IRREDUCIBLE ELEMENTS IN ALGEBRAIC NUMBER FIELDS

by

Daisy C. McCoy

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

DOCTOR OF PHILOSOPHY

in

Mathematics

APPROVED:

Charles J. Parry

C. J. Parry, Chairman

Ezra Brown

E. Brown

D. Farkas

D. Farkas

Peter Fletcher

P. Fletcher

Robert L. Wheeler

R. Wheeler

November, 1990

Blacksburg, Virginia

IRREDUCIBLE ELEMENTS IN ALGEBRAIC NUMBER FIELDS

by

Daisy C. McCoy

Committee Chairman: Charles J. Parry

Mathematics

(ABSTRACT)

This dissertation is a study of two basic questions involving irreducible elements in algebraic number fields. The first question is: Given an algebraic integer β in a field with class number greater than two, how many different lengths of factorizations into irreducibles exist? The distribution into ideal classes of the prime ideals whose product is the principal ideal (β) determines the possible length of the factorizations into irreducibles. Chapter 2 gives precise answers when the field has class number 3 or 4, as well as when the class group is an elementary 2–group of order 8.

The second question is: In a normal extension, when are there rational primes which split completely and remain irreducible? Chapter 3 focusses on the bicyclic biquadratic fields. The imaginary bicyclic biquadratic fields which contain such primes are completely determined.

ACKNOWLEDGEMENTS

Graduate study can be a long, lonely, and often discouraging experience. It was because of the help and encouragement of many people in the Virginia Tech community that I persevered.

My advisor, Charles J. Parry, was very generous with his guidance and support. His interest in my education as a mathematician and in my project was crucial. He provided valued assistance in a number of areas including research techniques, bibliographic insights, and editorial guidance. I am especially indebted to him for his computer calculations of class numbers. Charles Parry understands a student's need to spend time outside of the library and class room. I am grateful for his advice about the Appalachian Trail and other wilderness opportunites in the area.

Others have helped me in many ways as well. I wish to thank Ruth and Eddie Sherman and Robin Endelman for their hospitality and friendship. A special note of thanks also goes to Professor Daniel Farkas for the opportunity to work with him and the many thought provoking conversations we have had.

TABLE OF CONTENTS

Chapter I. Introduction

In the field of rational numbers, every integer has a unique factorization into irreducible elements; i.e., unique prime factorization. However, in an arbitrary number field, an algebraic integer may have several distinct factorizations into irreducible elements. In fact, the number of irreducible factors occuring in different factorizations of an integer may not be the same, depending on the class structure for the field. If the field has class number 1 or 2, then the number of irreducible factors in the factorizations of an integer is unique. In Chapter II we consider the problem of determining the number of different lengths of irreducible factorizations of an algebraic integer in fields with class number greater than 2. Theorems 7 and 8 give precise answers when the Davenport constant of the class group is 3 and Theorems 10 and 17 answer the question when the Davenport constant is 4. For each of these theorems, Section six gives explicit examples, showing how an integer may be found having a given number of irreducible factorizations with distinct lengths.

In the field of rational numbers, the prime numbers are the irreducible elements. However, every other algebraic number field will contain rational primes which are reducible. Chapter III explores the question of which number fields contain rational primes which remain irreducible. Narkiewicz [13] has shown that such number fields must have a Galois group with a cyclic subgroup of index not exceeding the Davenport constant of the class group. In particular, in a cyclic extension there are rational primes which remain prime and therefore are irreducible. Sliwa [19] gave a characterization of normal extensions K/Q containing irreducible rational primes using the Galois group $G(K/Q)$, the class group $H(K)$, and the action of G on $H(K)$.

The question becomes more interesting when restricted to the existence of rational primes which split completely in K and remain irreducible. A normal cyclic extension of degree $l = 2, 3$ or 5 over the rational numbers is easily seen to have this property if and only if it has class number greater than 1. In a bicylic biquadratic field K, a prime splits completely and remains irreducible if and only if its prime factors in each quadratic subfield of K are not principal in K. The detailed study of this condition in Chapter III yields a complete characterization of imaginary bicyclic fields containing irreducible rational primes which, as ideals, split completely.

