principal divisor of } k_1. \\ \frac{(a \cdot g/2 - \bar{\eta})(1-i) + 2\sqrt[4]{-f(g/2)^2 h \epsilon_0^2}}{4} & h \neq 1 \text{ and } \pm h \text{ is a principal divisor of } k_1. \\ \frac{(b \cdot g/2 - 1) + (b \cdot g/2 + 1)\bar{\eta} + 2\sqrt[4]{f(g/2)^2 h \epsilon_0^2}}{4} & \pm 2h \text{ is a principal divisor of } k_1. \end{cases}$$

$$\zeta = \begin{cases} \frac{(g + \bar{\alpha})(1-i) + 2\theta}{4} & h = 1. \\ \frac{(ag + \bar{\alpha})(1-i) + 2\theta}{4} & h \neq 1 \text{ and } \pm h \text{ is a principal divisor of } k_1. \end{cases}$$

$$\delta = \begin{cases} \frac{1 + \bar{\eta} + \theta}{2} & \pm h \text{ is a principal divisor of } k_1. \\ \frac{1 + i + \theta}{2} & \pm 2 \text{ is a principal divisor of } k_1. \end{cases}$$

$\phi = \frac{h + \alpha \pm \bar{\alpha} \pm \bar{\alpha}}{4}$  where the signs are chosen according as  $g/2 \equiv \pm 1 \pmod{4}$ .

$$\psi = \frac{1 + \bar{\alpha} + (1+i)\epsilon_0\theta}{2}.$$

$t$ : number of prime divisors of  $\Delta_{k_1/Q}$ .

$\rho$ : for a fixed real quadratic field  $k_1$ ,  $\rho$  is the ratio of all pure quartic fields  $K_1$  such that  $K_1/k_1$  has an integral basis to all those fields  $K_1$  which contain  $k_1$  for a fixed value of  $g$ .

$\sim$ : used to denote that two ideals of a field belong to the same ideal class.



### §3. Discriminants.

In this section we compute  $\Delta_{K_i/k_i}$  for  $i = 1, 2$ ,  $\Delta_{L/K_i}$ , for  $i = 1, 2, 3$  and  $\Delta_{L/k_3}$ .

**THEOREM 1.** *The relative discriminants are given by:*

$$\begin{aligned}
 \Delta_{K_1/k_1} &= \begin{cases} (2^2 g \sqrt{fh}) & fh \not\equiv 1 \pmod{8}, g - \text{odd or} \\ & fh \equiv 1 \pmod{4}, g - \text{even} \\ (g \sqrt{fh}) & fh \equiv 3 \pmod{8}, g - \text{even} \\ ((g/2) \sqrt{fh}) & fh \equiv 7 \pmod{8}, g - \text{even} \\ p^2(g \sqrt{fh}) & fh \equiv 1 \pmod{8}, g - \text{odd} \end{cases} \\
 \Delta_{K_2/k_2} &= \begin{cases} (2^2 g \sqrt{-fh}) & fh \equiv 0 \pmod{2}, g - \text{odd} \\ (2^3 g \sqrt{-fh}) & fh \equiv 3 \pmod{4}, g - \text{odd} \\ (2g \sqrt{-fh}) & fh \equiv 3 \pmod{8} \text{ or } fh \equiv 1 \pmod{4}, g - \text{even}; \\ & fh \equiv 5 \pmod{8}, g - \text{odd} \\ \hat{p}^2((g/2) \sqrt{-fh}) & fh \equiv 7 \pmod{8}, g - \text{even} \\ (g \sqrt{-fh}) & fh \equiv 1 \pmod{8}, g - \text{odd} \end{cases} \\
 \Delta_{L/K_1} &= \begin{cases} (1) & fh \equiv 3 \pmod{4} \\ P^2 & fh \equiv 2 \pmod{4} \\ (P_1 P_2)^2 & fh \equiv 1 \pmod{8}, g - \text{odd} \\ (2) & \text{otherwise} \end{cases} \\
 \Delta_{L/K_2} &= \begin{cases} (1) & fh \equiv 1 \pmod{4} \\ \hat{P}^2 & fh \equiv 2 \pmod{4} \\ (\hat{P}_1 \hat{P}_2)^2 & fh \equiv 7 \pmod{8}, g - \text{even} \\ (2) & \text{otherwise} \end{cases} \\
 \Delta_{L/K_3} &= \begin{cases} ((1+i)^3 g \sqrt{fh}) & fh \equiv 2 \pmod{4}, g - \text{odd} \\ (2^2 g \sqrt{fh}) & fh \equiv 3 \pmod{4}, g - \text{odd} \\ (g \sqrt{fh}) & fh \equiv 3 \pmod{8}, g - \text{even or} \\ & fh \equiv 1 \pmod{8}, g - \text{odd} \\ ((g/2) \sqrt{fh}) & fh \equiv 7 \pmod{8}, g - \text{even} \\ (2g \sqrt{fh}) & fh \equiv 1 \pmod{4}, g - \text{even or} \\ & fh \equiv 5 \pmod{8}, g - \text{odd} \end{cases} \\
 \Delta_{L/k_3} &= \begin{cases} (2^5 f^3 g^2 h^3) & fh \equiv 2 \pmod{4}, g - \text{odd} \\ (2^4 f^3 g^2 h^3) & fh \equiv 3 \pmod{4}, g - \text{odd} \\ (f^3 g^2 h^3) & fh \equiv 3 \pmod{8}, g - \text{even or} \\ & fh \equiv 1 \pmod{8}, g - \text{odd} \\ ((1/4) f^3 g^2 h^3) & fh \equiv 7 \pmod{8}, g - \text{even} \\ (2^2 f^3 g^2 h^3) & fh \equiv 1 \pmod{4}, g - \text{even or} \\ & fh \equiv 5 \pmod{8}, g - \text{odd} \end{cases}
 \end{aligned}$$

**PROOF:** Integral bases for  $K_1/Q$  and  $K_2/Q$  are given in Ljunggren [15] or Funakura [8], so

the discriminants of these extensions are easily computed. Using the formula

$$\Delta_{K_i/Q} = N_{k_i/Q}(\Delta_{K_i/k_i})\Delta_{k_i/Q}^2$$

and the factorizations of (2) given by Parry [19], the values of  $\Delta_{K_i/k_i}$  are readily determined.

Since  $1, i$  form a basis for the extension  $L/K_j$  it follows that  $\Delta_{L/K_j} | (2)^2$  for  $j = 1, 2$ . When  $fh \equiv 3 \pmod{4}$ , no prime divisor of (2) in  $K_1$  ramifies in  $L$ , so  $\Delta_{L/K_1} = (1)$ . Similarly,  $\Delta_{L/K_2} = (1)$  when  $fh \equiv 1 \pmod{4}$ .

Since  $\Delta_{L/Q} = N_{K_j/Q}(\Delta_{L/K_j}) \cdot \Delta_{K_j/Q}^2$  it follows that

$$\Delta_{L/Q} = \begin{cases} \Delta_{K_1/Q}^2 & fh \equiv 3 \pmod{4} \\ \Delta_{K_2/Q}^2 & fh \equiv 1 \pmod{4}. \end{cases}$$

Therefore  $N_{K_1/Q}(\Delta_{L/K_1}) = 2^4$  when  $fh \equiv 1 \pmod{4}$  and  $N_{K_2/Q}(\Delta_{L/K_2}) = 2^4$  when  $fh \equiv 3 \pmod{4}$ .

Using Hilbert's formula for the different it follows that all prime divisors of 2 in  $K_1$  which ramify in  $L$  must divide  $\Delta_{L/K_1}$  to the same exponent. Using this fact and the factorization of (2) given by Parry [19] we have that  $\Delta_{L/K_1} = (2)$  if  $fh \equiv 1 \pmod{4}$  and  $g$  is even, or  $fh \equiv 5 \pmod{8}$  and  $g$  is odd, and  $\Delta_{L/K_1} = (P_1 P_2)^2$  when  $fh \equiv 1 \pmod{8}$  and  $g$  is odd. Similarly,  $\Delta_{L/K_2} = (2)$  if  $fh \equiv 3 \pmod{4}$  and  $g$  is odd or if  $fh \equiv 3 \pmod{8}$  and  $g$  is even,  $\Delta_{L/K_2} = (\hat{P}_1 \hat{P}_2)^2$  when  $fh \equiv 7 \pmod{8}$  and  $g$  is even.

We now show  $\Delta_{L/K_1} = P^2$  when  $f \equiv 2 \pmod{4}$ . We have that  $(\sqrt[4]{fg^2h^3} + \sqrt[4]{f^3g^2h})^2 + gh\sqrt{fh} = 2gh\sqrt{fh} + 2fgh + fg\sqrt{fh} \equiv 4\sqrt{fh} \equiv 0 \pmod{4}$  so  $(\sqrt[4]{fg^2h^3} + \sqrt[4]{f^3g^2h}) + i\sqrt[4]{fg^2h^3} \equiv 0 \pmod{2}$ . Thus  $(\frac{\sqrt[4]{fg^2h^3} + \sqrt[4]{f^3g^2h} + i\sqrt[4]{fg^2h^3}}{2})$  is an integer of  $L$ . Now,

$$\Delta_{L/K_1} \left( 1, \frac{\sqrt[4]{fg^2h^3} + \sqrt[4]{f^3g^2h} + i\sqrt[4]{fg^2h^3}}{2} \right) = -gh\sqrt{fh}.$$

Since  $(gcd((2)^2, (-gh\sqrt{-fh}))) = P^2, \Delta_{L/K_1} | P^2$ . But Hilbert's formula for the different implies  $P^2 | \Delta_{L/K_1}$  so  $\Delta_{L/K_1} = P^2$ . Using a similar argument it follows that  $\Delta_{L/K_2} = \hat{P}^2$  when  $f \equiv 2 \pmod{4}$ .

To compute  $\Delta_{L/K_3}$ , we use the formula

$$N_{K_3/Q}(\Delta_{L/K_3}) \cdot \Delta_{K_3/Q}^2 = \Delta_{L/Q} = N_{K_1/Q}(\Delta_{L/K_1}) \cdot \Delta_{K_1/Q}^2$$

and the values of  $\Delta_{K_3/Q} = \begin{cases} 2^4 f^2 h^2 & fh \not\equiv 2 \pmod{4} \\ 2^6 f^2 h^2 & fh \equiv 2 \pmod{4} \end{cases}$  given by Bird and Parry [3]. Since Hilbert's formula for the different shows that all prime divisors of the same rational prime must divide  $\Delta_{L/K_3}$  to the same exponent,

$$\Delta_{L/K_3} = N_{K_1/Q}(\Delta_{L/K_1})^{1/4} \Delta_{K_1/Q}^{1/2} / \Delta_{K_3/Q}^{1/2}.$$

The values for  $\Delta_{L/k_3}$  follow from the formula

$$\Delta_{L/k_3} = N_{K_3/k_3}(\Delta_{L/K_3}) \cdot \Delta_{K_3/k_3}^2$$

and the values of  $\Delta_{K_3/k_3} = \begin{cases} (fh) & fh \not\equiv 2 \pmod{4} \\ (2fh) & fh \equiv 2 \pmod{4} \end{cases}$  given by Bird and Parry [3].

#### §4. Integral Bases.

In this section necessary and sufficient conditions for the existence of relative integral basis for the quadratic extensions  $K_1/k_1$ ,  $K_2/k_2$ ,  $L/K_1$ ,  $L/K_2$ ,  $L/K_3$  and the quartic extension  $L/k_3$  will be given. In addition an integral basis is given for each extension when it exists.

**THEOREM 2.** *Necessary and sufficient conditions are given for the existence of a relative integral basis for the given extension. In addition, an integral basis is given, when it exists. (Note: Here p.d. means principal divisor.)*

Extension Condition	$K_1/k_1$	$K_2/k_2$	$L/K_1$	$L/K_2$	$L/K_3$
$fh \equiv 2 \pmod{4}$ g-odd	$\pm h$ is a p.d. of $k_1$  $1, \theta$	$f = 2$  $1, \theta$	$P = (\pi)$  $1, (\frac{1+\bar{\pi}+i}{2})\pi$	$\bar{P} = (\bar{\pi})$  $1, (\frac{1+\bar{\pi}+i}{2})$	$fh = 2$  $1, \frac{\sqrt{(1+i)g}\sqrt{2(1+\sqrt{2})}}{\sqrt{2}}$
$fh \equiv 3 \pmod{4}$ g-odd	$\pm h$ is a p.d. of $k_1$  $1, \theta$	$h = 1$  $1, \alpha$	Always  $1, \frac{\bar{\pi}+i}{2}$	$B_2 = (\beta_2)$  $1, (\frac{1+i}{2})\beta_2$	$\pm h$ or $\pm 2h$ is a p.d. of $k_1$  $1, \theta$
$fh \equiv 3 \pmod{8}$ g-even	$\pm h$ is a p.d. of $k_1$  $1, \delta$	$h = 1$  $1, \alpha$	Always  $1, \frac{\bar{\pi}+i}{2}$	$B_2 = (\beta_2)$  $1, (\frac{1+i}{2})\beta_2$	$\pm h$ or $\pm 2h$ is a p.d. of $k_1$  $1, \delta$
$fh \equiv 7 \pmod{8}$ g-even	$\pm 2h$ is a p.d. of $k_1$  $1, \gamma$	$fh = 7$ or $fh = 15$ with $h = 3$ or $5$  $1, \varphi$	Always  $1, \frac{\bar{\pi}+i}{2}$	$P_1P_2 = (\pi_1)$  $1, (\frac{\alpha+i}{2})\pi_1$	$\pm h$ or $\pm 2h$ is a p.d. of $k_1$  $1, \gamma$
$fh \equiv 1 \pmod{4}$ g-even	$\pm h$ is a p.d. of $k_1$  $1, \theta$	$h = 1$  $1, \alpha$	$B_1 = (\beta_1)$  $1, (\frac{1+i}{2})\beta_1$	Always  $1, \frac{\bar{\alpha}+i}{2}$	$\pm h$ is a p.d. of $k_1$  $1, \frac{\theta}{1+i}$
$fh \equiv 5 \pmod{8}$ g-odd	$\pm h$ is a p.d. of $k_1$  $1, \theta$	$h = 1$  $1, (\frac{1+\alpha+\bar{\alpha}}{2})$	$B_1 = (\beta_1)$  $1, (\frac{1+i}{2})\beta_1$	Always  $1, \frac{\bar{\alpha}+i}{2}$	$\pm h$ is a p.d. of $k_1$  $1, \psi$
$fh \equiv 1 \pmod{8}$ g-odd	$I \cdot \mathfrak{p}_2 = (\zeta)$  $1, \frac{h+\eta}{\zeta}$	Never	$P_1P_2 = (\pi_1)$  $1, (\frac{\eta+i}{2})\pi_1$	Always  $1, \frac{\bar{\alpha}+i}{2}$	$\pm h$ is a p.d. of $k_1$  $1, \zeta$

First, we need

LEMMA. Let  $fh \equiv 3 \pmod{4}$ ,  $\epsilon_0 = a + b\sqrt{fh}$  and  $dh = \epsilon_0 s^2$  with  $d = 1$  or  $2$  and  $s \in k_1$ . If  $d = 1$  then  $a$  is odd and  $b \equiv 0 \pmod{4}$ . If  $d = 2$  then  $a$  is even and  $b$  is odd. In addition, if  $fh \equiv 7 \pmod{8}$  then  $a \equiv 0 \pmod{4}$ .

PROOF: Since  $fh \equiv 3 \pmod{4}$ ,  $a, b \in \mathbb{Z}$  and  $s = u + v\sqrt{fh}$  with  $u, v \in \mathbb{Z}$ . Thus

$$\begin{aligned}
 dh = \epsilon_0 s^2 &= (a + b\sqrt{fh})(u + v\sqrt{fh})^2 \\
 &= [a(u^2 + v^2 fh) + 2buvfh] + [b(u^2 + v^2 fh) + 2auv] \sqrt{fh}.
 \end{aligned}$$

Since  $h$  is odd,  $a$  is odd when  $d = 1$ . Since  $fh \equiv 3 \pmod{4}$ ,  $1 = a^2 - fhb^2 \equiv 1 - fhb^2 \pmod{8}$  so  $fhb^2 \equiv 0 \pmod{8}$ . Thus  $b \equiv 0 \pmod{4}$ . Suppose now  $d = 2$  and note  $a \not\equiv b$

(mod 2) when  $fh \equiv 3 \pmod{4}$ . If  $b$  is even, then  $a$  is odd so  $2 \equiv dh \equiv a(u^2 + v^2 fh) \equiv u^2 - v^2 \pmod{4}$ . Since the last congruence has no solution,  $a$  is even and  $b$  is odd. If  $fh \equiv 7 \pmod{8}$  then

$$1 = a^2 - fhb^2 \equiv a^2 + 1 \pmod{8}$$

so  $a^2 \equiv 0 \pmod{8}$ . Thus  $a \equiv 0 \pmod{4}$ .

**PROOF OF THEOREM:** First we use the criteria of Mann [17] to determine necessary and sufficient conditions for the existence of an integral basis. In order to determine an integral basis when it exists, it is sufficient to give a basis consisting of integers which has discriminant equal to the field discriminant given by Theorem 1. Since the discriminant of a basis is routinely calculated, it suffices to show the basis consists of integers in each case.

Using Mann's criteria  $K_1/k_1$  has an integral basis if and only if  $\Delta_{K_1/k_1} = (D)$  is principal and  $K_1 = k_1(\sqrt{D})$  for some generator  $D$  of  $\Delta_{K_1/k_1}$ . From Theorem 1, this is equivalent to  $dh = \epsilon s^2$  where  $d = g\sqrt{fh}/D$ ,  $\epsilon$  is a unit of  $k_1$  and  $s \in k_1$ . By absorbing square factors into  $s$ , unless  $fh \equiv 1 \pmod{8}$  with  $g$  odd, we may take  $d = 1$  or  $2$ . Taking norms gives,  $(dh)^2 = (s\bar{s})^2$ . Thus  $\pm dh = s\bar{s}$ , so  $\pm dh$  is a principal divisor of  $k_1$ .