Chapter II. Lengths of Irreducible Factorizations in Fields with Small Class Numbers

§1. Introduction.

Every nonzero integer of an algebraic number field has a unique factorization into irreducible elements if and only if the field has class number 1. L. Carlitz [5] has shown that the number of irreducible factors occurring in a factorization is unique if and only if the class number of the field is less than or equal 2. For fields of class number greater than 2, Narkiewicz [14], Narkiewicz and Sliwa [15], and Allen and Pleasants [1] have obtained asymptotic estimates for the number of different lengths of irreducible factorizations. In this chapter we obtain explicit formulas for the number of different lengths of irreducible factorizations of an algebraic integer, when the ideal class group of the field has Davenport constant at most four.

§2. Notation and Terminology.

K:	an algebraic number field.
β:	nonzero, nonunit, integer of K.
$l(\beta)$:	Number of different lengths of factorizations of β into irreducible elements, where the length of an irreducible factorization is the number of irreducible factors.
h:	Class number of K.
H:	Ideal class group of K.
$X_i (0 \leq i < h)$:	Ideal classes of K, where X_0 denotes the principal class.
$o(X_i)$:	Order of the class X_i.
$\Omega_i(\beta)$:	Number of prime ideals (counting multiplicities) in X_i which divide β.
$s = \Omega(\beta)$:	Number of prime ideals (counting multiplicities) which divide β.

$(\beta) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$: Factorization of (β) into prime ideals.

$[\mathfrak{p}_i]$: The ideal class of $\mathfrak{p}_i$.

$S = S(\beta)$: The sequence $[\mathfrak{p}_1], [\mathfrak{p}_2], \ldots, [\mathfrak{p}_s]$ of ideal classes determined by β.

Block: A finite sequence of elements of H whose product is X_0.

Block Product: If $B = X_0^{b_0}X_1^{b_1}\ldots X_{h-1}^{b_{h-1}}$ and $C = X_0^{c_0}X_1^{c_1}\ldots X_{h-1}^{c_{h-1}}$ are blocks and b_i, $c_i$are nonnegative integers then

$$BC = X_0^{b_0+c_0}X_1^{b_1+c_1}\ldots X_{h-1}^{b_{h-1}+c_{h-1}}.$$

Irreducible Block: A block which cannot be written as a product of two subblocks.

$D(H)$: The Davenport constant of H; i.e., the maximum length of an irreducible block of H.

R: The free commutative semigroup generated by the set of all irreducible blocks of H. The elements of R can be represented as formal linear polynomials $\Sigma a_i B_i$ where each a_i is a nonnegative integer and the B_i range over all the irreducible blocks of H.

$w(F)$: If $F \in R$, the weight of $F, w(F)$, is the sum of the coefficients of F.

§3. Preliminary Results.

Some general observations are made in this section, which apply to any number field, K.

Lemma 1. *If $\beta = \beta_0\beta_1$ where $\Omega_i(\beta_0) = 0$ for $1 \leq i < h$ and $\Omega_0(\beta_1) = 0$, then $l(\beta) = l(\beta_1)$.*

Proof: Since every prime ideal factor of β_0 is principal, the number of irreducible elements in any factorization of β_0 is $\Omega_0(\beta_0)$. Hence $l(\beta_0) = 1$ and $l(\beta) = l(\beta_1)$.

In view of Lemma 1, for the remainder of this chapter we will assume that $\Omega_0(\beta) = 0$.

There is an obvious one-to-one correspondence between the set of all partitions of S into irreducible blocks and a subset R' of R. The coefficient of an irreducible block B of an F in R' is precisely the number of times the block B occurs in the given partition of S.

LEMMA 2. *If F belongs to R' and some terms $G = \sum_{i=1}^{m} b_i B_i$ of F are replaced with the terms $G' = \sum_{j=1}^{m} c_j C_j$ in R subject to the condition that*

$$\Pi_{i=1}^{m} B_i^{b_i} = \Pi_{j=1}^{n} C_j^{c_j}$$

then the polynomial F' obtained by this substitution also belongs to R'.

PROOF: Since F corresponds to a partition of S into irreducible blocks, the product condition insures that F' also corresponds to a partition of S. Thus F' belongs to R'.