Conversely, if  $\pm dh$  is a principal divisor of  $k_1$ , then  $(dh) = (s)(\bar{s})$  for some  $s \in k_1$ . Since  $dh$  divides  $\Delta_{k_1/Q}$ , all prime divisors of  $dh$  ramify in  $k_1$ . Thus  $(s) = (\bar{s})$ , so  $(dh) = (s^2)$ . Hence  $dh = \epsilon s^2$  for some unit  $\epsilon$  of  $k_1$  and so  $K_1/k_1$  has an integral basis.

If  $dh \neq 1$  then it is not a square in  $k_1$ , so  $dh = s^2\epsilon$  if and only if  $\epsilon$  is an odd power of the fundamental unit. Thus we may choose  $\epsilon = \epsilon_0$ .

If  $g$  is odd and  $fh \not\equiv 1 \pmod{8}$  or if  $fh \equiv 1 \pmod{4}$  and  $g$  is even then  $1, \theta$  is an integral basis for  $K_1/k_1$ .

If  $fh \equiv 3 \pmod{8}$  and  $g$  is even then  $d = 1$ , so by the Lemma  $a$  is odd and  $b \equiv 0 \pmod{4}$ . If  $\pm h$  is a principal divisor, then

$$\theta^2 \equiv g\sqrt{fh}\epsilon_0 \equiv ag\sqrt{fh} \equiv (1 + fh + g\sqrt{fh}) \equiv (1 + \bar{\eta})^2 \pmod{4}.$$

Hence  $\frac{1+\bar{\eta}+\theta}{2}$  is an integer of  $K_1$  and  $1, \frac{1+\bar{\eta}+\theta}{2}$  is an integral basis for  $K_1/k_1$ .

When  $fh \equiv 7 \pmod{8}$  and  $g$  is even then  $K_1/k_1$  has an integral basis if and only if  $\pm 2h$  is a principal divisor of  $k_1$ . From the Lemma  $b$  is odd and  $a \equiv 0 \pmod{4}$ . Thus, if  $\pm 2h$  is a principal divisor of  $k_1$ , then

$$\begin{aligned} (g/2)\epsilon_0\sqrt{fh} &\equiv (-g/2)b \equiv \left(\frac{(g/2)b-1}{2}\right)^2 - \left(\frac{(g/2)+1}{2}\right)^2 \\ &\equiv \left(\frac{(g/2)b-1}{2}\right)^2 - \left(\frac{(g/2)+1}{2}\right)^2 + 2\left(\frac{((g/2)b)^2-1}{4}\right)\sqrt{fh} \\ &\equiv \left[\left(\frac{(g/2)b-1}{2}\right) + \left(\frac{(g/2)+1}{2}\right)\sqrt{fh}\right]^2 \pmod{4}. \end{aligned}$$

Thus  $\sqrt[4]{f(g/2)^2h\epsilon_0^2} \equiv \frac{(g/2)b-1}{2} + \frac{(g/2)+1}{2}\sqrt{fh} \pmod{2}$ , so

$$\gamma = \frac{(g/2)b-1 + ((g/2)b+1)\bar{\eta} + 2\sqrt[4]{f(g/2)^2h\epsilon_0^2}}{4}$$

is an integer of  $K_1$ . Moreover  $1, \gamma$  is an integral basis for  $K_1/k_1$ .

When  $fh \equiv 1 \pmod{8}$  and  $g$  is odd  $K_1/k_1$  has an integral basis if and only if  $\mathfrak{p}^2$  is principal and  $h = \lambda\epsilon s^2$  where  $\mathfrak{p}^2 = (\lambda)$  and  $s \in k_1$ . The last statement is equivalent to the statement  $I\mathfrak{p}$  is principal. Now  $(2) = \mathfrak{q}_1\mathfrak{q}_2$  in  $k_1$  where  $\mathfrak{q}_1 = \left(\frac{h+g\sqrt{fh}}{2}, 2\right)$  and  $\mathfrak{q}_2 = \left(\frac{h-g\sqrt{fh}}{2}, 2\right)$ . Note  $\mathfrak{p} = \mathfrak{q}_1$  or  $\mathfrak{p} = \mathfrak{q}_2$ . Since  $\mathfrak{p}^2 \sim 1 \sim \mathfrak{q}_1\mathfrak{q}_2$ ,  $\mathfrak{q}_1 \sim \mathfrak{p} \sim \mathfrak{q}_2$ . Thus  $I\mathfrak{p}$  is principal if and only if  $I\mathfrak{q}_2$  is principal, say  $I\mathfrak{q}_2 = (\zeta)$ . To show that  $\frac{h+\sqrt{gh}\sqrt{fh}}{\zeta}$  is an integer it suffices to show its relative trace and norm for  $K_1/k_1$  are integers. Since the trace,  $2h/\zeta$ , is in the ideal  $I\mathfrak{q}_1$  it is an integer. Now  $\zeta^2 N_{K_1/k_1} \left(\frac{h+\sqrt{gh}\sqrt{fh}}{\zeta}\right) = h(h-g\sqrt{fh}) \in I^2\mathfrak{q}_2^2 = (\zeta)^2$ , so the norm is an integer of  $k_1$ . Since  $\mathfrak{p}(g\sqrt{fh}) = \Delta_{K_1/k_1}|\Delta_{K_1/k_1} \left(1, \frac{h+\sqrt{gh}\sqrt{fh}}{\zeta}\right) = \left(\frac{4gh\sqrt{fh}}{\zeta^2}\right) = \mathfrak{q}_1^2(g\sqrt{fh})$ , it follows that  $\mathfrak{p} = \mathfrak{q}_1$  and that  $1, \frac{h+\sqrt{gh}\sqrt{fh}}{\zeta}$  is an integral basis for  $K_1/k_1$ .

Next we consider  $K_2/k_2$ . Note that  $K_2 = Q((1+i)\sqrt[4]{fg^2h^3}) = k_2(\sqrt{2gh}\sqrt{-fh})$ . From Mann's criteria and Theorem 1, it follows that  $K_2/k_2$  has an integral basis if and only if  $dh = \pm s^2$  for some  $s \in k_2$  where  $(d) = (2g\sqrt{-fh})/\Delta_{K_2/k_2}$ . By absorbing square factors

into  $s$  we have  $d = 2, 1$ , or  $\hat{p}^2$ . If  $fh$  is even or  $fh \equiv 1 \pmod{8}$  with  $g$  odd the equation becomes  $2h = \pm s^2$ . Hence  $f = 2$ . In the remaining cases with  $fh$  odd, except when  $fh \equiv 7 \pmod{8}$  and  $g$  is even, the equation becomes  $h = \pm s^2$ , so  $h = 1$ . When  $fh \equiv 7 \pmod{8}$  and  $g$  is even the condition becomes  $\hat{p} \sim I$  and  $\hat{p}^2 = (\sigma)$  is principal. Since  $N_{k_2/Q}(\sigma) = 4$ , this can happen only when  $fh = 7$  or  $15$ . Moreover, when  $fh = 15$ ,  $h = 3$  or  $5$ .

When an integral basis exists, it is given by

$$\begin{aligned}
& 1, \sqrt{-g\sqrt{-2h}} \quad \text{if } f = 2 \\
& 1, \sqrt{2g\sqrt{-f}} \quad \text{if } fh \equiv 3 \pmod{4} \text{ and } g \text{ is odd} \\
& 1, \sqrt{(g/2)\sqrt{-f}} \quad \text{if } g \text{ is even and } fh \equiv 3 \pmod{8} \text{ or} \\
& \hspace{15em} fh \equiv 1 \pmod{4} \\
& 1, \frac{1 + \sqrt{2g\sqrt{-f}} + \sqrt{-f}}{2} \quad \text{if } fh \equiv 5 \pmod{8} \text{ and } g \text{ is odd} \\
& 1, \frac{1 \pm \sqrt{-7} + \frac{(i+1)}{2}\sqrt{g\sqrt{7}} \pm \frac{(i-1)}{2}\sqrt{7g\sqrt{7}}}{4} \quad \text{if } fh = 7 \text{ and } g \text{ is even} \\
& 1, \frac{h \pm \sqrt{-15} + \frac{(i+1)}{2}\sqrt{gh\sqrt{15}} \pm \frac{(i-1)}{2}\sqrt{\frac{15g}{h}\sqrt{15}}}{4} \quad \text{if } fh = 15 \text{ and } g \text{ is even}
\end{aligned}$$

where the  $+$  holds if and only if  $g/2 \equiv 1 \pmod{4}$ .

We next consider  $L/K_1$ . When  $fh \equiv 3 \pmod{4}$   $\Delta_{L/K_1} = (1)$ . Since  $L = K_1(\sqrt{-1})$ , Mann's criteria holds so  $L/K_1$  has an integral basis. It is easily checked that  $1, \frac{\sqrt{fh+i}}{2}$  is an integral basis.

When  $fh \equiv 2 \pmod{4}$  an integral basis exists if and only if  $P^2$  is principal, say  $P^2 = (\tau)$  where  $\tau \in K_1$ , and  $L = K_1(\sqrt{\tau\epsilon})$  where  $\epsilon$  is a unit of  $K_1$ . The second condition is true if and only if  $(-1) \cdot s^2 = \tau \cdot \epsilon$  for some  $s \in K_1$ . Equivalently  $(s)^2 = (\tau) = P^2$  or in other words  $P$  is a principal ideal in  $K$ .

When  $P$  is principal, say  $P = (\pi)$  we have  $T_{L/K_1} \left( \left( \frac{1+\sqrt{fh+i}}{2} \right) \pi \right) = (1 + \sqrt{fh}) \pi$  and  $N_{L/K_1} \left( \left( \frac{1+\sqrt{fh+i}}{2} \right) \pi \right) = \frac{2+fh}{4} \cdot \pi^2 + \frac{2\sqrt{fh} \cdot \pi^2}{4}$  are integers of  $K_1$  since  $(\pi)^4 = (2)$ .

When  $fh \equiv 1 \pmod{8}$  and  $g$  is odd, using Mann's criteria,  $L/K_1$  has an integral

basis if and only if  $(P_1P_2)^2$  is principal, say  $(P_1P_2)^2 = (\tau)$ , and  $L = K_1(\sqrt{\tau\epsilon})$  where  $\epsilon$  is a unit of  $K_1$ . As in the previous case this is true if and only if  $P_1P_2$  is principal, say  $P_1P_2 = (\pi)$ . Now  $T_{L/K_1} \left( \left( \frac{\sqrt[4]{fg^2h^3+i}}{2} \right) \pi \right) = \sqrt[4]{fg^2h^3} \cdot \pi$  is an integer of  $K_1$  and  $N_{L/K_1} \left( \left( \frac{\sqrt[4]{fg^2h^3+i}}{2} \right) \pi \right) = \left( \frac{1+gh\sqrt{fh}}{4} \right) \pi^2$ . While determining the basis for  $K_1/k_1$  we saw that  $\mathfrak{p} = \left( \frac{h+g\sqrt{fh}}{2}, 2 \right)$ . It follows that  $1 + gh\bar{\eta} \in \mathfrak{p}^2 = \left( \frac{4}{\pi^2} \right)$ . So  $\left( \frac{1+gh\bar{\eta}}{4} \right) \cdot \pi^2$  is an integer of  $K_1$ . Hence,  $\left( \frac{\sqrt[4]{fg^2h^3+i}}{2} \right) \cdot \pi$  is an integer of  $L$ .

When  $fh \equiv 5 \pmod{8}$  and  $g$  is odd or  $fh \equiv 1 \pmod{4}$  and  $g$  is even, using Mann's criteria, it follows that  $L/K_1$  has an integral basis if and only if  $B_1$  is principal, say  $B_1 = (\beta_1)$ . Now  $T_{L/K_1} \left( \left( \frac{1+i}{2} \right) \beta_1 \right) = \beta_1$  and  $N_{L/K_1} \left( \left( \frac{1+i}{2} \right) \beta_1 \right) = \epsilon$  are integers of  $K_1$  where  $\epsilon$  is some unit of  $K_1$ . So  $\left( \frac{1+i}{2} \right) \beta_1$  is an integer of  $L$ .

Proofs similar to those for  $L/K_1$  give the results for  $L/K_2$ .

We now consider  $L/K_3$ . Mann's criteria shows that  $L/K_3$  has an integral basis if and only if  $L = K_3 \left( \sqrt{gh\sqrt{fh}} \right) = K_3 \left( \sqrt{dg\sqrt{fh}\epsilon} \right)$  where  $(d) = (\Delta_{L/K_3}/g\sqrt{fh})$  is determined by Theorem 1 and  $\epsilon$  is a unit of  $K_3$ . This condition is equivalent to  $dh = \epsilon \cdot s^2$  for some  $s \in K_3$ . By absorbing square factors of  $d$  into  $s$ , we may assume  $d = 1 + i$  when  $f \equiv 2 \pmod{4}$  and  $d = 1$  otherwise.

When  $f = 2$  and  $h = 1$

$$dh = (1 + i) = (1 + \sqrt{2}) \cdot \left( \frac{\sqrt{2}(1 + i)}{1 + \sqrt{2} + i} \right)^2 = \epsilon \cdot s^2 \text{ so } L/K_3$$

has an integral basis. Since  $\omega^4 = \left( \frac{\sqrt{(1+i)g\sqrt{2}(1+\sqrt{2})}}{\sqrt{2}} \right)^4 = ig^2(1 + \sqrt{2})^2$  is an integer and  $1, \omega$  is a basis for  $L/K_3$  with discriminant generating the field discriminant, it follows that  $1, \omega$  form an integral basis for  $L/K_3$ .

When  $fh \equiv 2 \pmod{4}$ ,  $(2)(h)^2 = (s\bar{s})^2$  so  $(2)$  is the square of a principal ideal of  $k_1$ . Thus, when  $fh \neq 2$ , Satz 13 of Kuroda [14] applies to show that  $\epsilon = i^c((1 + i)\sqrt{\frac{\epsilon_0}{2}})^j$  for some integers  $c$  and  $j$ . By combining square terms, we may take  $c, j \in \{0, 1\}$ . If  $j = 0$  then  $(1 + i)h = i^c s^2$  so that  $2h^2 = (s\bar{s})^2$ . Hence  $\sqrt{2} \in k_1$  contradicting that  $fh \neq 2$ . Thus  $j = 1$



so  $h = i^c \sqrt{\frac{\epsilon_0}{2}} s^2$ . Taking conjugates gives

$$(-i)^c \sqrt{\frac{\epsilon_0}{2}} \bar{s}^2 = i^c \sqrt{\frac{\epsilon_0}{2}} s^2$$

so  $\bar{s}^2 = (-1)^c s^2$ .

If  $c = 0$  then  $s^2 \in k_1$  so either  $s$  or  $i \cdot s \in k_1$ . But  $s^2 > 0$  so  $s \in k_1$ . But  $h = \sqrt{\frac{\epsilon_0}{2}} \cdot s^2$ , so by squaring and taking norms we obtain  $4h^4 = (ss')^4$ , a contradiction. If  $c = 1$  then  $\bar{s}^2 = -s^2$  so  $s = t(1 \pm i)$  for some  $t \in k_1$ . So  $h = \pm 2\sqrt{\frac{\epsilon_0}{2}} t^2$ . Squaring and taking norms again gives

$$h^4 = 4(tt')^4.$$

Thus no solution exists when  $fh \equiv 2 \pmod{4}$  and  $fh \neq 2$ .

When  $fh \not\equiv 2 \pmod{4}$ ,  $d = 1$  so the condition for  $L/K_3$  to have an integral basis becomes  $h = \epsilon s^2$ . When  $fh \neq 3$  either  $\epsilon = i^c \epsilon'$  or  $\epsilon = i^c(1+i)\sqrt{\frac{\epsilon_0}{2}}$  where  $\epsilon'$  is a unit of  $k_1$  and  $c = 0$  or  $1$ . If  $\epsilon = i^c(1+i)\sqrt{\frac{\epsilon_0}{2}}$  then  $i^c s^2(1+i)\sqrt{\frac{\epsilon_0}{2}} = h = (-i)^c (\bar{s})^2(1-i)\sqrt{\frac{\epsilon_0}{2}}$ . Thus  $s^2(1+i) = (i^{-2c})\bar{s}^2(1-i) = (i^{-2c})\bar{s}^2(1+i)(-i)$ . So  $(\frac{s}{\bar{s}})^2 = (i^{-1-2c})$ . This equation has no solution in  $K_3$ .

If  $\epsilon = \epsilon'$  then  $\frac{h}{\epsilon} = s^2 \in k_1$ . If  $s \in k_1$  it follows that  $\pm h$  is a principal divisor of  $k_1$ . If  $s \notin k_1$  we have  $k_1(s) = K_3 = k_1(\sqrt{-1})$ . So  $\frac{h}{\epsilon} = -t^2$  for some  $t \in k_1$ . Again it follows that  $\pm h$  is a principal divisor of  $k_1$ . On the other hand if  $\pm h$  is a principal divisor of  $k_1$  then  $h = s^2 \epsilon$  for some  $\epsilon, s \in k_1$  where  $\epsilon$  is a unit.

If  $\epsilon = i\epsilon'$  we have  $h = s^2 i\epsilon'$  so  $h = -\bar{s}^2 i\epsilon'$ . Hence  $s^2 = -\bar{s}^2 = (i\bar{s})^2$  and so  $s = \pm i\bar{s}$ . This implies  $s = x(1 \pm i)$  for some  $x \in k_1$ . Then  $s^2 = \pm 2x^2 i$  and so  $\pm h = 2x^2 \epsilon'$ . Therefore  $\pm 2h = (2x)^2 \epsilon'$ . It follows that  $\pm 2h$  is a principal divisor of  $k_1$ . Note that since  $2h$  and  $-2h$  are not squares in  $k_1$  we may choose  $\epsilon' = \epsilon_0$ . On the other hand when  $\pm 2h$  is a principal divisor of  $k_1$  it follows that  $\pm 2h = x^2 \epsilon_0$  for some  $x \in k_1$ . Therefore  $\pm h = \left(\frac{x}{1 \pm i}\right)^2 (i\epsilon_0)$ . Note that the equation  $\pm 2h = x^2 \epsilon_0$  does not have a solution for  $x \in k_1$  when  $fh \equiv 1 \pmod{4}$ , since then 2 is unramified in  $k_1$ .