The substitution of Lemma 2 can be considered as a transformation on R'. The notation

$$T(\sum_{i=1}^{m} b_i B_i) = \sum_{j=1}^{m} c_j C_j$$

will be used to denote such transformations.

LEMMA 3. *The number of different weights of elements of R' is precisely $l(\beta)$.*

PROOF: For any F in $R', w(F)$ is precisely the number of irreducible elements in the factorization of β determined by the partition of S corresponding to F.

Each element F of R' determines a solution to the Diophantine equation

$$2y_1 + 3y_2 + \cdots + Dy_{D-1} = s \qquad (*)$$

where y_i is the number of irreducible blocks of length $i+1$ which occur in F and $D = D(H)$. A non-negative integral solution to (*) will be called an <u>admissible</u> solution if it is determined by some F in R'.

LEMMA 4. *$l(\beta)$ is precisely the number of distinct sums of the form $y_1+y_2+\cdots+y_{D-1}$ where $(y_1,\cdots,y_{D-1})$ runs through the set of admissible solutions to (*).*

PROOF: Each F in R' gives an admissible solution to (*) with $w(F) = y_1+\cdots+y_{D-1}$. Conversely, any admissible solution with $y_1+\cdots+y_{D-1} = t$, corresponds to an F in R' with $w(F) = t$. The result follows from Lemma 3.

§4. Class groups of order 3 and 4.

When H has order 3 or 4, it is shown that $l(\beta)$ is a linear function of $m = min\{\Omega_i(\beta)\}$ such that $X_i \in H$ has maximum order.

LEMMA 5. *If $H = Z_3$, then $l(\beta)$ is the number of solutions to $3x+2y = s$ with $0 \le x$ and $0 \le y \le m$.*

PROOF: The irreducible blocks of H are $X_i^3 (i = 1,2)$ and X_1X_2. Hence the number of irreducible blocks of length 2 in any partition of $S(\beta)$ is at most m. Thus $l(\beta)$ is bounded above by the number of solutions to the equation satisfying the inequalities.

Conversely, let (x,y) be a solution to the equation which satisfies the inequalities. Since (β) is a principal ideal, $\Omega_1(\beta)+2\Omega_2(\beta) \equiv 0 (mod\ 3)$. Thus $\Omega_1(\beta) \equiv \Omega_2(\beta) \equiv m (mod\ 3)$ and so $2y \equiv s \equiv \Omega_1(\beta)+\Omega_2(\beta) \equiv 2m (mod\ 3)$. Hence

$$F = \frac{1}{3}(\Omega_1(\beta)-y)X_1^3 + \frac{1}{3}(\Omega_2(\beta)-y)X_2^3 + yX_1X_2$$

is in R' and corresponds to the solution (x,y). Since distinct solutions to (*) give distinct values of $x+y$, the result follows from Lemma 4.

LEMMA 6. *If $H = Z_2 \times Z_2$, then $l(\beta)$ is the number of solutions to $3x+2y = s$ with $0 \le x \le m$ and $0 \le y$.*

PROOF: Here the irreducible blocks are $X_i^2 (i = 1,2,3)$ and $X_1X_2X_3$. Since x denotes the number of irreducible blocks of length 3 in any partition of S, it is clear that $x \le m$. The remainder of the proof is similar to that of Lemma 5.

THEOREM 7. *If $H = Z_3$, then $l(\beta) = \frac{m+\epsilon}{3}$ where $\epsilon \equiv s(mod\ 3)$ and $1 \leq \epsilon \leq 3$.*

PROOF: If $3x + 2y = s$, then

$$y \equiv 2s(mod\ 3)$$

so $y = 2s - 3t$ for some integer t and so $x = 2t - s$. It follows from Lemma 5 that $\frac{2s-m}{3} \leq t \leq \frac{2s}{3}$ and $\frac{s}{2} \leq t$. But $\frac{s}{2} \leq \frac{2s-m}{3}$. Note that $2s - m \equiv 0(mod\ 3)$ and that $2s \equiv 3 - \epsilon(mod\ 3)$ with $0 \leq 3 - \epsilon \leq 2$, so that $t \leq \frac{2s-3+\epsilon}{3} = \frac{2s+\epsilon}{3} - 1$. By Lemma 5,

$$l(\beta) = \frac{2s+\epsilon}{3} - 1 - \frac{2s-m}{3} + 1 = \frac{m+\epsilon}{3}.$$