When  $fh = 3$ ,  $h = 1 = 1 \cdot 1^2$ . Thus in this case  $L/K_3$  always has an integral basis and  $h$  is a principal divisor of  $k_1$ .

When  $\pm h$  is a principal divisor of  $k_1$  we have seen that  $\theta = \sqrt[4]{fg^2h\epsilon_0^2} \in L$ . When  $\pm 2h$  is a principal divisor of  $k_1$ , we have  $\pm 2h = s^2\epsilon_0$  for some  $s \in k_1$ . Hence  $h^2 = \left(\frac{s}{1+i}\right)^4 (-\epsilon_0^2)$ . Thus  $\sqrt[4]{fg^2h^3} = \frac{s}{1+i} \sqrt[4]{-fg^2h\epsilon_0^2} = \frac{s}{1+i} \cdot \theta$ . So it follows that  $\theta \in L$ .

It was shown while determining the basis for  $K_1/k_1$  that when  $fh \equiv 3 \pmod{8}$ ,  $g$  is even, and  $\pm h$  is a principal divisor of  $k_1$ ,  $\delta = \frac{1+\eta+\theta}{2}$  is an integer of  $L$ . If  $\pm 2h$  is a principal divisor of  $k_1$ , then by the Lemma  $a$  is even and  $b$  is odd. Thus,  $(1+i)^2 = 2i \equiv gb f h i + ag\sqrt{-fh} \equiv g\epsilon_0\sqrt{-fh} \pmod{4}$ . So  $1+i \equiv \sqrt[4]{-fg^2h\epsilon_0^2} \pmod{2}$  and  $\delta = \frac{1+i+\sqrt[4]{-fg^2h\epsilon_0^2}}{2}$  is an integer of  $L$ .

While determining the basis for  $K_1/k_1$  it was shown when  $fh \equiv 7 \pmod{8}$ ,  $g$  is even, and  $\pm 2h$  is a principal divisor of  $k_1$  that  $\gamma$  is an integer of  $L$ . When  $h = 1$ ,  $\left(\frac{g/2-\sqrt{f}}{1+i}\right)^2 \equiv (g/2)i\sqrt{f} \equiv (\sqrt[4]{-f(g/2)^2})^2 \pmod{4}$ . Thus  $\gamma = \frac{(\frac{g/2-\sqrt{f}}{1+i})+\sqrt[4]{-f(g/2)^2}}{2} = \frac{(g/2-\sqrt{f})(1-i)+2\sqrt[4]{-f(g/2)^2}}{4}$  is an integer of  $L$ . When  $h \neq 1$  and  $\pm h$  is a principal divisor of  $k_1$ , since  $a$  is odd and  $b \equiv 0 \pmod{4}$ ,  $\left(\frac{ag/2-\sqrt{fh}}{1+i}\right)^2 \equiv (ag/2)i\sqrt{fh} \equiv (\sqrt[4]{-f(g/2)^2h\epsilon_0^2})^2 \pmod{4}$ . Hence  $\gamma = \frac{(\frac{a \cdot g/2-\sqrt{fh}}{1+i})+\sqrt[4]{-f(g/2)^2h\epsilon_0^2}}{2} = \frac{(a \cdot g/2-\sqrt{fh})(1-i)+2\sqrt[4]{-f(g/2)^2h\epsilon_0^2}}{4}$  is an integer of  $L$ .

When  $fh \equiv 1 \pmod{4}$ ,  $g$  is even, and  $\pm h$  is a principal divisor of  $k_1$ ,  $\left(\frac{\theta}{1+i}\right)^2 = (-g/2)i \cdot \sqrt{fh} \cdot \epsilon$ , where  $\epsilon = 1$  if  $h = 1$  and  $\epsilon = \epsilon_0$  otherwise, which is an integer of  $L$ .

When  $fh \equiv 5 \pmod{8}$ ,  $g$  is odd and  $\pm h$  is a principal divisor of  $k_1$  it follows that  $N(\epsilon_0) = 1$ . Note that  $\epsilon_0^3 = r + s\sqrt{fh}$  where  $r, s \in \mathbb{Z}$  with  $r$  odd and  $s \equiv 0 \pmod{4}$ . Now  $[(1+i)\epsilon_0\theta]^2 \equiv 2i\epsilon_0^3g\sqrt{fh} \equiv 2\sqrt{-fh} \equiv 1 - fh + 2\sqrt{-fh} \equiv (1+\bar{\alpha})^2 \pmod{4}$ . Thus  $\frac{1+\bar{\alpha}+(1+i)\epsilon_0\theta}{2}$  is an integer of  $L$ .

Finally, we consider the case  $fh \equiv 1 \pmod{8}$  and  $g$ -odd. Let  $a_0 + b_0\sqrt{fh} = \epsilon = \begin{cases} \epsilon_0 & h \neq 1 \\ 1 & h = 1 \end{cases}$ . Note that since  $fh \equiv 1 \pmod{8}$ ,  $a_0$  and  $b_0$  are integers. When  $\pm h$  is a

principal divisor of  $k_1$ ,  $N(\epsilon) = 1$ . Since  $a_0^2 - b_0^2 fh \equiv a_0^2 - b_0^2 \equiv 1 \pmod{8}$ ,  $a_0$  is odd and  $b_0 \equiv 0 \pmod{4}$ . Thus  $\left(\frac{ga_0 + \sqrt{-fh}}{1+i}\right)^2 \equiv ga_0 \sqrt{fh} \equiv (\sqrt[4]{fg^2 h \epsilon^2})^2 \pmod{4}$ . Therefore,  $\frac{(ga_0 + \sqrt{-fh})(1-i) + 2\sqrt[4]{fg^2 h \epsilon^2}}{4}$  is an integer of  $L$ .

**THEOREM 3.**  $L/k_3$  always has an integral basis. A basis is given by

$$\begin{array}{ll}
 1, \frac{\eta(1+i) + \bar{\eta}}{2}, \frac{\bar{\eta}(1+i)}{2}, \frac{\bar{\bar{\eta}}(1+i)}{2} & fh \equiv 2 \pmod{4}, g - \text{odd} \\
 1, \eta, \frac{1+i\bar{\eta}}{2}, \frac{\eta+i\bar{\bar{\eta}}}{2} & fh \equiv 3 \pmod{4}, g - \text{odd} \\
 1, \frac{1+i\bar{\eta}}{2}, \frac{1+\eta+\bar{\eta}}{2}, \frac{1+3i+\eta+(1+i)\bar{\eta}+(-1)^{\frac{h-1}{2}}i\bar{\bar{\eta}}}{4} & fh \equiv 3 \pmod{8}, g - \text{even} \\
 1, \frac{1+i\bar{\eta}}{2}, \frac{1+\eta+(g/2)h\bar{\eta}}{2(1+i)}, \frac{1+(g/2)fi+\eta+((g/2)h+i)\bar{\eta}+(-1)^{(h-1)/2}i\bar{\bar{\eta}}}{4(1+i)} & fh \equiv 7 \pmod{8}, g - \text{even} \\
 1, \alpha, \frac{1+i\bar{\alpha}}{2}, \frac{\alpha+i\bar{\bar{\alpha}}}{2} & fh \equiv 1 \pmod{4}, g - \text{even} \\
 1, \frac{1+i\bar{\alpha}}{2}, \frac{1+\alpha+\bar{\alpha}}{2}, \frac{1+3i+\alpha+(1+i)\bar{\alpha}+(-1)^{(h-1)/2}i\bar{\bar{\alpha}}}{4} & fh \equiv 5 \pmod{8}, g - \text{odd} \\
 1, \frac{1+i\bar{\alpha}}{2}, \frac{1+\alpha+gh\bar{\alpha}}{2(1+i)}, \frac{1-fgi+\alpha+(gh+i)\bar{\alpha}+(-1)^{\frac{h-1}{2}}i\bar{\bar{\alpha}}}{4(1+i)} & fh \equiv 1 \pmod{8}, g - \text{odd}
 \end{array}$$

**PROOF:** Since  $k_3$  has class number 1,  $L/k_3$  always has an integral basis. As in Theorem 2, it is only necessary to check that all elements of each basis are integers and that its discriminant equals the field discriminant in each case. The latter is routine and will be left to the reader.

When  $fh \equiv 0 \pmod{2}$  and  $g$  is odd,  $\bar{\eta}^2 = fh \equiv -fh \equiv (i\bar{\eta})^2 \pmod{4}$ . So  $\bar{\eta} \equiv i\bar{\eta} \pmod{2}$  and thus  $(\frac{1+i}{2})\bar{\eta}$  is an integer. Since  $\left(\frac{\eta(1+i)+\bar{\eta}}{2}\right)^2 = \left(\frac{fg/2+ghi}{2}\right)\bar{\eta} + \frac{fgh(1+i)}{2}$  and  $fg/2 \equiv gh \equiv 1 \pmod{2}$ ,  $\left(\frac{fg/2+ghi}{2}\right)\bar{\eta}$  is an integer of  $L$ . Hence  $\frac{\eta(1+i)+\bar{\eta}}{2}$  is an integer. Since  $(\bar{\bar{\eta}})^2 = fg\sqrt{fh} \equiv -fg\sqrt{fh} \equiv (i\bar{\bar{\eta}})^2 \pmod{4}$ ,  $\bar{\bar{\eta}} \equiv i\bar{\bar{\eta}} \pmod{2}$  and so  $(\frac{1+i}{2})\bar{\bar{\eta}}$  is an integer of  $L$ .

When  $fh \equiv 3 \pmod{4}$ ,  $(i\bar{\eta})^2 = -fh \equiv 1 \pmod{4}$ . So  $i\bar{\eta} \equiv 1 \pmod{2}$  and therefore  $\frac{1+i\bar{\eta}}{2}$  is an integer of  $L$ . We also have that  $h \equiv f^2h \equiv -f \pmod{4}$  and thus  $\eta^2 \equiv gh\sqrt{fh} \equiv -fg\sqrt{fh} \equiv (i\bar{\eta})^2 \pmod{4}$ . Thus  $\eta \equiv i\bar{\eta} \pmod{2}$  so  $\frac{\eta+i\bar{\eta}}{2}$  is an integer of  $L$ .

When  $fh \equiv 3 \pmod{8}$  and  $g$  is even,  $(1 + \bar{\eta})^2 = (1 + fh) + 2\sqrt{fh} \equiv gh\sqrt{fh} \equiv \eta^2 \pmod{4}$ . Therefore  $1 + \bar{\eta} \equiv \eta \pmod{2}$  and thus  $\frac{1+\eta+\bar{\eta}}{2}$  is an integer of  $L$ . Hence  $\left(\frac{1+i\bar{\eta}}{2}\right) \left(\frac{1+\eta+\bar{\eta}}{2}\right) = (1/4)[1 + ifh + \eta + (1+i)\bar{\eta} + ih\bar{\eta}]$  is an integer of  $L$ . Since  $fh \equiv 3 \pmod{4}$ ,  $(1/4)[1 + 3i + \eta + (1+i)\bar{\eta} + (-1)^{\frac{\Lambda-1}{2}}i\bar{\eta}]$  is also an integer of  $L$ .

Suppose now that  $fh \equiv 7 \pmod{8}$  and  $g$  is even. Since  $\eta^2 = gh\sqrt{fh} \equiv (1 + (g/2)h\bar{\eta})^2 \pmod{8}$ , it follows that  $\frac{1+\eta+(g/2)h\bar{\eta}}{2(1+i)}$  is an integer of  $L$ . Hence  $\left(\frac{1+i\bar{\eta}}{2}\right) \left(\frac{1+\eta+(g/2)h\bar{\eta}}{2(1+i)}\right) = \frac{1}{4(1+i)}[1 + (g/2)fh^2i + \eta + ((g/2)h + i)\bar{\eta} + ih\bar{\eta}]$  is an integer of  $L$ . Also, since  $g$  is even  $(1+i)|\bar{\eta}$ . Thus  $\frac{1}{4(1+i)}[(1 + (g/2)fi) + \eta + ((g/2)h + i)\bar{\eta} + ih\bar{\eta}] - \left(\frac{h-(-1)^{(\Lambda-1)/2}}{4}\right) \left(\frac{i\bar{\eta}}{1+i}\right) = \frac{1}{4(1+i)}[(1 + (g/2)fi) + \eta + ((g/2)h + i)\bar{\eta} + (-1)^{(\Lambda-1)/2}i\bar{\eta}]$  is an integer of  $L$ .

When  $fh \equiv 1 \pmod{4}$ ,  $\frac{1+i\bar{\alpha}}{2} = \frac{1-\bar{\eta}}{2} = \frac{1-\sqrt{fh}}{2}$  is an integer. In addition  $f \equiv fh^2 \equiv h \pmod{4}$ , so when  $g$  is even,  $\alpha^2 = (g/2)ih\sqrt{fh} \equiv (g/2)if\sqrt{fh} \equiv (i\bar{\alpha})^2 \pmod{4}$ . Hence  $\frac{\alpha+i\bar{\alpha}}{2}$  is an integer of  $L$ .

When  $fh \equiv 5 \pmod{8}$  and  $g$  is odd then  $(1+\bar{\alpha})^2 = (1-fh) + 2\sqrt{-fh} \equiv 2gh\sqrt{-fh} \equiv \alpha^2 \pmod{4}$ . Therefore  $\frac{1+\alpha+\bar{\alpha}}{2}$  is an integer of  $L$ . Hence  $\left(\frac{1+i\bar{\alpha}}{2}\right) \left(\frac{1+\alpha+\bar{\alpha}}{2}\right) = \frac{(1-fhi)+\alpha+(1+i)\bar{\alpha}+hi\bar{\alpha}}{4}$  is an integer of  $L$ . Since  $fh \equiv 5 \pmod{8}$  it follows that  $\frac{(1+3i)+\alpha+(1+i)\bar{\alpha}+(-1)^{\frac{\Lambda-1}{2}}i\bar{\alpha}}{4}$  is an integer of  $L$ .

When  $fh \equiv 1 \pmod{8}$  and  $g$  is odd,  $(1+gh\bar{\alpha})^2 = (1-fg^2h^3) + 2gh\sqrt{-fh} \equiv 2gh\sqrt{-fh} \equiv \alpha^2 \pmod{8}$ . Thus  $\frac{1+\alpha+gh\bar{\alpha}}{2(1+i)}$  is an integer of  $L$ . Hence  $\left(\frac{1+i\bar{\alpha}}{2}\right) \left(\frac{1+\alpha+gh\bar{\alpha}}{2(1+i)}\right) = \frac{1}{4(1+i)}[(1 - fgh^2i) + \alpha + (gh + i)\bar{\alpha} + ih\bar{\alpha}]$  is an integer of  $L$ . Since  $f$  and  $g$  are odd  $(1+i)$  divides  $\bar{\alpha}$ . So  $\frac{1}{4(1+i)}[(1 - fgi) + \alpha + (gh + i)\bar{\alpha} + ih\bar{\alpha}] - \left(\frac{h-(-1)^{\frac{\Lambda-1}{2}}}{4}\right) \left(\frac{i\bar{\alpha}}{1+i}\right) = \frac{1}{4(1+i)}[(1 - fgi) + \alpha + (gh + i)\bar{\alpha} + (-1)^{\frac{\Lambda-1}{2}}i\bar{\alpha}]$  is an integer of  $L$ .

## §5. Class Number Considerations.

In this section we explicitly compute the value of  $\rho$ , which we defined in Section 2, and show that it is related to the rank of the 2-class group of  $k_1$ . Corollary 3 of this section is a variation on Theorem 2 of [8]. Here  $1, -fh$  will be referred to as trivial principal divisors of  $k_1$  while all others will be called nontrivial.

THEOREM 4. If  $N(\epsilon_0) = -1$  then

$$\rho = \begin{cases} 0 & \text{if } fh \equiv 1 \pmod{8} \text{ with } g \text{ odd and } p_2^2 \nmid (1). \\ \frac{1}{2^{t-1}} & \text{otherwise.} \end{cases}$$

If  $N(\epsilon_0) = +1$  and there are no nontrivial odd principal divisors of  $k_1$ , then  $\rho = \frac{1}{2^{t-1}}$ . If

$N(\epsilon_0) = +1$  and  $k_1$  has a nontrivial odd principal divisor then

$$\rho = \begin{cases} \frac{1}{2^{t-3}} & \text{if } fh \equiv 3 \pmod{8}, \text{ or } fh \equiv 7 \pmod{8} \text{ with } g \text{ odd.} \\ \frac{1}{2^{t-2}} & \text{if } fh \equiv 2 \pmod{4}, fh \equiv 5 \pmod{8}, \text{ or } fh \equiv 1 \pmod{8} \text{ and} \\ & p_2 \text{ generates a strongly ambiguous class of } k_1 \text{ when } g \text{ is odd.} \\ 0 & \text{otherwise.} \end{cases}$$

PROOF: To insure  $f > 1$ , fix a prime divisor  $q$  of  $fh$  and require it to divide  $f$ . When  $fh$  is even we will choose  $q = 2$ .

When  $N(\epsilon_0) = -1$  then  $fh \not\equiv 3 \pmod{4}$  and Theorem 3.1 of Barrucand and Cohn [2] shows that  $k_1$  has no nontrivial principal divisors. If  $fh \equiv 1 \pmod{8}$  with  $g$  odd and  $p_2^2 \nmid (1)$  then it follows from Theorem 2 that  $K_1/k_1$  never has an integral basis. Otherwise, there is exactly one value of  $h$  for which  $K_1/k_1$  has an integral basis and exactly  $2^{t-1}$  possible values for  $h$ , so  $\rho = 1/2^{t-1}$ .

Assume now that  $N(\epsilon_0) = +1$  and that  $k_1$  has no nontrivial odd principal divisors. Note this can only occur when  $fh \equiv 3 \pmod{4}$ . If  $g$  is odd or  $fh \equiv 3 \pmod{8}$  with  $g$  even then Theorem 2 shows that  $K_1/k_1$  has an integral basis exactly when  $h = 1$ . Now the two nontrivial principal divisors  $n_1$  and  $n_2$  are both even and we may assume  $q|n_1$ . Thus when  $fh \equiv 7 \pmod{8}$  and  $g$  is even,  $K_1/k_1$  has an integral basis if and only if  $2h = \pm n_2 > 0$ . Since there are  $2^{t-2}$  possible values for  $h$ ,  $\rho = 1/2^{t-2}$ .

Assume now that  $N(\epsilon_0) = +1$  and that  $k_1$  has a nontrivial odd principal divisor. If  $fh \equiv 3 \pmod{4}$  then both principal divisors  $n_1$  and  $n_2$  must be odd and as above we assume  $q|n_1$ . If  $fh \equiv 3 \pmod{8}$  or  $fh \equiv 7 \pmod{8}$  with  $g$  odd then Theorem 2 shows  $K_1/k_1$  has an integral basis if and only if  $h = 1$  or  $\pm n_2$  with the sign chosen so that  $h > 0$ . Since there are  $2^{t-2}$  possible values for  $h$ ,  $\rho = \frac{1}{2^{t-3}}$ . If  $fh \equiv 2 \pmod{4}$ ,  $fh \equiv 5 \pmod{8}$

or  $fh \equiv 1 \pmod{8}$  with  $g$  even, then as above there are exactly two values of  $h$  such that  $K_1/k_1$  has an integral basis. However, here there are  $2^{t-1}$  possible values for  $h$ , so  $\rho = \frac{1}{2^{t-2}}$ . Suppose  $fh \equiv 1 \pmod{8}$  with  $g$  odd and  $\mathfrak{p}_2$  generates a strongly ambiguous class of  $k_1$ . Thus  $\mathfrak{p}_2 \sim I$  where  $I$  is an ambiguous ideal of  $k_1$ . This means  $I | (\sqrt{fh})$ . Since  $(\sqrt{fh})$  is a principal ideal of  $k_1$ , we can always choose  $I$  with  $(I, (q)) = 1$ . Now the principal divisor  $(n_2)$  satisfies  $J^2 = (n_2)$  for some ideal  $J$  of  $k_1$ . Let  $IJ = J_1^2 J_2$  where  $J_2$  is a square free ideal of  $k_1$ . Then  $K_1/k_1$  has an integral basis precisely for the values  $h = h_1$  and  $h = h_2$  where  $h_1 > 0$ ,  $h_2 > 0$  and  $I^2 = (h_1)$ ,  $J_2^2 = (h_2)$ . As above  $\rho = \frac{1}{2^{t-2}}$ . If  $fh \equiv 1 \pmod{8}$  with  $g$  odd and  $\mathfrak{p}_2$  does not belong to a strongly ambiguous class of  $k_1$ , then  $\mathfrak{p}_2 \not\sim I$  or  $I\mathfrak{p}_2 \not\sim (1)$  for any choice of  $I$ . Thus no extension  $K_1/k_1$  has an integral basis in this case. If  $fh \equiv 7 \pmod{8}$  and  $g$  is even, then since all principal divisors must be odd, it also follows that no extension  $K_1/k_1$  has an integral basis.

COROLLARY 1. Let  $u$  denote the rank of the 2-class group of  $k_1$  and assume  $\rho \neq 0$ . If  $N(\epsilon_0) = -1$  then  $\rho = 1/2^u$ . If  $N(\epsilon_0) = +1$  then

$$\rho = \begin{cases} \frac{1}{2^{u-1}} & \text{if } fh \text{ is the sum of two squares, or } fh \equiv 3 \pmod{4} \text{ and } \\ & k_1 \text{ has a nontrivial odd principal divisor.} \\ \frac{1}{2^u} & \text{if } fh \equiv 1, 2 \pmod{4} \text{ and is not the sum of two squares, or} \\ & fh \equiv 3 \pmod{4} \text{ and } k_1 \text{ has no nontrivial odd principal divisors.} \end{cases}$$

PROOF: It is shown in Theorem 3.1 of [2] that  $u = t - 1$  or  $t - 2$  according as  $fh$  is the sum of two squares or not. The results are now immediate from Theorem 4.

COROLLARY 2. If  $\rho \neq 0$  and  $k_1$  has odd class number then every extension  $K_1/k_1$  has an integral basis.

PROOF: Since  $k_1$  has odd class number  $u = 0$ . If  $fh$  is the sum of two squares then  $t = 1$ , so  $N(\epsilon_0) = -1$  and  $\rho = 1$ . If  $fh \equiv 3 \pmod{4}$  then  $t = 2$ , so no nontrivial odd principal divisors exist. Thus we always have  $\rho = 1$ , so  $K_1/k_1$  always has an integral basis.

COROLLARY 3. For a fixed real quadratic field  $k_1$ ,  $K_1/k_1$  has an integral basis for all pure quartic fields  $K_1$  containing  $k_1$ , if and only if  $\rho \neq 0$  and  $fh = 2, p, q, 2q, q_1q_2$ , or  $fh = 2p$ ,

$p_1 p_2$  with  $N(\epsilon_0) = +1$ , or  $fh = pq$  where  $\pm p$  and  $\pm q$  are principal divisors. Here the  $p$ 's and  $q$ 's denote primes which are congruent to 1 and 3 (mod 4) respectively.

PROOF: The first condition is equivalent to  $\rho = 1$ . When  $N(\epsilon_0) = -1$ , then  $t = 1$  so  $fh = 2$  or  $p$ . Since  $k_1$  has  $N(\epsilon_0) = -1$  for these values of  $fh$ , the converse also holds. If  $fh \equiv 1, 2 \pmod{4}$  and is not the sum of two squares or  $fh \equiv 3 \pmod{4}$  and no nontrivial odd principal divisors exist then  $\rho = 1$  if and only if  $t = 2$  which is true exactly when  $fh = q, 2q$  or  $q_1 q_2$ . If  $N(\epsilon_0) = +1$  and  $fh$  is the sum of two squares,  $\rho = 1$  if and only if  $t = 2$  or  $fh = 2p$  or  $p_1 p_2$ . If  $fh \equiv 3 \pmod{4}$  and  $k_1$  has nontrivial odd principal divisors,  $\rho = 1$  if and only if  $t = 3$  so  $fh = pq$ . Here the nontrivial odd principal divisors must necessarily be  $\pm p$  and  $\pm q$ .

It should be noted that the requirement  $\rho \neq 0$  in Corollaries 2 and 3 cannot be dropped. For example, when  $fh = 321 = 3 \cdot 107$  the field  $k_1$  has class number 3 and  $\mathfrak{p}_2$  belongs to an ideal class of order 3. Hence  $K_1/k_1$  never has an integral basis when  $g$  is odd.

## Chapter IV: STEINITZ CLASSES OF ORDER 2 IN QUADRATIC AND QUARTIC FIELDS

### §1. Introduction.

If an extension  $M/K$  of number fields has an integral basis then its relative discriminant  $\Delta_{M/K}$  must be principal. Since the converse is false, this gives rise to the question: Given a number field  $K$ , does there exist an extension  $M$  of  $K$  such that  $\Delta_{M/K}$  is principal, but  $M/K$  has no integral basis?

If  $d$  is the discriminant of any  $K$  basis for  $M$  then  $\Delta_{M/K} = B^2(d)$  for some ideal  $B$  of  $K$ . The ideal class of  $B$  is called the Steinitz class of  $M$  with respect to  $K$ . Artin [1] has shown that  $M$  has a relative integral basis over  $K$  if and only if the Steinitz class for  $M/K$  is principal. Since  $\Delta_{M/K}$  is principal whenever the Steinitz class of  $M/K$  has order 1 or 2, the question can be rephrased as: Does there exist an extension  $M/K$  having Steinitz class of order 2?

In [20], Pierce claims to have shown that if  $K$  is a quadratic or normal quartic number field with even class number and  $l \equiv 3 \pmod{4}$  is a prime then there exists a normal extension  $M/K$  of degree  $l$  which has no integral basis, but  $\Delta_{M/K}$  is principal. If such a field  $M$  exists, Pierce says  $K$  has property (\*) with respect to  $l$ . We shall also refer to the conditions in this manner. In this article, the primary concern is whether or not  $K$  has (\*) for primes  $l \equiv 1 \pmod{4}$ , but the main results are valid for all odd primes. For quadratic and cyclic quartic fields, new proofs of Pierce's results are given. However, in the case of bicyclic, biquadratic fields, we discovered Pierce's result was not quite correct. A corrected version of his result is given in the last section of this article.

### §2. Notation and Terminology.

$K$ : Algebraic number field.

$l$ : Odd rational prime which does not divide  $[K : \mathbb{Q}]$ .



$H \approx Z_{2^{b_1}} \times Z_{2^{b_2}} \times \cdots \times Z_{2^{b_n}} \times H'$ : Ideal class group of  $K$  where  $b_1 \geq b_2 \geq \cdots \geq b_n$  and  $H'$  is the maximal subgroup of  $H$  of odd order.

$C_1, C_2, \dots, C_n$ : Basis for the 2-Sylow subgroup of  $H$  so that  $C_i$  generates a cyclic subgroup of  $H$  of order  $2^{b_i}$ .

$A_i$ : Prime ideal of  $K$  in  $C_i$ .

$(a_i) = A_i \cap Q$ .

$H_1$ : Subgroup of  $H$  that consists of all elements  $C$  such that  $C^{(l-1)/2}$  has odd order.

$K'$ : 2-part of the Hilbert class field of  $K$ .

$K_1$ : Subfield of  $K'$  corresponding to  $H_1$ .

$\Delta_{M/N}$ : Discriminant for  $M/N$ .

$l-1 = 2^{e_0} l_0$ .

$\zeta$ : Primitive  $l$ -th root of unity.

$2^{e_1} l_1, 2^e r$ : Ramification indices of  $l$  in  $K$  and  $K(\zeta)$  respectively where  $l_1$  and  $r$  are odd.

$2^{e_2} l_2 = [K(\zeta) : K]$  where  $l_2$  is odd.

$\mathcal{L}$ : a prime ideal of  $K(\zeta)$  lying over  $(l)$ .

$L = \mathcal{L} \cap K$ .

$\nu_2$ : the 2-adic valuation on  $Q$ .

### §3. Preliminary Results.

In [16], Long showed that for a fixed odd prime  $l$ , an ideal class of  $K$  is a Steinitz class for some normal extension of degree  $l$  over  $K$  if and only if it is of the form  $C^{(l-1)/2}$  where  $C$  is a class containing a prime divisor of  $l$  or a prime of  $K$  which splits completely in  $K(\zeta)$ . He also showed that the classes of  $K$  which are Steinitz classes for some normal extension of degree  $l$  form a subgroup of the ideal class group of  $K$ . Hence,  $K$  has (\*) for  $l$  if and only if this subgroup contains an element of even order.

PROPOSITION 1. If  $e_0 > b_1$  then  $K$  does not have property (\*) with respect to  $l$ . (Here  $l$  may divide  $[K : Q]$ .)

PROOF: If  $C \in H$  then  $C^{(l-1)/2}$  has odd order. Hence  $K$  does not have (\*) with respect to  $l$ .

For the remainder of the article  $K/Q$  will be a normal extension. Let  $I$  and  $I_0$  denote the inertia fields for  $\mathcal{L}$  over  $Q$  and  $K$  respectively and  $I_1$  denote the inertia field for  $L$  over  $Q$ .

LEMMA 2. *The inertia fields satisfy  $I \cap K = I_1$  and  $IK = I_0$ .*

PROOF: Let  $L_1 = L \cap I_1 = \mathcal{L} \cap I_1$ . Since  $L_1$  is unramified over  $Q$ ,  $I_1 \subseteq I$ . Since  $L_1$  ramifies totally in  $K$ ,  $I_1 = I \cap K$ . Since  $K/I_1$  is a normal extension,  $[IK : K] = [I : I_1]$ . Since  $I/I_1$  is a normal extension,  $L_1$  does not ramify in  $I$ . Thus the different of  $I/I_1$  is relatively prime to  $L_1$ . Since the different of  $IK/K$  divides the different of  $I/I_1$ , it is also relatively prime to  $L_1$ . In particular,  $L$  does not ramify in  $IK$ , so  $IK \subseteq I_0$ . Suppose  $IK \subsetneq I_0$ . Let  $\mathcal{L}_0 = \mathcal{L} \cap I_0$  and let  $I'$  denote the inertia field of  $\mathcal{L}_0$  over  $I$ . Since  $\mathcal{L}_0$  is unramified over  $IK$ ,  $[I' : I] \geq [I_0 : IK] > 1$ . But  $\mathcal{L}_0 \cap I'$  is unramified over  $Q$ , so  $I' = I$ . Thus  $IK = I_0$ .

LEMMA 3. *The 2-part of the ramification index of  $\mathcal{L}$  over  $Q$  is determined by  $e = \max\{e_0, e_1\}$ .*

PROOF: Since  $l \nmid [K : Q]$ ,  $G(IK/I) \simeq G(K/I_1)$  is cyclic of order  $2^{e_1}l_1$ . Hence there exists a unique subfield  $J'$  of  $IK$  with  $I \subseteq J'$  and  $[J' : I] = l_1$ . Since  $\mathcal{L} \cap I$  is unramified over  $Q$  and  $(l)$  is totally ramified in  $Q(\zeta)$ ,  $I \cap Q(\zeta) = Q$ . Thus  $[I(\zeta) : I] = l - 1$  and some prime divisor of  $(l)$  in  $I$  ramifies totally in  $I(\zeta)$ . Since  $l \nmid [K(\zeta) : Q]$ ,  $G_1 = G(K(\zeta)/I)$  is cyclic and hence  $G_1 \simeq Z_{2^e} \times Z_r$ . Since  $l_1 = [J' : I]$  is odd and  $2^{e_0} \mid l - 1 = [I(\zeta) : I]$ ,  $2^{e_0} \mid [J'(\zeta) : J']$ . Also,  $2^e \mid [K(\zeta) : I]$  implies  $2^e \mid [K(\zeta) : J']$ . Since  $G_1$  is cyclic there exist unique subfields  $J_0 \subseteq J'(\zeta)$  and  $J \subseteq K(\zeta)$  with  $[J_0 : J'] = 2^{e_0}$  and  $[J : J'] = 2^e$ . Because  $e \geq \max(e_0, e_1)$ ,  $J_0 \subseteq J$  and  $IK \subseteq J$ . Also, since  $[J'(\zeta) : J']$  is a divisor of  $\phi(l) = 2^{e_0}l_0$ ,  $[J_0(\zeta) : J_0] = [J'(\zeta) : J_0]$  is a divisor of  $l_0$  and hence is odd.

Since  $G(J/J') \simeq Z_{2^e}$ , either  $IK \subseteq J_0$  or  $J_0 \subseteq IK$ . If  $J_0 \subseteq IK$  then  $[J_0(\zeta) \cap IK : J_0]$  is both odd and a power of 2. Thus  $J_0(\zeta) \cap IK = J_0$  and so  $[K(\zeta) : IK] = [J_0(\zeta) : J_0]$  is odd.

Hence  $e = \nu_2[K(\zeta) : I] = \nu_2[IK : I] = e_1$ . If  $IK \subseteq J_0$ , then  $K(\zeta) \subseteq J_0(\zeta) = J'(\zeta) \subseteq K(\zeta)$ , so  $J'(\zeta) = K(\zeta)$ . In this case,  $e_0 = \nu_2[J'(\zeta) : I] = \nu_2[K(\zeta) : I] = e$ .

LEMMA 4. *Let  $K \subseteq F \subseteq K(\zeta)$  with  $[F : K] = 2^d$ . Then  $L$  does not ramify in  $F$  if and only if  $d \leq e_1 + e_2 - e$ .*

PROOF: If  $e(\mathcal{L}/L)$  denotes the ramification index of  $\mathcal{L}$  over  $L$  then  $\nu_2(e(\mathcal{L}/L)) = e - e_1$ . If  $\hat{I}$  is the largest subfield of  $I_0$  which contains  $K$  with  $[\hat{I} : K]$  being a power of 2 then  $[\hat{I} : K] = 2^{e_1 + e_2 - e}$ . Since  $G(K(\zeta)/K)$  is cyclic,  $d \leq e_1 + e_2 - e$  if and only if  $F \subseteq \hat{I}$ . But  $F \subseteq \hat{I}$  if and only if  $F \subseteq I_0$  if and only if  $L$  does not ramify in  $F$ .

COROLLARY 5. *If  $e_0 \leq e_1$  and  $K \subseteq F \subseteq K(\zeta)$  with  $[F : K] = 2^d$  then  $F/K$  is unramified at  $(l)$ .*

PROOF: Since  $e_0 \leq e_1$ ,  $e = e_1$  so  $e_1 + e_2 - e = e_2$ . Since  $[K(\zeta) : K] = 2^{e_2} l_2$  with  $l_2$  odd,  $d \leq e_2$  so Lemma 4 applies.

COROLLARY 6. *If  $Q(\zeta) \cap K = Q$  and  $K \subseteq F \subseteq K(\zeta)$  with  $[F : K] = 2^d$  where  $d \leq e_1$  then  $F/K$  is unramified at  $(l)$ .*

PROOF: Since  $Q(\zeta) \cap K = Q$ ,  $e_2 = e_0$  so  $e_1 + e_2 - e = \min(e_1, e_2)$  by Lemma 3. Since  $d \leq e_1$  and  $d \leq e_2$ , Lemma 4 applies.

LEMMA 7. *When  $e_0 \leq b_1$ ,  $K$  does not have  $(*)$  with respect to  $l$  if and only if  $K_1 \subseteq K(\zeta)$  and  $L^{(l-1)/2}$  is in a class of odd order for all prime divisors  $L$  of  $(l)$  in  $K$ .*

PROOF: By Long [9] we need only show that  $K_1 \subseteq K(\zeta)$  if and only if  $P^{(l-1)/2}$  is in a class of odd order for all prime ideals  $P$  of  $K$  which split completely in  $K(\zeta)$ . Now,  $K_1 \subseteq K(\zeta)$  if and only if the set of primes which split completely in  $K(\zeta)$  also split completely in  $K_1$ . Since a prime  $P$  of  $K$  splits completely in  $K_1$  if and only if  $P^{(l-1)/2}$  belongs to a class of odd order, the result follows.