THEOREM 8. *If $H = Z_2 \times Z_2$, then $l(\beta) = \frac{m+\epsilon}{2}$ where $\epsilon \equiv s(mod\ 2)$ and $\epsilon = 1$ or 2.*

PROOF: As in the preceding proof $y = 2s - 3t$ and $x = 2t - s$. From Lemma 6, $\frac{s}{2} \leq t \leq \frac{s+m}{2}$ and $t \leq \frac{2s}{3}$, but $\frac{s+m}{2} \leq \frac{2s}{3}$. Since (β) is a principal ideal, $\Omega_1(\beta) + \Omega_3(\beta) \equiv \Omega_2(\beta) + \Omega_3(\beta) \equiv 0(mod\ 2)$, so $\Omega_1(\beta) \equiv \Omega_2(\beta) \equiv \Omega_3(\beta) \equiv m(mod\ 2)$. In particular, $s \equiv m(mod\ 2)$. Note that $s \equiv 2 - \epsilon(mod\ 2)$ with $2 - \epsilon = 0$ or 1, so that $t \geq \frac{s+2-\epsilon}{2} = \frac{s-\epsilon}{2} + 1$. By Lemma 6

$$l(\beta) = \frac{s+m}{2} - \left(\frac{s-\epsilon}{2} + 1\right) + 1 = \frac{m+\epsilon}{2}.$$

We now consider the case $H = Z_4$. Number the ideal classes so that $o(X_1) = o(X_3) = 4$ and $o(X_2) = 2$. Let $\Omega_1(\beta) = k, \Omega_2(\beta) = l$ and $\Omega_3(\beta) = m$. With no loss of generality, we may assume $k \geq m$.

LEMMA 9. *If $H = Z_4$, then $l(\beta) \leq \left[\frac{m}{2}\right] + 1$.*

PROOF: By Lemma 4, $l(\beta)$ is bounded by the number of solutions to

$$4x + 3y + 2z = s$$

which give distinct values for $x + y + z$. Since $y \equiv s(mod\ 2), y = s - 2u$ for some integer u and

$$2x + z = -s + 3u \text{ so}$$

$$z \equiv s + u (mod\ 2). \text{ Thus}$$

$$z = s + u - 2v \text{ and}$$

$$x = -s + u + v, \text{ so}$$

$$x + y + z = s - v.$$

Since the irreducible blocks of H are $X_i^4 (i = 1, 3), X_i^2 X_2 (i = 1, 3), X_1 X_3$ and X_2^2, in any partition of $S(\beta)$ the l X_2 terms occur either as singletons in blocks of length 3 or as pairs in blocks of length 2. Thus $l \leq y + 2z$, so $v \leq \frac{3s-l}{4}$. On the other hand,

$$\begin{aligned} z &\leq m + \frac{1}{2} \text{ (number of } X_2\text{'s not used in blocks of length 3)} \\ &= m + \frac{1}{2}(l - y). \text{ Thus} \end{aligned}$$

$$y + 2z \leq l + 2m \text{ and hence}$$

$$\frac{3s - l}{4} - \frac{m}{2} \leq v \leq \frac{3s - l}{4}.$$

Thus there are at most $\left[\frac{m}{2}\right] + 1$ distinct values of $x + y + z$ where (x, y, z) is a solution to (*). This gives the desired bound for $l(\beta)$.

THEOREM 10. *If $H = Z_4$, then* $l(\beta) = \begin{cases} [m/2] + 1 & \text{if } l > 0 \\ [m/4] + 1 & \text{if } l = 0. \end{cases}$