THEOREM 8. *If  $b_2 \geq e_0$  or  $b_1 \geq e_0 + e_1 + e_2 - e$  then  $K$  has  $(*)$  with respect to  $l$ .*

PROOF: If not then by Lemma 7,  $K_1 \subseteq K(\zeta)$ . Since  $G(K(\zeta)/K)$  is cyclic, it follows that  $H/H_1$  is cyclic. Since  $H_1 \simeq \sum_{b_i > e_0 - 1} 2^{b_i - e_0 + 1} Z_{2^{b_i}} \times \sum_{b_i \leq e_0 - 1} Z_{2^{b_i}} \times H'$  and  $H/H_1$  is cyclic, it follows that  $b_2 \leq e_0 - 1$  and  $\nu_2([H : H_1]) = b_1 - e_0 + 1 \leq e_1 + e_2 - e$  by Lemma 4. The result now follows.

COROLLARY 9. *If  $L$  ramifies totally in  $K(\zeta)$  and  $b_1 \geq e_0$  then  $K$  has (\*) with respect to  $l$ .*

PROOF: Since  $L$  ramifies totally in  $K(\zeta)$ ,  $e = e_1 + e_2$ . Thus  $e_0 = e_0 + e_1 + e_2 - e$ , so Theorem 8 applies.

COROLLARY 10. *If  $e = e_1 + e_2$  and  $b_1 \geq e_0$  then  $K$  has (\*) with respect to  $l$ .*

COROLLARY 11. *If  $l$  does not ramify in  $K$  and  $b_1 \geq e_0$  then  $K$  has (\*) with respect to  $l$ .*

PROOF: Immediate from Corollary 9.

COROLLARY 12. *Let  $M$  be the subfield of  $Q(\zeta)$  such that  $[M : Q] = 2^{e_0}$ . If  $M \subseteq K$  and  $b_1 \geq e_0$  then  $K$  has (\*) with respect to  $l$ .*

PROOF: If  $M \subseteq K$  then  $e_1 = e$  and  $e_2 = 0$  so Corollary 10 applies.

THEOREM 13. *Let  $K$  be imaginary and  $H \simeq Z_{2^b} \times H'$  with  $0 \leq b - e_0 + 1 \leq e_1 + e_2 - e$ . Then  $K$  does not have (\*) with respect to  $l$  if and only if  $L^{(l-1)/2}$  is in a class of odd order.*

PROOF: Let  $J_0$  denote the maximal subfield of  $I_0$  which has degree a power of 2 over  $K$ . Then  $J_0 \subseteq K'$  and  $[J_0 : K] = 2^{e_1 + e_2 - e}$ . Since  $[K_1 : K] = 2^{b - e_0 + 1}$  with  $b_1 - e_0 + 1 \leq e_1 + e_2 - e$  and  $G(K'/K)$  is cyclic,  $K_1 \subseteq J_0 \subseteq K(\zeta)$ . By Lemma 7,  $K$  does not have (\*) with respect to  $l$  if and only if  $L^{(l-1)/2}$  is in a class of odd order.

COROLLARY 14. *Let  $K$  be real and  $H \simeq Z_{2^b} \times H'$  with  $0 \leq b - e_0 + 1 \leq e_1 + e_2 - e$ . If  $e_1 < e$  or  $b - e_0 + 1 < e_1 + e_2 - e$  then  $K$  does not have (\*) with respect to  $l$  if and only if  $L^{(l-1)/2}$  is in a class of odd order. If  $e_1 = e$  and  $b - e_0 + 1 = e_2$  then  $K$  has (\*) with respect to  $l$ .*

PROOF: If  $e_1 < e$  then  $e_1 + e_2 - e < e_2$  so  $J_0$  is real and the proof of Theorem 13 applies. If  $b - e_0 + 1 < e_1 + e_2 - e$  then  $J_0$  can be replaced with its maximal real subfield in the proof

of Theorem 13. If  $e_1 = e$  and  $b - e_0 + 1 = e_2$  then  $[K_1 : K] = [J_0 : K] = 2^{e_2}$ . Thus  $J_0$  is the maximal subfield of  $K(\zeta)$  with degree over  $K$  equal to a power of 2. Hence  $J_0$  is imaginary. Since  $K_1$  is real,  $K_1 \not\subseteq K(\zeta)$  so by Lemma 7,  $K$  has (\*) with respect to  $l$ .

**THEOREM 15.** Assume that  $L^{(l-1)/2}$  is in a class of odd order. Suppose  $b_1 > b_2 > 0$ ,  $b_2 < e_0$ , and  $b_1 = e_0 + t$  with  $0 \leq t < e_2 - 1$  when  $e_1 = e$  and  $K$  is real, and  $0 \leq t < e_2 + e_1 - e$  otherwise. Let  $K_0$  be the unique subfield of  $K' \cap K(\zeta)$  with  $[K_0 : K] = 2^{t+1}$  and  $H_0$  be the subgroup of  $H$  corresponding to  $K_0$ . Then  $K$  has (\*) with respect to  $l$  if and only if  $H_0$  contains an element of order  $2^{e_0}$ .

**PROOF:** Since  $b_1 = e_0 + t$  and  $b_2 < e_0$ ,

$$\begin{aligned} H_1 &\approx 2^{t+1} Z_{2^{b_1}} \times Z_{2^{b_2}} \times \cdots \times Z_{2^{b_n}} \times H' \\ &\approx Z_{2^{b_1-t-1}} \times Z_{2^{b_2}} \times \cdots \times Z_{2^{b_n}} \times H'. \end{aligned}$$

Now  $[H : H_1] = 2^{t+1} = [H : H_0]$  and  $K' \cap K(\zeta)/K$  is a cyclic extension. By Lemma 7,  $K$  has (\*) with respect to  $l$  if and only if  $K_1 \neq K_0$  or equivalently,  $H_1 \neq H_0$ . But  $|H_0| = |H_1|$ , so  $H_0 \neq H_1$  if and only if  $H_0$  contains an element of order  $2^{b_1-t} = 2^{e_0}$ .

**PROPOSITION 16.** Assume that  $L^{(l-1)/2}$  is in a class of odd order. Suppose  $K$  is real,  $e_1 = e$ ,  $b_1 > b_2 > 0$  and  $b_2 < e_0 = b_1 - e_2 + 1$ . Then  $K$  has (\*) with respect to  $l$ .

**PROOF:** Let  $K_0$  be the subfield of  $K(\zeta)$  such that  $[K_0 : K] = 2^{e_2}$ . From the proof of Theorem 15,  $[K_1 : K] = 2^{e_2}$ . By Lemma 7 it follows that  $K$  has (\*) with respect to  $l$  if and only if  $K_1 \neq K_0$ . But  $K_0$  is imaginary so  $K_0/K$  is a ramified extension. Hence  $K_1 \neq K_0$ .

**COROLLARY 17.** If in addition to the hypothesis of Theorem 15,  $[K_0 : K] = 2$  then  $K$  has (\*) with respect to  $l$  if and only if  $A_i$  stays prime in  $K_0$  for some  $i > 1$ .

**PROOF:** Note that  $A_i$  stays prime in  $K_0$  for some  $i$  if and only if  $C_i \notin H_0$ . So  $A_j$  stays prime in  $K_0$  for some  $j$  with  $b_j = b_i$  if and only if  $H_0$  contains fewer elements of order  $2^{b_i}$ .

than  $H$ . Since  $[H : H_0] = 2$  this is true if and only if  $H_0$  has an element of order  $2^{b_1}$ . The result now follows from Theorem 15.

For the remainder of the article  $K_0$  and  $H_0$  will be as defined in Theorem 15.

#### §4. Quadratic Fields.

In this section we specialize to the case where  $K = Q(\sqrt{d})$  is a quadratic field. If  $b_1 < e_0$  then Proposition 1 shows that  $K$  does not have (\*) with respect to  $l$ . If  $b_1 \geq e_0$  and  $l$  does not ramify in  $K$  then Corollary 9 shows that  $K$  has (\*) with respect to  $l$ . Hence we may assume that  $l$  divides  $d$ , which will be assumed to hold for the remainder of this section. Thus we have  $e_1 = 1$ ,  $e = e_0$  and  $e_2 = e_0 - 1$  or  $e_0$  according as  $K \subseteq Q(\zeta)$  or not. Set  $\delta = 0$  or 1 according as  $K \subseteq Q(\zeta)$  or not. If  $b_1 \geq e_0 + \delta$  then Theorem 8 shows that  $K$  has (\*) with respect to  $l$ . Thus we need only consider the case  $b_1 = e_0$  and  $K \not\subseteq Q(\zeta)$ . When  $l \equiv 3 \pmod{4}$ ,  $e_0 = 1$  and Theorem 8 shows that  $K$  has (\*) with respect to  $l$  unless  $H \simeq Z_2 \times H'$ . Assuming  $H$  has this form, Corollary 14 shows that  $K$  has (\*) for  $l$  when  $K$  is real. If  $K$  is imaginary then  $K = Q(\sqrt{-ld_1})$  where  $d_1 > 1$ , so  $L$  and hence  $L^{(l-1)/2}$  belongs to a class of order 2. Theorem 13 shows that  $K$  has (\*) for  $l$ . This is Pierce's result for quadratic fields.

If  $l \equiv 1 \pmod{4}$ ,  $b_1 = e_0$ ,  $b_2 = 0$ ,  $e_2 = e_0$  and  $e_1 = 1$  then  $L^{(l-1)/2}$  is principal. Thus Theorem 13 or Corollary 14 applies to show  $K$  does not have (\*) with respect to  $l$ .

For the remainder of this section we shall assume that  $l \equiv 1 \pmod{4}$ ,  $b_1 = e_0$ ,  $0 < b_2 < e_0$  and  $l$  ramifies in  $K$ , but  $K \neq Q(\sqrt{l})$ . It follows that  $K(\sqrt{l})/K$  is an unramified extension and that  $K(\sqrt{l})$  is the field  $K_0$  described in Theorem 15.

**PROPOSITION 18.**  *$K$  has (\*) with respect to  $l$  if and only if the subgroup  $H_0$  of  $H$  corresponding to  $K_0$  contains an element of order  $2^{b_1}$ .*

**PROOF:** This is immediate from Theorem 15.

**THEOREM 19.**  *$K$  has (\*) with respect to  $l$  if and only if  $\left(\frac{l}{a_i}\right) = -1$  for some  $i > 1$ .*

**PROOF:** First assume that  $\left(\frac{l}{a_i}\right) = -1$  for some  $i > 1$ . If  $\left(\frac{l}{a_1}\right) = 1$  then  $C_1$  belongs to  $H_0$ ,

so  $H_0$  contains a class of order  $2^{b_1}$ . Thus  $K$  has (\*) with respect to  $l$ . If  $\left(\frac{l}{a_1}\right) = -1$  then neither  $A_1$  nor  $A_i$  split completely in  $K(\sqrt{l})$ , so neither  $C_1$  nor  $C_i$  belongs to  $H_0$ . Since  $[H : H_0] = 2$ ,  $C_1 C_i$  belongs to  $H_0$  and  $C_1 C_i$  has order  $2^{b_1}$ . As above  $K$  has (\*) with respect to  $l$ .

Conversely, assume that  $\left(\frac{l}{a_i}\right) = 1$  for  $2 \leq i \leq n$ . Thus, for each  $i > 1$ ,  $C_i$  belongs to  $H_0$ . If  $H_0$  contains an element of order  $2^{b_1}$  then  $H_0 = H$ , contradicting that  $[H : H_0] = 2$ . Thus  $H_0$  contains no element of order  $2^{b_1}$  and hence  $K$  does not have (\*) with respect to  $l$ .

REMARK. If  $l \equiv 5 \pmod{8}$  we need only use Theorem 19 when  $H \simeq Z_4 \times Z_2 \times \cdots \times Z_2 \times H'$ . In this case  $C_2, \dots, C_n$  are ambiguous classes which are not in the principal genus. If 2 ramifies in  $K$  then since  $\left(\frac{2}{l}\right) = -1$ ,  $K$  does have (\*) for  $l$ . There are numerous examples where this happens, for example  $d = -65$  and  $l = 5$  or  $13$ . Here  $H \simeq Z_4 \times Z_2$ . For  $d = -2755 = -5 \cdot 19 \cdot 29$ ,  $H = Z_4 \times Z_2$  and  $K$  does not have (\*) for  $l = 5$ , but has it for  $l = 29$ .

COROLLARY 20. The imaginary quadratic field  $K = Q(\sqrt{-d})$  has (\*) for the prime  $l$  if and only if  $x^2 + dy^2 = 4^j d_0 z^{2^a}$  has a solution with  $d_0 \mid \Delta_{K/Q}$ ,  $d_0$  square free  $1 \neq d_0 \neq d$ ,  $(z, \Delta_{K/Q}) = 1$ ,  $\left(\frac{l}{z}\right) = -1$ ,  $(x, y) = 1$ ,  $j = 0$  or  $1$  and  $a < b_2$ . If  $\Delta_{K/Q}$  is even then  $j = 0$ .

PROOF: If  $K$  has (\*) with respect to  $l$  then Theorem 19 shows there exists a prime  $p$  which has a prime factor  $\mathfrak{p}$  in  $K$  belonging to an ideal class of order  $2^b$  with  $b \leq b_2$  and  $\left(\frac{l}{p}\right) = -1$ . Thus  $\mathfrak{p}^{2^{b-1}}$  belongs to an ambiguous class of  $K$ , so  $\mathfrak{p}^{2^a} I = \left(\frac{x+y(\sqrt{-d})}{2^j}\right)$  where  $a = b - 1$ ,  $I$  is an ambiguous ideal and  $x, y \in Z$ . Taking norms gives

$$x^2 + dy^2 = 4^j d_0 p^{2^a}$$

where  $d_0$  is the norm of  $I$ . Since  $I$  is an ambiguous ideal it can be chosen with  $d_0 \mid \Delta_{K/Q}$ . Since  $\mathfrak{p}^{2^a}$  is not principal, neither is  $I$ , so  $d_0 \neq 1$  and  $d_0 \neq d$ . Since  $\mathfrak{p}$  was any ideal belonging to the given class, it can be chosen relatively prime to  $\Delta_{K/Q}$ . Since we may choose  $I$  to be

a square free ideal,  $d_0$  will be square free. Suppose some prime  $q$  divides both  $x$  and  $y$ . If  $q = 2$  then  $j = 0$ . Thus  $q^2 \mid d_0 p^{2^a}$ , so  $q \mid p$  and hence  $q = p$ . Thus  $p \mid p^{2^a} I$ , so  $p \mid p^{2^a}$  since  $p \nmid \Delta_{K/Q}$ . But  $p$  belongs to a class of order  $2^b > 1$ , so  $p$  splits completely in  $K$ . Thus  $p \nmid p^{2^a}$  so  $(x, y) = 1$ .

Conversely, assume the quadratic form has a solution. Let  $z = p_1^{c_1} \dots p_t^{c_t}$  where  $p_1, \dots, p_t$  are distinct primes. Since  $x^2 \equiv -dy^2 \pmod{p_i}$  and  $p_i \nmid \Delta_{K/Q}$ , each prime splits completely in  $K$ . Say  $(p_i) = \mathfrak{p}_{i_1} \mathfrak{p}_{i_2}$ . Now  $(d_0) = I^2$  for some ideal of  $K$  and  $\left(\frac{x+\sqrt{-dy}}{2}\right) = IB$  for some ideal  $B$  of  $K$  having norm  $z^{2^a}$ . If  $(p_i) \mid B$  then  $x \equiv y \equiv 0 \pmod{p_i}$  contradicting that  $(x, y) = 1$ . Thus after renumbering the prime ideals

$$B = (\mathfrak{p}_{1_1}^{c_1} \cdot \mathfrak{p}_{2_1}^{c_2} \dots \mathfrak{p}_{t_1}^{c_t})^{2^a} = A^{2^a}.$$

Now  $A^{2^a} I \sim (1)$  so  $A^{2^a} \sim I$ . Hence  $A$  belongs to an ideal class of order  $2^{a+1}$ . Since  $\left(\frac{l}{z}\right) = -1$ , the class of  $A$  does not belong to  $H_0$ . Since  $[H : H_0] = 2$  and  $a + 1 < b_1$ ,  $H_0$  contains a class of order  $2^{b_1}$ . Theorem 15 shows that  $K$  has (\*) with respect to  $l$ .

Using the table of Oriat [18], we have determined whether or not  $Q(\sqrt{-d})$ , with  $1 \leq d \leq 24572$ , has (\*) with respect to  $l$  for all primes  $l \equiv 1 \pmod{8}$  which divide  $d$  with  $l \equiv 1 + 2^{b_1} \pmod{2^{b_1+1}}$  and  $1 < b_2 < e_0$ . Note the case  $b_2 = 1$  can easily be decided by Theorem 19. In the range of the table  $b_2 = 2$ . Hence there exist primes  $p$  and  $q$  with  $q \mid \Delta_{K/Q}$  and  $\left(\frac{p}{q}\right) = -1$  such that the quadratic form in Corollary 20 has a solution with  $z = p$  and  $a = 1$ . If  $\left(\frac{l}{p}\right) = -1$  then Corollary 20 shows that  $Q(\sqrt{-d})$  has (\*) with respect to  $l$ . Assume  $\left(\frac{l}{p}\right) = +1$ , then any prime divisor  $\mathfrak{p}$  of  $p$  in  $K$  belongs to  $H_0$ , but is not in the principal genus. If the 2-rank of  $H$  is 2 then  $H_0$  contains no element of order  $2^{b_1}$  so  $K$  does not have (\*) with respect to  $l$ . When the 2-rank of  $H$  is 3, we need to determine whether or not  $C_3$  belongs to  $H_0$ . In the range of the table  $b_3 = 1$ , so there exists an ambiguous ideal  $A$  for  $K/Q$  which is not in the principal genus. Let  $\alpha = N_{K/Q}(A)$ . If  $\left(\frac{l}{\alpha}\right) = -1$  then  $K$  has (\*) with respect to  $l$  by Theorem 19 while if  $\left(\frac{l}{\alpha}\right) = +1$  then it follows from Proposition 18



that  $K$  does not have (\*) with respect to  $l$ .

$d$	Invariants of $H$	$l$	$d_0$	$p$	$j$	$z$	$y$	$\left(\frac{l}{p}\right)$	$q$	$\alpha$	(*)
2329	(4,8)	137	2	43	0	37	1	-1			Yes
3262	(4,8)	233	34	17	0	28	1	-1			Yes
3358	(4,8)	73	23	13	0	23	1	-1			Yes
3934	(4,8)	281	14	41	0	140	1	-1			Yes
4633	(4,8)	41	82	23	0	41	3	1	113		No
4658	(4,16)	17	17	109	0	357	4	-1			Yes
4718	(4,16)	337	14	29	0	84	1	-1			Yes
4777	(4,16)	281	17	37	0	136	1	-1			Yes
5134	(4,8)	17	2	53	0	22	1	1	151		No
5986	(4,8)	41	2	71	0	64	1	-1			Yes
5986	(4,8)	73	2	71	0	64	1	1	41		No
6953	(4,16)	17	2	59	0	3	1	1	409		No
7769	(4,8,3)	457	2	107	0	123	1	1	17		No
8322	(2,4,8)	73	73	23	0	73	2	1	3	3	No
8638	(4,8)	617	34	29	0	56	1	-1			Yes
8738	(4,16)	17	17	47	0	51	2	1	257		No
9214	(4,16)	17	17	71	0	221	2	-1			Yes
9554	(4,8,5)	281	2	93	0	88	1	-1			Yes
10001	(4,8,5)	73	2	71	0	9	1	1	137		No
10001	(4,8,5)	137	2	71	0	9	1	-1			Yes
10074	(2,4,8)	73	46	37	0	230	1	1	23	23	No
10549	(2,4,8)	137	22	23	0	33	1	-1			Yes
10961	(4,32)	97	194	43	0	291	5	1	113		No
11326	(4,8,3)	809	7	41	0	21	1	-1			Yes
12206	(4,16,3)	17	34	173	0	170	9	-1			Yes
12505	(2,4,8)	41	5	59	0	70	1	1	61	2	No
12937	(4,8)	761	17	43	0	136	1	-1			Yes
13022	(4,16)	17	17	83	0	255	2	1	383		No
13073	(4,16)	17	17	67	0	187	3	1	769		No
13143	(4,16)	336	3	67	0	18	1	-1			Yes
13359	(4,8,3)	73	3	71	0	42	1	1	61		No
13906	(4,16)	17	17	73	0	187	2	-1			Yes
15538	(4,16)	17	34	41	0	204	1	-1			Yes
15742	(4,16)	17	17	61	0	17	2	-1			Yes
16814	(4,16,3)	1201	2	107	0	78	1	-1			Yes
18649	(4,16)	17	17	37	0	68	1	-1			Yes
18721	(4,32)	97	194	103	0	1261	5	1	193		No
20658	(2,4,8)	313	22	31	0	22	1	-1			Yes
20734	(4,8,3)	1481	2	103	0	22	1	-1			Yes
21243	(4,8)	73	73	23	1	365	1	1	97		No
22654	(4,16)	241	47	23	0	47	1	-1			Yes
23137	(4,16)	17	34	37	0	153	1	-1			Yes
23137	(4,16)	1361	34	37	0	153	1	-1			Yes
23377	(4,16)	241	194	13	0	97	1	-1			Yes
23871	(4,8,3)	73	109	103	0	545	6	-1			Yes

## §5. Cyclic Quartic Fields.

In this section we consider the case where  $K$  is a cyclic quartic extension of  $Q$  and  $k$  is its unique quadratic subfield.

PROPOSITION 21. If  $K \subseteq Q(\zeta)$  or  $l \nmid \Delta_{K/Q}$  then  $K$  has (\*) with respect to  $l$  if and only if  $b_1 \geq e_0$ . If  $Q(\sqrt{l}) \subseteq K \not\subseteq Q(\zeta)$  or  $l \nmid \Delta_{k/Q}$  but  $l \mid \Delta_{K/Q}$  and  $b_1 \neq e_0$ , then  $K$  has (\*) with respect to  $l$  if and only if  $b_1 > e_0$ . If  $Q(\sqrt{l}) \neq k$ , but  $l \mid \Delta_{k/Q}$  and  $b_1 \neq e_0$  or  $e_0 + 1$  then  $K$  has (\*) with respect to  $l$  if and only if  $b_1 > e_0 + 1$ .

PROOF: If  $l \equiv 3 \pmod{4}$  then  $e_1 \leq 1$ , so in all cases it follows from Lemma 3 that  $e = e_0$ . Thus  $e_0 + e_1 + e_2 - e = e_1 + e_2$ . If  $K \subseteq Q(\zeta)$  then  $e_1 = 2$  and  $e_2 = e_0 - 2$  so  $e_1 + e_2 = e_0$ . Similarly, when  $l \nmid \Delta_{K/Q}$ ,  $e_1 = 0$  and  $e_2 = e_0$  so  $e_1 + e_2 = e_0$ . If  $Q(\sqrt{l}) \subseteq K \not\subseteq Q(\zeta)$  then  $e_1 = 2$ ,  $e_2 = e_0 - 1$  so  $e_1 + e_2 = e_0 + 1$ . When  $l \nmid \Delta_{k/Q}$ , but  $l \mid \Delta_{K/Q}$ ,  $e_1 = 1$  and  $e_2 = e_0$  so  $e_1 + e_2 = e_0 + 1$ . When  $l \mid \Delta_{k/Q}$  and  $Q(\sqrt{l}) \neq k$  then  $e_1 = 2$ ,  $e_2 = e_0$  so  $e_1 + e_2 = e_0 + 2$ . The results are now immediate from Theorem 8 and Proposition 1.

COROLLARY 22. Assume the 2-class group of  $K$  is cyclic,  $b_1 = e_0$ ,  $l$  is totally ramified in  $K$ , but  $K \not\subseteq Q(\zeta)$ . Then  $K$  has (\*) with respect to  $l$  if and only if  $l \equiv 5 \pmod{8}$  and the prime divisor of  $l$  in  $k$  belongs to a class of even order or  $K$  is real with  $e = e_1$ , and  $e_2 = 1$ .

PROOF: It follows from Theorem 13 and Corollary 14 that  $K$  has (\*) with respect to  $l$  if and only if  $L^{(l-1)/2}$ , or equivalently  $L^{2^{e_0-1}}$ , belongs to a class of even order in  $K$  or  $K$  is real and  $e = e_1$  and  $e_2 = 1$ . Since  $l$  is totally ramified in  $K$ ,  $l \equiv 1 \pmod{4}$ . Thus the condition can only be fulfilled when  $l \equiv 5 \pmod{8}$  and  $L^2$  belongs to a class of even order. But  $L^2$  is an ideal of  $k$ .

Note that by Corollary 14, if  $e_1 = e$  and  $e_2 = 1$ ,  $K$  has (\*) with respect to  $l$ . The result now follows.

COROLLARY 23. Assume the 2-class group of  $K$  is cyclic,  $b_1 = e_0 + 1$ ,  $l \mid \Delta_{k/Q}$  but  $k \neq Q(\sqrt{l})$ . Then  $K$  has (\*) with respect to  $l$  if and only if  $l \equiv 5 \pmod{8}$  and the prime divisor of  $l$  in  $k$  belongs to a class of even order or  $K$  is real with  $e = e_1$  and  $e_2 = 2$ .

PROOF: Same as the previous Corollary.

COROLLARY 24. Assume the 2-class group of  $K$  is cyclic,  $b_1 = e_0$ ,  $l \mid \Delta_{K/Q}$ , but  $l \nmid \Delta_{k/Q}$ . If  $l \equiv 1 \pmod{4}$  and  $l$  stays prime in  $k$  then  $K$  does not have (\*) with respect to  $l$ .

PROOF: Since  $L^{(l-1)/2} = (l)^{(l-1)/4}$  is principal, Theorem 13 or Corollary 14 applies to show  $K$  has (\*) with respect to  $l$ .

Pierce's result [20] is now easily obtained.

COROLLARY 25. If  $l \equiv 3 \pmod{4}$  then  $K$  has (\*) with respect to  $l$  if and only if  $K$  has even class number.

PROOF: Since  $l \equiv 3 \pmod{4}$ ,  $l \nmid \Delta_{k/Q}$ . Thus from Theorem 8 and Proposition 21, only the case  $l \mid \Delta_{K/Q}$ ,  $b_1 = 1$  and  $b_2 = 0$  remains. If  $K$  is real then Corollary 14 applies to show that  $K$  has (\*) with respect to  $l$ . Hence we may assume that  $K$  is imaginary. Here  $L$  is in a class of even order so it follows from Theorem 13 that  $K$  has (\*) with respect to  $l$ .

We now give eleven examples where  $l \equiv 5 \pmod{8}$  and the class group structure has been determined, in all but one case, by Brown and Parry [5,6] to satisfy the hypothesis of Corollary 17. In all these  $k$  has odd class number and it was shown in the articles referred to above that all ambiguous classes of  $K/k$  are strong.

For the first eight examples,  $K$  has the form  $Q(\sqrt{-d\epsilon\sqrt{p}})$  such that  $l \mid d$ ,  $p \nmid d$ ,  $p \neq l$  is a prime and  $\epsilon$  is the fundamental unit of  $Q(\sqrt{p})$ . In the last four examples,  $K = Q(\sqrt{-d\epsilon\sqrt{l}})$  with  $d = p$  or  $2p$  where  $p \neq l$  is a prime.

	$d$	Conditions	(*)
1.	$l$	$p \equiv 5 \pmod{8}$ , $\left(\frac{l}{p}\right)_4 = -\left(\frac{p}{l}\right)_4 = 1$	No
2.	$2l$	$p \equiv 5 \pmod{8}$ , $\left(\frac{l}{p}\right)_4 = -\left(\frac{p}{l}\right)_4 = -1$	No
3.	$lq$	$p \equiv 5 \pmod{8}$ , $q$ -prime, $q \equiv 1 \pmod{4}$ , $q \neq p$ or $l$ , $\left(\frac{q}{l}\right)_4 = \left(\frac{l}{q}\right)_4 = -\left(\frac{p}{l}\right)_4$ , $\left(\frac{q}{p}\right)_4 = 1$	No
4.	$lq$	$p \equiv 5 \pmod{8}$ , $q$ -prime, $q \equiv 1 \pmod{4}$ , $q \neq p$ or $l$ , $\left(\frac{q}{p}\right)_4 = \left(\frac{l}{q}\right)_4 = -\left(\frac{p}{q}\right)_4 = -\left(\frac{l}{p}\right)_4 = 1$	Yes
5.	$lq$	$p \equiv 1 \pmod{8}$ , $q$ -prime, $q \equiv 3 \pmod{4}$ , $q \neq p$ or $l$ , $\left(\frac{l}{p}\right)_4 \equiv \left(\frac{q}{l}\right)_4 = -\left(\frac{p}{l}\right)_4$ , $\left(\frac{q}{p}\right)_4 = -1$	No
6.	$l$	$p \equiv 1 \pmod{8}$ , $\left(\frac{l}{p}\right)_4 = -1$ , $\left(\frac{2}{p}\right)_4 = \left(\frac{2}{l}\right)_4 = (-1)^{(p+7)/8}$	Yes

	$d$	Conditions	(*)
7.	$lq$	$p = 2, q \equiv 1 \pmod{8}, \left(\frac{2}{p}\right)_4 \neq (-1)^{(p-1)/8} = \left(\frac{p}{2}\right), \left(\frac{2}{p}\right) = 1 = -\left(\frac{p}{2}\right)$	Yes
8.	$p$	$p \equiv 1 \pmod{4}, \left(\frac{p}{l}\right)_4 = -\left(\frac{l}{p}\right)_4 = 1$	No
9.	$2p$	$p \equiv 3 \pmod{4}, \left(\frac{-2}{p}\right) = \left(\frac{p}{2}\right)_4 = 1$	Yes
10.	$2p$	$p \equiv 1 \pmod{4}, \left(\frac{-2}{p}\right) = \left(\frac{p}{2}\right)_4 = -\left(\frac{l}{p}\right)_4$	Yes
11.	$p$	$p \equiv 3 \pmod{4}, \left(\frac{p}{l}\right)_4 = \left(\frac{2}{p}\right) = -1$	Yes

We prove examples 2 and 4. The proofs of examples 1, 3, 5 and 8 are similar to the proof of example 2, and the proofs of examples 6, 7, 9, 10 and 11 are similar to the proof of example 4.

In example 2,

$$H \approx Z_4 \times Z_2 \times Z_2 \times H'.$$

Let  $A, P, L_1$  and  $L_2$  be the prime ideals of  $K$  lying above 2,  $p$  and  $l$  respectively. By Corollary 17 we need to show  $A, P, L_1$  and  $L_2$  split completely in  $K(\sqrt{l}) = K(\sqrt{-2\epsilon\sqrt{p}})$ . Since  $\left(\frac{l}{p}\right) = 1$ ,  $p$  splits completely in  $Q(\sqrt{l})$  and so  $P$  splits completely in  $K(\sqrt{l})$ . Because  $l \cdot p \equiv 1 \pmod{8}$ , 2 splits completely in  $Q(\sqrt{l \cdot p})$ . Since 2 stays prime in  $Q(\sqrt{p})$  and ramifies in  $K$ ,  $A$  must split completely in  $K(\sqrt{l})$ .

Now  $l$  splits completely in  $Q(\sqrt{p})$  and ramifies in  $K$ . If we show  $l$  splits completely in  $Q(\sqrt{-2\epsilon\sqrt{p}})$  then  $L_1$  and  $L_2$  must split completely in  $K(\sqrt{-2\epsilon\sqrt{p}})$ . Since  $\left(\frac{l}{p}\right)_4 = -1$ ,  $l$  splits completely in  $Q(\sqrt{p})$  and gains degree two in  $Q(\sqrt{-\epsilon\sqrt{p}})$ . Because  $l \equiv 5 \pmod{8}$ ,  $l$  stays prime in  $Q(\sqrt{2})$ . Thus  $l$  does not split completely in  $Q(\sqrt{2}, \sqrt{p})$ . If  $l$  does not split completely in  $Q(\sqrt{-2\epsilon\sqrt{p}})$  then  $Q(\sqrt{p})$  is the decomposition field for  $l$  in the extension  $Q(\sqrt{2}, \sqrt{-\epsilon\sqrt{p}})/Q$ . Since  $Q(\sqrt{2}, \sqrt{-\epsilon\sqrt{p}})/Q(\sqrt{p})$  is not a cyclic extension  $l$  splits completely in  $Q(\sqrt{-2\epsilon\sqrt{p}})$ .

We now prove example 4. We first show that

$$H \approx Z_4 \times Z_2 \times Z_2 \times Z_2 \times H'.$$

Let  $(l) = \hat{l}_1 \cdot \hat{l}_2$  and  $(q) = q_1 \cdot q_2$  where  $\hat{l}_i$  and  $q_i$  are ideals of  $k$ . Also let  $h$  denote the class

number of  $k$  and  $\hat{l}_1^h = (a + b\sqrt{p})$ ,  $\hat{l}_2^h = (a - b\sqrt{p})$ ,  $q_1^h = (c + d\sqrt{p})$  and  $q_2^h = (c - d\sqrt{p})$ . Then we have the following character table:

Norm \ Character	$\sqrt{p}$	$\hat{l}_1$	$\hat{l}_2$	$q_1$	$q_2$
$\epsilon\sqrt{p}$	1	$\left(\frac{1}{p}\right)_4$	$\left(\frac{1}{p}\right)_4$	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p}\right)_4$
$a + b\sqrt{p}$	$\left(\frac{1}{p}\right)_4$	$\left(\frac{1}{q}\right)_4 \cdot \left(\frac{1}{p}\right)_4$	$\left(\frac{2}{p}\right)_4$	$x$	$x \left(\frac{1}{p}\right)_4$
$a - b\sqrt{p}$	$\left(\frac{1}{p}\right)_4$	$\left(\frac{2}{p}\right)_4$	$\left(\frac{1}{q}\right)_4 \cdot \left(\frac{1}{p}\right)_4$	$x \left(\frac{1}{p}\right)_4$	$x$
$c + d\sqrt{p}$	$\left(\frac{2}{p}\right)_4$	$y$	$y \left(\frac{1}{q}\right)_4$	$\left(\frac{1}{q}\right)_4 \cdot \left(\frac{2}{p}\right)_4$	$\left(\frac{2}{q}\right)_4$
$c - d\sqrt{p}$	$\left(\frac{2}{p}\right)_4$	$y \left(\frac{1}{q}\right)_4$	$y$	$\left(\frac{2}{q}\right)_4$	$\left(\frac{1}{q}\right)_4 \cdot \left(\frac{2}{p}\right)_4$

where  $x$  is the quadratic character of  $a + b\sqrt{p}$  modulo  $q_1$  and  $y$  is the quadratic character of  $c + d\sqrt{p}$  modulo  $\hat{l}_1$ . When  $\left(\frac{1}{q}\right)_4 = \left(\frac{2}{p}\right)_4 = -\left(\frac{2}{q}\right)_4 = -\left(\frac{1}{p}\right)_4 = 1$  the table becomes

Norm \ Character	$\sqrt{p}$	$\hat{l}_1$	$\hat{l}_2$	$q_1$	$q_2$
$\epsilon\sqrt{p}$	1	-1	-1	1	1
$a + b\sqrt{p}$	-1	$-\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p}\right)_4$	$x$	$x$
$a - b\sqrt{p}$	-1	$\left(\frac{2}{p}\right)_4$	$-\left(\frac{2}{p}\right)_4$	$x$	$x$
$c + d\sqrt{p}$	1	$y$	$y$	-1	-1
$c - d\sqrt{p}$	1	$y$	$y$	-1	-1

So exactly two ambiguous classes are in the principal genus and hence

$$H \approx Z_4 \times Z_2 \times Z_2 \times Z_2 \times H'.$$

If we show that  $L$  stays prime in  $K(\sqrt{l}) = K(\sqrt{-q\epsilon\sqrt{p}})$  then Corollary 17 applies to show  $K$  has (\*) with respect to  $l$ . Now  $l$  splits completely in  $Q(\sqrt{p})$  and ramifies in  $K$ . If we show  $l$  does not split completely in  $Q(\sqrt{-q\epsilon\sqrt{p}})$  then  $L$  must stay prime in  $K(\sqrt{-q\epsilon\sqrt{p}})$ . Since  $\left(\frac{1}{p}\right)_4 = -1$ ,  $l$  splits completely in  $Q(\sqrt{p})$  and gains degree two in  $Q(\sqrt{-\epsilon\sqrt{p}})$ . Since we also have that  $\left(\frac{q}{l}\right) = 1$ ,  $l$  splits completely in  $Q(\sqrt{q}, \sqrt{p})$ . Therefore  $l$  does not split completely in  $Q(\sqrt{q}, \sqrt{-\epsilon\sqrt{p}})$  so it does not split completely in  $Q(\sqrt{-q\epsilon\sqrt{p}})$ .