PROOF: First suppose $l > 0$. Since (β) is a principal ideal, $k + 2l + 3m \equiv 0 (mod\ 4)$ so $k \equiv m (mod\ 2)$. Also, $k \equiv m + 2l (mod\ 4)$ and

$$s = k + l + m \equiv l (mod\ 2).$$

Let $m \equiv \epsilon \equiv 2\epsilon_1 + \epsilon_0 (mod\ 4)$ with $0 \leq \epsilon \leq 3$ and $0 \leq \epsilon_0, \epsilon_1 \leq 1$. Set

$$v = \frac{3s - l - 2\epsilon_0}{4} \text{ and note that}$$

$$\begin{aligned} 4v &= 3s - l - 2\epsilon_0 \\ &= 3k + 2l + 3m - 2\epsilon_0 \end{aligned}$$

$$\equiv 2(m - \epsilon_0) \equiv 0(mod\ 4),$$

so that v is an integer. First, we assume that l (and hence s) is even, so $u = \frac{s}{2} - \epsilon_1$ is an integer. Using the equations given in the proof of Lemma 9, we obtain

$$\begin{aligned} x &= \left(\frac{k-\epsilon}{4}\right) + \left(\frac{m-\epsilon}{4}\right) \\ y &= 2\epsilon_1 \\ z &= \frac{l+2\epsilon_0}{2} - \epsilon_1. \end{aligned}$$

An element of R' corresponding to this solution is

$$F = \left(\frac{k-\epsilon}{4}\right) X_1^4 + \left(\frac{m-\epsilon}{4}\right) X_3^4 + \epsilon_1 X_1^2 X_2 + \epsilon_1 X_3^2 X_2 + \left(\frac{l}{2} - \epsilon_1\right) X_2^2 + \epsilon_0 X_1 X_3.$$

Since we will need a cubic term with positive coefficient, if $\epsilon_1 = 0$ apply the transformation

$$T_0(X_1^4 + X_2^2) = 2X_1^2 X_2 \text{ to } F,$$

giving the polynomial F'. Note that $w(F) = w(F')$.

Define the following transformations on R,

$$\begin{aligned} T_1(X_1^4 + X_3^2 X_2) &= X_1^2 X_2 + 2X_1 X_3 \\ T_2(X_3^4 + X_1^2 X_2) &= X_3^2 X_2 + 2X_1 X_3 \\ T_3(X_1^2 X_2 + X_3^2 X_2) &= 2X_1 X_3 + X_2^2. \end{aligned}$$

Note that each T_i increases the weight of a polynomial by 1. Assume for the moment that either $\epsilon_1 = 1$ or $k > m$. Apply T_2 followed by T_1 to $F(F'$ if $\epsilon_1 = 0)$ $\frac{m-\epsilon}{4}$ times. Then apply T_3 ϵ_1 times. Since each T_i increases the weight by 1,

$$l(\beta) \geq 2\left(\frac{m-\epsilon}{4}\right) + \epsilon_1 + 1 = \frac{m-\epsilon_0}{2} + 1 = \left[\frac{m}{2}\right] + 1.$$

If $k = m$ and $\epsilon_1 = 0$, apply T_2 followed by T_1 to F' $\frac{m-\epsilon}{4} - 1$ times, apply T_2 one additional time and then apply T_3 $\epsilon_1 + 1 = 1$ time. As above

$$\begin{aligned} l(\beta) &\geq 2\left(\frac{m-\epsilon}{4} - 1\right) + 1 + \epsilon_1 + 1 + 1 \\ &= \left[\frac{m}{2}\right] + 1. \end{aligned}$$

Now, assume l, and hence s, is odd. Note that $k \equiv m + 2 \equiv 2(1-\epsilon_1) + \epsilon_0 (mod\ 4)$ with $0 \leq 2(1-\epsilon_1) + \epsilon_0 \leq 3$. Set $u = \frac{s-1}{2}$ and $v = \frac{3s-l-2\epsilon_0}{4}$, so

$$\begin{aligned} x &= \frac{k+m-2-2\epsilon_0}{4} = \frac{k+m-(2-2\epsilon_1+\epsilon_0+2\epsilon_1+\epsilon_0)}{4} \\ &= \frac{k-(2(1-\epsilon_1)+\epsilon_0)}{4} + \frac{m-\epsilon}{4} = \frac{k+4\epsilon_1-(\epsilon+2)}{4} + \frac{m-\epsilon}{4} \\ y &= 1 \\ z &= \frac{l-1+2\epsilon_0}{2}. \end{aligned}$$