## §6. Bicyclic, Biquadratic Fields.

We begin this section with an example which shows that Pierce's result is not correct in this case. That is, there exist fields with even class number which do not have (\*) with respect to a prime  $l \equiv 3 \pmod{4}$ . Let  $K = Q(\sqrt{-15}, \sqrt{-7})$ . Since the quadratic subfields  $Q(\sqrt{-15})$ ,  $Q(\sqrt{105})$ ,  $Q(\sqrt{-7})$  of  $K$  have class numbers 2, 2 and 1 respectively, it follows from the class number formula [14] that  $K$  has class number 2. Since  $K(\sqrt{-3})/K$  is unramified,  $K(\sqrt{-3})$  is the Hilbert class field of  $K$ . Thus all primes of  $K$  which split completely in  $K(\sqrt{-3}) = K(\zeta)$  are principal. Also, 3 has only one prime divisor in  $K$ . Since  $\left(\frac{\sqrt{-15}}{10+\sqrt{105}}\right)^2 = \frac{-3}{41+4\sqrt{105}} = -3\varepsilon$  where  $\varepsilon$  is a unit of  $Q(\sqrt{105})$ , it follows that the prime divisor of 3 in  $K$  is also principal. Thus  $K$  has no nonprincipal Steinitz classes for the prime 3. Later, we give a corrected version of Pierce's result.

**PROPOSITION 26.** *If either  $l \nmid \Delta_{K/Q}$  or  $K \cap Q(\zeta) \neq Q$  then  $K$  has (\*) with respect to  $l$  if and only if  $b_1 \geq e_0$ . If  $K \cap Q(\zeta) = Q$ ,  $l \mid \Delta_{K/Q}$  and  $b_1 \neq e_0$  then  $K$  has (\*) with respect to  $l$  if and only if  $b_1 > e_0$ .*

**PROOF:** If  $b_1 < e_0$  then Proposition 1 shows that  $K$  does not have (\*) with respect to  $l$ . The converse of the first statement follows from Corollaries 9 and 11. If  $K \cap Q(\zeta) = Q$ , but  $l \mid \Delta_{K/Q}$  then  $e_0 = e, e_1 = 1, e_2 = e_0$ , so the last statement follows from Theorem 8.

**COROLLARY 27.** *If  $l \equiv 3 \pmod{4}$  then  $K$  has (\*) with respect to  $l$  if and only if  $K$  has even class number,  $h$ , and at least one of the following is satisfied:*

- (a)  $l \nmid \Delta_{K/Q}$
- (b)  $K \cap Q(\zeta) \neq Q$
- (c)  $K$  is real
- (d)  $h \equiv 0 \pmod{4}$
- (e)  $l$  has exactly two prime divisors in  $K$ .

**PROOF:** Suppose  $K$  is real and all of  $a, b$ , and  $d$  are false, but  $h$  is even. Then Corollary 14 shows  $K$  has (\*) with respect to  $l$ . Thus it follows from Proposition 26 that we may

assume that  $a, b, c$  and  $d$  are all false but  $h \equiv 2 \pmod{4}$  and prove that  $K$  has (\*) with respect to  $l$  if and only if  $l$  has exactly two prime divisors in  $K$ . Since  $l \equiv 3 \pmod{4}$  and  $h \equiv 2 \pmod{4}$ , it follows that  $H_1 = H'$  and  $[K_1 : K] = 2$ . Since  $l \mid \Delta_{K/Q}$ ,  $K \cap Q(\zeta) = Q$  and  $K$  is imaginary  $K(\sqrt{-l})/K$  is unramified and hence  $K_1 = K(\sqrt{-l})$ . First, assume that  $l$  has exactly one prime divisor  $L$  in  $K$ . Thus  $L$  has degree 2 and index 2 over  $l$ . Since  $G(K_1/Q) \approx Z_2 \times Z_2 \times Z_2$ ,  $L$  must split in  $K_1$ . Thus  $L$  belongs to a class of odd order in  $K$ . Theorem 13 shows that  $K$  does not have (\*) with respect to  $l$ .

Assume now that  $l$  has exactly two prime divisors  $L$  and  $L'$  in  $K$ . Since  $l$  must ramify in exactly two quadratic subfields of  $K$ , one of the imaginary subfields has the form  $k = Q(\sqrt{-ld})$ . Since  $\sqrt{-l} \notin K$ ,  $d > 1$ . Note that  $k(\sqrt{-l})/k$  is unramified. Also, since  $h \equiv 2 \pmod{4}$  the class number  $h_0$  of  $k$  must satisfy either  $h_0 \equiv 2 \pmod{4}$  or  $h_0 \equiv 4 \pmod{8}$ . Moreover,  $h_0 \equiv 4 \pmod{8}$  if and only if  $K/k$  is unramified. Since  $d > 1$ , the prime divisor of  $l$  in  $k$  must belong to a class of order 2. If  $h_0 \equiv 2 \pmod{4}$ , it must gain degree 2 in  $k(\sqrt{-l})$ , while if  $h_0 \equiv 4 \pmod{8}$ , it must gain degree 2 in  $K_1$ . In either case, both  $L$  and  $L'$  must gain degree 2 in  $K_1$ . Thus  $L$  and  $L'$  belong to classes of order 2 in  $K$ . Theorem 13 shows that  $K$  has (\*) with respect to  $l$ .

**COROLLARY 28.** Assume  $l \equiv 1 \pmod{4}$ ,  $l \mid \Delta_{K/Q}$ ,  $\sqrt{l} \notin K$ ,  $H/H'$  is cyclic and  $e_0 = b_1$ . Then  $K$  has (\*) with respect to  $l$  if and only if  $l$  splits completely in some quadratic subfield  $k$  of  $K$  and the prime divisors of  $l$  in  $k$  belong to ideal classes whose order is divisible by  $2^{e_0}$  or classes whose order is divisible by  $2^{e_0-1}$  which lift to classes of the same order in  $K$ .

**PROOF:** Theorem 13 or Corollary 14 shows  $K$  has (\*) with respect to  $l$  if and only if  $L^{(l-1)/2}$  or equivalently  $L^{2^{e_0-1}}$  belongs to a class of even order in  $K$ . Let  $k$  be the quadratic subfield of  $K$  which is the inertia field for  $L$  over  $Q$ . Then  $L^2$  is a prime divisor of  $l$  in  $k$ . Note if an ideal  $I$  of  $k$  lifts to a principal ideal  $(\alpha)$  then  $I^2 = (\alpha^{1+\sigma})$  where  $(\sigma) = G(K/k)$ . Thus  $L^2$  lifts to an ideal class of  $K$  of either the same order, or half the order of the class it belongs

to in  $k$ . The result now follows.

**COROLLARY 29.** *Assume  $l \equiv 1 \pmod{4}$ ,  $l \mid \Delta_{K/Q}$ ,  $\sqrt{l} \notin K$  and  $H/H'$  is cyclic. If  $l$  is unramified in a quadratic subfield  $k = Q(\sqrt{d})$  of  $K$  where  $k$  has even class number then  $K = Q(\sqrt{ld_1}, \sqrt{d})$  with  $d_1 \mid d$  and  $1 < d_1 \leq |d|$ . Moreover, the 2-class group of  $k$  must be cyclic.*

**PROOF:** Since  $l \equiv 1 \pmod{4}$ ,  $l \mid \Delta_{K/Q}$  and  $\sqrt{l} \notin K$ , it follows that  $K(\sqrt{l})/K$  is an unramified extension of degree 2. Since  $k$  has even class number, there is a divisor  $d_1$  of  $d$  such that  $k(\sqrt{d_1})/k$  is unramified. Since  $K/k$  is ramified at the prime divisors of  $(l)$ ,  $k(\sqrt{d_1}) \neq K$ , so  $K(\sqrt{d_1})/K$  is also unramified of degree 2. Since  $H/H'$  is cyclic it follows that  $K(\sqrt{d_1}) = K(\sqrt{l})$ . Thus  $Q(\sqrt{l}, \sqrt{d_1}) \cap K \neq Q$ . Since  $\sqrt{l}, \sqrt{d_1} \notin K$ , it follows that  $\sqrt{ld_1} \in K$ , so  $K = Q(\sqrt{ld_1}, \sqrt{d})$ . Since  $K/k$  is ramified, the class group of  $k$  is embedded in that of  $K$ . Hence  $k$  must have cyclic 2-class group.

**COROLLARY 30.** *If in addition to the hypothesis of Corollary 29,  $K$  is imaginary then  $d = -p \neq -2$  or  $d = -pq$  where  $p \neq q$  are primes with  $p \equiv 1$  or  $2 \pmod{4}$  and  $q \equiv 2$  or  $3 \pmod{4}$ . In either case  $d_1 = p$ .*

**PROOF:** If  $d > 0$  then  $K$  is real, so  $d < 0$ . Since the 2-class group of  $k$  is cyclic, the discriminant of  $k$  has exactly two prime divisors. Thus  $d$  has one of the values listed above. Since  $k(\sqrt{d_1})/k$  is unramified, we may choose  $d_1 = p$ .

**REMARK.** *The hypothesis that  $H/H'$  is cyclic in the previous two Corollaries can be replaced with the assumption that  $K(\sqrt{l})$  is the genus field of  $K$  over  $Q$ .*

**COROLLARY 31.** *Let  $K = Q(\sqrt{d}, \sqrt{lp})$  where  $l \equiv 1 \pmod{4}$  and  $d$  satisfies the conditions of Corollary 30. Then  $K_0 = K(\zeta) \cap K' = K(\sqrt{l})$  and  $H_0$  is the subgroup of  $H$  generated by ideals from the three quadratic subfields of  $K$ .*

**PROOF:** Note  $K(\zeta) \cap K'$  is clearly contained in the genus field of  $K$  over  $Q$ . But the genus



field is  $K(\sqrt{l})$  which is clearly contained in  $K(\zeta) \cap K'$ . It is shown in Kubota [13] that  $H_0$  is as described.

**COROLLARY 32.** *Let  $K$  be as in Corollary 30 with  $l \equiv 1 \pmod{4}$  and  $e_0 = b_1 > b_2 > 0$ . Then  $K$  has (\*) with respect to  $l$  if and only if one of the following conditions is satisfied:*

- (i)  *$l$  splits completely in a quadratic subfield  $k$  of  $K$  and the prime divisors of  $l$  in  $k$  belong to ideal classes of  $k$  whose order is divisible by  $2^{e_0}$  or classes whose order is divisible by  $2^{e_0-1}$  which lift to classes of the same order in  $K$ .*
- (ii) *Some quadratic subfield of  $K$  contains an ideal class of order  $2^{e_0+1}$  or a class of order  $2^{e_0}$  which lifts to a class of the same order.*

**PROOF:** Let  $k$  be the inertia field of  $L$  over  $Q$ . Since  $L^2$  is a prime divisor of  $l$  in  $k$ ,  $L^{(l-1)/2} = (L^2)^{(l-1)/4}$  belongs to a class of even order in  $K$  if and only if condition (i) is satisfied. When (i) holds, Lemma 7 shows that  $K$  has (\*) with respect to  $l$ . In order to use Theorem 15 to complete the proof, it needs to be shown that  $H_0$  has an element of order  $2^{e_0}$  if and only if (ii) holds. Since  $H_0$  is the subgroup of  $H$  generated by the ideal classes of the quadratic subfields, this is immediate.

**COROLLARY 33.** *Let  $K = Q(\sqrt{-p}, \sqrt{pl})$  where  $l$  and  $p$  are primes with  $l \equiv 5 \pmod{8}$  and  $p \equiv 1 \pmod{4}$ .*

- (a) *If  $p \equiv 5 \pmod{8}$  and  $\left(\frac{p}{l}\right) = -1$  then  $H/H' \approx Z_2 \times Z_2$  and so  $K$  does not have (\*) with respect to  $l$ .*
- (b) *If  $p \equiv 5 \pmod{8}$  and  $\left(\frac{p}{l}\right) = +1$  then  $K$  has (\*) with respect to  $l$  if and only if  $\left(\frac{p}{l}\right)_4 = \left(\frac{l}{p}\right)_4 = 1$ .*
- (c) *If  $p \equiv 1 \pmod{8}$  then  $K$  has (\*) with respect to  $l$ .*

**PROOF:** Let  $k_0 = Q(\sqrt{lp})$ ,  $k_1 = Q(\sqrt{-p})$ ,  $k_2 = Q(\sqrt{-l})$  and  $h_i$  ( $i = 0, 1, 2$ ) denote the class number of  $k_i$ . It follows from Kuroda [14] that  $h = \frac{1}{2}h_0h_1h_2$  or  $h = h_0h_1h_2$  according as the fundamental unit  $\varepsilon_0$  of  $k_0$  has norm  $-1$  or  $+1$ . Moreover, Halter-Koch [9] shows that the

lift maps on the class groups of  $k_1$  and  $k_2$  are injections and the lift map for  $k_0$  has a kernel of order 1 or 2 according as the norm of  $\varepsilon_0$  is  $+1$  or  $-1$ . Congruence conditions modulo 4 on  $h_0$  will be obtained from Brown [4] and on  $h_1$  and  $h_2$  from Hasse [11].

In part (a),  $N(\varepsilon_0) = -1$  and  $h_0 \equiv h_1 \equiv h_2 \equiv 2 \pmod{4}$ . Thus  $h \equiv 4 \pmod{8}$ . In the field  $k_0$ ,  $(2) = \mathfrak{p}_1 \mathfrak{p}_2$  and  $(p) = \mathfrak{p}^2$  for some prime ideals  $\mathfrak{p}_1, \mathfrak{p}_2$  and  $\mathfrak{p}$  of  $k_0$ . Since  $E_0 = Q(\sqrt{l}, \sqrt{p})$  is the Hilbert 2-class field of  $k_0$  and  $\left(\frac{2}{l}\right) = \left(\frac{2}{p}\right) = \left(\frac{l}{p}\right) = -1$ , it follows that  $\mathfrak{p}$  and  $\mathfrak{p}_1$  belong to ideal classes of even order in  $k_0$  while  $\mathfrak{p}\mathfrak{p}_1$  belongs to a class of odd order. Since  $\mathfrak{p} = (\sqrt{-p})$  becomes principal in  $K$ ,  $\mathfrak{p}_1$  belongs to a class of odd order in  $K$ . Now  $\mathfrak{p}_1 = P_1^2, \mathfrak{p}_2 = P_2^2$  for some prime ideals  $P_1$  and  $P_2$  of  $K$ . But  $(2) = \mathfrak{q}^2$  for some prime ideal  $\mathfrak{q}$  of  $k_1$ , so  $\mathfrak{q} = P_1 P_2$ . Since  $\mathfrak{q}$  lifts to a class of order 2 in  $K$ ,  $P_1$  and  $P_2$  generate distinct cosets of  $H/H'$ , each of order 2. Thus  $H/H' \approx Z_2 \times Z_2$  and Proposition 26 shows  $K$  does not have (\*) with respect to  $l$ .

In part (b),  $h_1 \equiv h_2 \equiv 2 \pmod{4}$  and  $h \equiv 0$  or  $8 \pmod{16}$  according as  $\left(\frac{p}{l}\right)_4 = \left(\frac{l}{p}\right)_4 = 1$  or  $-1$ . Moreover, when  $h \equiv 8 \pmod{16}$ ,  $h_0 \equiv 4 \pmod{8}$  or  $h_0 \equiv 2 \pmod{4}$  according as  $N(\varepsilon_0) = -1$  or  $+1$ . Since the kernel of the lift map for  $k_0$  has order 2 exactly when  $N(\varepsilon_0) = -1$ , it follows that condition (ii) of Corollary 32 is not satisfied when  $h \equiv 8 \pmod{16}$ . Moreover,  $E_1 = Q(\sqrt{-1}, \sqrt{-p})$  is the Hilbert 2-class field of  $k_1$ , so the prime divisors of  $l$  in  $k_1$  belong to classes of odd order. Thus condition (i) is not satisfied either. Since  $E_0 = Q(\sqrt{l}, \sqrt{p})$  is contained in the Hilbert 2-class field  $F_0$  of  $k_0$  and  $F_0/k_0$  is a cyclic extension of degree 2 or 4, it follows that a prime divisor  $\mathfrak{p}_1$  of  $(2)$  in  $k_0$  generates the 2-class group of  $k_0$ . In any case  $\mathfrak{p}_1$  generates a class of even order in  $K$ . Since  $\mathfrak{p}_1 = P_1^2$  in  $K$ ,  $P_1$  belongs to an ideal class of order divisible by 4. Since  $H_0/H' \approx Z_2 \times Z_2$ , it follows that  $H/H' \approx Z_4 \times Z_2$ , so Corollary 32 shows  $K$  does not have (\*) with respect to  $l$ .

When  $\left(\frac{p}{l}\right)_4 = \left(\frac{l}{p}\right)_4 = 1$  then  $h_0 \equiv 0$  or  $4 \pmod{8}$  according as  $N(\varepsilon_0) = -1$  or  $+1$ . In either case (ii) of Corollary 32 is satisfied. Thus either Proposition 26 or Corollary 32 applies to show  $K$  has (\*) with respect to  $l$ .

In part (c),  $h_1 \equiv 0 \pmod{4}$  so Proposition 26 or Corollary 32 shows  $K$  has (\*) with respect to  $l$ .

To simplify notation in the following result, we adopt the convention that  $\left(\frac{n}{2}\right) = \left(\frac{2}{n}\right)$  for any odd integer  $n > 1$ .

**COROLLARY 34.** *Let  $l, p$  and  $q$  denote distinct primes with  $l \equiv 5 \pmod{8}$ ,  $p \equiv 1$  or  $2 \pmod{4}$  and  $q \equiv 2$  or  $3 \pmod{4}$ . Let  $K = Q(\sqrt{-pq}, \sqrt{lp})$ ,  $k_0 = Q(\sqrt{lp})$ ,  $k_1 = Q(\sqrt{-pq})$ ,  $k_2 = Q(\sqrt{-lq})$  and  $h_i (i = 0, 1, 2)$  denote the class number of  $k_i$ .*

- (a) *If  $\left(\frac{p}{l}\right) = \left(\frac{q}{l}\right) = \left(\frac{p}{q}\right) = -1$  then  $H/H'$  is cyclic of order 4 and  $K$  has (\*) with respect to  $l$ .*
- (b) *If  $\left(\frac{pq}{l}\right) = -1$  then  $K$  does not have (\*) with respect to  $l$  if and only if  $\left(\frac{p}{l}\right) = +1$ ,  $\left(\frac{q}{l}\right) = \left(\frac{p}{l}\right)_4 \cdot \left(\frac{l}{p}\right)_4 = -1$  and either  $\left(\frac{p}{q}\right) = -1$  or  $\left(\frac{p}{q}\right) = +1$  and  $h_1 \equiv 4 \pmod{8}$ . Moreover, when the latter condition holds  $H/H' \approx Z_4$  or  $H/H' \approx Z_4 \times Z_2$  according as  $\left(\frac{p}{q}\right) = -1$  or  $\left(\frac{p}{q}\right) = +1$ .*
- (c) *If  $\left(\frac{pq}{l}\right) = +1$  then  $K$  does not have (\*) with respect to  $l$  if and only if  $\left(\frac{p}{l}\right) = \left(\frac{q}{l}\right) = +1$ ,  $\left(\frac{p}{l}\right)_4 \cdot \left(\frac{l}{p}\right)_4 = -1$ ,  $h_2 \equiv 4 \pmod{8}$  and either  $\left(\frac{p}{q}\right) = -1$  or  $\left(\frac{p}{q}\right) = +1$  and  $h_1 \equiv 4 \pmod{8}$ . When the latter conditions hold  $H/H' \approx Z_4 \times Z_2$  or  $Z_4$  according as  $\left(\frac{p}{q}\right) = +1$  or  $-1$ .*

**PROOF:** Here  $h = \frac{1}{2}h_0h_1h_2$  and the lift map on the class group of  $k_0$  is an injection. Moreover, the lift maps on the class groups of  $k_1$  and  $k_2$  have kernels of order 1 or 2 according as the norm of  $\varepsilon_0$  is  $+1$  or  $-1$ .

In part (a),  $h_0 \equiv h_1 \equiv h_2 \equiv 2 \pmod{4}$  so  $h \equiv 4 \pmod{8}$ . Now  $(p) = \mathfrak{p}_1\mathfrak{p}_2$  splits completely in  $k_2$  and each  $\mathfrak{p}_i$  ramifies in  $K$ , say  $\mathfrak{p}_i = P_i^2$ . Since  $E_2 = Q(\sqrt{l}, \sqrt{-q})$  is the Hilbert 2-class field of  $k_2$  and  $\left(\frac{l}{p}\right) = -1$ , it follows that each  $\mathfrak{p}_i$  belongs to an ideal class of even order in  $k_2$ . Moreover, since  $\left(\frac{l}{p}\right) = -1$ ,  $\varepsilon_0$  has norm  $-1$ , so the lift maps for  $k_1$  and  $k_2$  are injections. Thus  $\mathfrak{p}_i$  belongs to a class of even order in  $K$  and so  $P_i$  belongs to a

class that has order divisible by 4. Hence  $H/H' \approx Z_4$ . Here  $l$  splits completely in  $k_1$  and its prime factors in  $k_1$  gain degree 2 in  $E_1 = Q(\sqrt{p}, \sqrt{-q})$ . Since  $E_1$  is the Hilbert 2-class field of  $k_1$ , these primes belong to classes of even order in  $k_1$ . Corollary 28 shows that  $K$  has (\*) with respect to  $l$ .

In part (b) when  $\left(\frac{p}{l}\right) = -1$ , then  $\varepsilon_0$  has norm  $-1$  and the lift maps for  $k_1$  and  $k_2$  are injections. Since  $\left(\frac{q}{l}\right) = +1, h_2 \equiv 0 \pmod{4}$ , so  $h \equiv 0 \pmod{8}$ . Here either Corollary 32 or Proposition 26 shows that  $K$  has (\*) with respect to  $l$ . Similarly when  $\left(\frac{p}{l}\right)_4 \left(\frac{l}{p}\right)_4 = +1$ ,  $h_0 \equiv 0 \pmod{4}$  and the result follows. Assume now that  $\left(\frac{p}{l}\right)_4 \left(\frac{l}{p}\right)_4 = -1$ , then  $h_0 \equiv 2 \pmod{4}$  and  $N(\varepsilon_0) = +1$ . If, in addition,  $\left(\frac{p}{q}\right) = +1$  then  $h_1 \equiv 0 \pmod{4}$ . If  $h_1 \equiv 0 \pmod{8}$  then  $H_0$  contains an element of order 4, so Corollary 32 or Proposition 26 again applies. Thus we may assume  $\left(\frac{p}{q}\right) = -1$  or  $\left(\frac{p}{q}\right) = +1$  and  $h_1 \equiv 4 \pmod{8}$ . Since the lift map for  $k_1$  has kernel of order 2,  $H_0$  contains no elements of order 4. Moreover,  $h \equiv 4 \pmod{8}$  or  $h \equiv 8 \pmod{16}$  according as  $\left(\frac{p}{q}\right) = -1$  or  $\left(\frac{p}{q}\right) = +1$ . In the latter case  $h_1 \equiv 4 \pmod{8}$  so the Hilbert 2-class field  $F_1$  of  $k_1$  has cyclic Galois group over  $k_1$ . Since  $K/K_1$  is ramified  $F_1 K/K$  is a cyclic unramified extension of degree 4. Here  $H/H' \approx Z_4 \times Z_2$ . When  $\left(\frac{p}{q}\right) = -1$ , the argument used in part (a) applies to the prime  $q$  and the field  $k_0$  showing  $H/H' \approx Z_4$ . Since  $l$  stays prime in  $k_1$ , either Corollary 32 or Corollary 28 applies to show  $K$  does not have (\*) with respect to  $l$ . Thus we may assume  $\left(\frac{p}{l}\right) = \left(\frac{q}{l}\right) = +1$ . Similarly, if any of  $\left(\frac{p}{l}\right)_4 \left(\frac{l}{p}\right)_4 = +1, h_2 \equiv 0 \pmod{8}$  or  $h_1 \equiv 0 \pmod{8}$  (and hence  $\left(\frac{p}{q}\right) = +1$ ) then  $H_0$  contains an element of order 4 and  $K$  has (\*) with respect to  $l$ . Hence we may also assume that  $\left(\frac{p}{l}\right)_4 \left(\frac{l}{p}\right)_4 = -1, h_2 \equiv 4 \pmod{8}$  and either  $\left(\frac{p}{q}\right) = -1$  or  $\left(\frac{p}{q}\right) = +1$  and  $h_1 \equiv 4 \pmod{8}$ . Here  $h \equiv 4 \pmod{8}$  or  $h \equiv 8 \pmod{16}$  according as  $\left(\frac{p}{q}\right) = -1$  or  $+1$ . Moreover,  $H_0$  contains no elements of order 4. Since  $h_2 \equiv 4 \pmod{8}$ , the Hilbert 2-class field  $F_2$  of  $k_2$  has cyclic Galois group of order 4. As in part (b),  $H$  must contain an element of order 4, so  $H/H' \approx Z_4 \times Z_2$  or  $Z_4$  according as  $\left(\frac{p}{q}\right) = +1$  or  $\left(\frac{p}{q}\right) = -1$ . Since  $E_1 = Q(\sqrt{p}, \sqrt{-q})$  is the 2-Hilbert class field of  $k_1$ , the prime divisors of  $l$  in  $k_1$  do not belong to classes having

order divisible by 4. Thus Corollary 28 or Corollary 32 applies to show that  $K$  does not have (\*) with respect to  $l$ .

**THEOREM 35.** *Let  $K = Q(\sqrt{m}, \sqrt{ul})$  where  $m$  and  $u$  are squarefree,  $l \equiv 1 \pmod{4}$ ,  $K \cap Q(\zeta) = Q$ , and  $l \nmid m \cdot u$ . Suppose  $b_1 = e_0$  and  $1 \leq b_2 < b_1$ . Then  $K$  has (\*) with respect to  $l$  if and only if either*

- (a)  $L^{(l-1)/2}$  is in a class of even order, or
- (b) for some  $i > 1$ ,  $\left(\frac{m}{a_i}\right) = 1$  or  $0$ ,  $\left(\frac{u}{a_i}\right) = -1$  or  $0$ ,  $\left(\frac{l}{a_i}\right) = -1$  or  $0$ , and if  $a_i^2 \mid m \cdot u$  then  $\left(\frac{m/a_i}{a_i}\right) = \left(\frac{u/a_i}{a_i}\right)$ ; i.e.  $A_i$  is of degree 1 over  $Q$  and gains degree 2 in  $K(\sqrt{l})$ .

**PROOF:** If condition (a) holds then  $K$  has (\*) with respect to  $l$ . Assume condition (b) holds. Here  $K_0 = K(\zeta) \cap K' = K(\sqrt{l})$ . If  $C_1 \in H_0$  then Theorem 15 shows that  $K$  has (\*) with respect to  $l$ . Thus we may assume  $C_1 \notin H_0$ . Now condition (b) implies  $C_i \notin H_0$  also. Since  $[H : H_0] = 2$ ,  $C_1 C_i \in H_0$ , but  $C_1 C_i$  has order  $2^{b_1}$ . Thus Theorem 15 again applies to show  $K$  has (\*) with respect to  $l$ .

Now assume that condition (a) does not hold and for each  $i > 1$  condition (b) is not satisfied. Then for each  $i > 1$ ,  $A_i$  splits completely in  $K(\sqrt{l})$ , so  $C_i \in H_0$ . Since  $[H : H_0] = 2$ ,  $H_0$  contains no element of order  $2^{b_1}$ . Theorem 15 shows  $K$  does not have (\*) with respect to  $l$ .

In the next two corollaries all hypotheses of Theorem 35 except conditions (a) and (b) are assumed to hold.

**COROLLARY 36.** *If  $\left(\frac{m}{l}\right) = -1$  then  $K$  has (\*) with respect to  $l$  if and only if (b) holds.*

**PROOF:** Since  $\left(\frac{m}{l}\right) = -1$ ,  $L^2 = (l)$ . Because  $l \equiv 1 \pmod{4}$ ,  $L^{(l-1)/2}$  is principal.

**COROLLARY 37.** *If the 2-part of the exponent of the ideal class group of  $Q(\sqrt{m})$  divides  $2^{e_0-2}$  then  $K$  has (\*) with respect to  $l$  if and only if (b) holds.*

**PROOF:** Here  $L^{(l-1)/2}$  is principal.

Let  $K = Q(\sqrt{6}, \sqrt{-370})$ ,  $k_0 = Q(\sqrt{6})$ ,  $k_1 = Q(\sqrt{-370})$ , and  $k_2 = Q(\sqrt{-555})$ . Now,  $h_0 = 1$ ,  $h_1 = 12$ , and  $h_2 = 4$ . So  $h = (1/2) \cdot 1 \cdot 12 \cdot 4 = 2^3 \cdot 3$ . The standard formula shows that the number of ambiguous classes for  $K/k_0$  is 4. Since  $h_0 = 1$ , these are precisely the classes of order 1 or 2 in  $K$ , so  $H \approx Z_4 \times Z_2 \times Z_3$ .

In  $K$ ,  $(5) = P_5^2 \cdot \hat{P}_5^2 = (1 + \sqrt{6})(1 - \sqrt{6})$ . Since  $(\frac{37}{5}) = -1$  it follows that  $P_5$  stays prime in  $K(\sqrt{37})$ . This means the class of  $P_5$  is not in  $H_0$ , then it follows that the ideal class of  $P_5$  is not a square. Hence,  $P_5$  is in a class of order 2. Thus we can choose  $A_2 = P_5$ .

When  $l = 5$ ,  $m = 6$  and  $u = -74$  with  $(\frac{-74}{5}) = 1$ . Thus Corollary 37 shows  $K$  does not have (\*) with respect to 5.

When  $l = 37$ ,  $m = 6$ , and  $u = -10$  with  $(\frac{6}{5}) = 1$ ,  $(\frac{-10}{5}) = 0$ ,  $(\frac{37}{5}) = -1$  and  $5^2 \nmid mu$ . Thus Corollary 37 shows that  $K$  has (\*) with respect to 37.

Let  $K = Q(\sqrt{5}, \sqrt{-33})$ ,  $k_0 = Q(\sqrt{5})$ ,  $k_1 = Q(\sqrt{-33})$ , and  $k_2 = Q(\sqrt{-165})$ ,  $h_0 = 1$ ,  $h_1 = 4$ , and  $h_2 = 8$ . So  $h = \frac{1}{2} \cdot 1 \cdot 4 \cdot 8 = 16$ . The standard formula shows that the number of ambiguous classes for  $K/k_0$  is 8. Since  $h_0 = 1$ , these are precisely the classes of order 1 or 2 in  $K$ . It follows that  $H \approx Z_4 \times Z_2 \times Z_2$ .

In  $K$ ,  $(11) = P_{11}^2 \cdot \hat{P}_{11}^2 = (4 + \sqrt{5})(4 - \sqrt{5})$ . Since  $(\frac{-3}{11}) = -1$  it follows that  $P_{11}$  stays prime in  $K(\sqrt{-3})$ . It then follows that the ideal class of  $P_{11}$  is not a square. Hence,  $P_{11}$  is in a class of order 2. Then we can choose  $A_2 = P_{11}$ .

Since  $(\frac{5}{11}) = 1$ , Corollary 36 applies to show that  $K$  does not have (\*) with respect to  $l = 5$ .

## REFERENCES

- [1] E. Artin, Collected papers, Addison-Wesley, Reading, Mass., (1965), 229–321.
- [2] P. Barrucand and H. Cohn, A rational genus, class number divisibility and unit theory for pure cubic fields, *J. No. Theory* 2 (1970), 7–21.
- [3] R. H. Bird and C. J. Parry, Integral bases for bicyclic biquadratic fields over quadratic subfields, *Pac. J. Math.* 66 (1976), 29–36.
- [4] E. Brown, Class numbers of real quadratic numbers fields, *Trans. Amer. Math. Soc.*, 190 (1974), 99–107.
- [5] E. Brown and C. J. Parry, The 2-class group of certain biquadratic number fields, *J. reine angew. Math.*, 295 (1977), 61–71.
- [6] E. Brown and C. J. Parry, The 2-class group of biquadratic fields, II, *Pac. J. Math.*, 78 (1978), 11–26.
- [7] H. Edgar and B. Peterson, Some contributions to the theory of cyclic quartic extensions of the rationals, *J. No. Theory* 12 (1980), 77–83.
- [8] T. Funakura, On integral bases of pure quartic fields, *Math. J. Okayama Univ.* 26 (1984), 27–41.
- [9] F. Halter-Koch, Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Körper, *J. Number Theory*, 4 (1972), 144–156.
- [10] K. Hardy, R. H. Hudson, D. Richman, K. S. Williams and N. M. Holtz, Calculation of the class numbers of imaginary cyclic quartic fields, *Carleton-Ottawa Mathematical Lecture Note Series No. 7*, July 1986.
- [11] H. Hasse, Über die Teilbarkeit durch  $2^3$  der Klassenzahl imaginär-quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *J. reine angew. Math.*, 241 (1970), 1–6.
- [12] D. Hilbert, Bericht über die algebraischen Zahlkörper, *Jber. Deutsche Math.-Verein.* 4 (1894–95).
- [13] T. Kubota, Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörpers, *Nagoya Math J.*, 6 (1953), 119–127.
- [14] S. Kuroda, Über den Dirichletschen Körper, *J. Fac. Sci. Imp. Univ. Tokyo, Sec. I*, vol. IV, Part 5 (1943), S. 383.
- [15] W. Ljunggren, Über die Lösung einiger unbestimmten Gleichungen vierten Grades, *Avh. Norske Vid. Akad. Oslo, I. Mat.-Naturv. Klasse* 14 (1934), 1–35.

- [16] R. L. Long, Steinitz classes of cyclic extensions of prime degree, *J. reine angew. Math.* 250 (1970), 87–88.
- [17] H. B. Mann, On integral bases, *Proc. Amer. Math. Soc.* 9 (1958), 167–172.
- [18] B. Oriat, Groupes des classes d'idéaux des corps quadratiques imaginaires  $Q(d^{1/2})$ ,  $-24572 < d < 0$ , *Theorie des nombres, Années, 1986/87–1987/88, Fasc. 2*, 63 pp., *Publ. Math. Fac. Sci. Besancon, Univ, Franhe-Compté, Besancon* 1988.
- [19] C. J. Parry, Pure quartic number fields whose class numbers are even, *J. Reine Angew. Math.*, 264 (1975), 102–112.
- [20] S. Pierce, Steinitz classes in quartic fields, *Proc. Amer. Math. Soc.*, 43 (1974), 39–41.
- [21] E. Weiss, *Algebraic Number Theory*, McGraw–Hill, New York, (1963), 154–167.



**VITA**

John Alexander Hymo was born on April 22, 1961, in Washington, D.C. He graduated from Mount Vernon High School in 1979. He received the B.S. degree in Mathematics from Allegheny College in 1983. He received the M. S. degree in Mathematics from Virginia Tech in 1985. He is a member of the A.M.S.

*John A. Hymo*