An element of R corresponding to this solution is

$$\begin{aligned} F = &\left(\frac{k+4\epsilon_1-(\epsilon+2)}{4}\right) X_1^4 + \left(\frac{m-\epsilon}{4}\right) X_3^4 + (1-\epsilon_1) X_1^2 X_2 \\ &+ \epsilon_1 X_3^2 X_2 + \left(\frac{l-1}{2}\right) X_2^2 + \epsilon_0 X_1 X_3. \end{aligned}$$

Apply T_1 followed by T_2 or T_2 followed by T_1, according as $\epsilon_1 = 1$ or 0, to F $\frac{m-\epsilon}{4}$ times. Apply T_1 ϵ_1 times, obtaining

$$\begin{aligned} l(\beta) &\geq 2\left(\frac{m-\epsilon}{4}\right) + \epsilon_1 + 1 \\ &= \left[\frac{m}{2}\right] + 1. \end{aligned}$$

The first result is now immediate from Lemma 9.

Now assume $l = 0$. Here $s = k+m$ with $k \equiv m (mod\ 4)$. Moreover, any admissible solution of the Diophantine equation $4x + 3y + 2z = s$ must have $y = 0$. The Diophantine equation reduces to

$$2x + z = \frac{k+m}{2}$$

which has solution $z = \frac{k+m}{2} - 2x$ with $0 \leq z \leq m$. Hence $\frac{k-m}{4} \leq x \leq \frac{k+m}{4}$. However, each admissible solution must correspond to an element of R' of the form

$$aX_1^4 + bX_3^4 + cX_1X_3$$

with $x = a + b$ and $z = c$. Therefore,

$$4b + c = m \text{ so } z = c \equiv m (mod\ 4).$$

Thus $2x = \frac{k+m}{2} - z \equiv \frac{k-m}{2} (mod\ 4)$ or

$$x \equiv \frac{k-m}{4} (mod\ 2).$$

Thus at most $\left[\frac{m}{4}\right] + 1$ of the solutions to the Diophantine equation are admissible, so

$$l(\beta) \leq \left[\frac{m}{4}\right] + 1.$$

On the other hand,

$$F = \left(\frac{k-\epsilon}{4}\right) X_1^4 + \left(\frac{m-\epsilon}{4}\right) X_3^4 + \epsilon X_1 X_3$$

corresponds to the solution $x = \frac{k+m-2\epsilon}{4}, z = \epsilon$. Let T_4 denote the transformation $T_4(X_1^4 + X_3^4) = 4X_1X_3$. Note that T_4, which increases the weight of a polynomial by 2, can be applied to F $\frac{m-\epsilon}{4}$ times. Hence

$$l(\beta) \geq \frac{m-\epsilon}{4} + 1$$

and so equality must hold.

§5. Elementary class group of order 8.

When H is an elementary abelian 2-group of rank 3, $D(H) = 4$ (see Olson [16]), so the Diophantine equation becomes

$$4x + 3y + 2z = s. \tag{*}$$

Here, it will be shown that $l(\beta)$ is a linear function in x_0 and y_0 where (x_0, y_0, z_0) is an admissible solution to (*) with $x = x_0$ maximal and $y = y_0$ maximal subject to $x = x_0$.

Each element of H has a unique expression in the form $X_\alpha = X_1^i \times X_2^j \times X_3^k$ with $0 \le i, j, k \le 1$, where X_1, X_2 and X_3 generate H. Denote α using the 3 digits $1 \cdot i\ 2 \cdot j\ 3 \cdot k$ and then omit any zero digits. Thus, for example $X_{13} = X_1 \times X_2^0 \times X_3$.

There are 21 irreducible blocks of H, 7 of each length 2,3, and 4. Those of length 2 are simply the squares of the non-identity elements of H. The irreducible blocks of length 3 and 4 are:

$$X_1X_2X_{12}, X_1X_3X_{13}, X_1X_{23}X_{123}, X_2X_3X_{23}, X_2X_{13}X_{123}, X_3X_{12}X_{123},$$

$$X_{12}X_{13}X_{23}, X_1X_2X_3X_{123}, X_1X_2X_{13}X_{23}, X_1X_3X_{12}X_{23}, X_1X_{12}X_{13}X_{123}, X_2X_3X_{12}X_{13},$$

$$X_2X_{12}X_{23}X_{123}, \text{ and } X_3X_{13}X_{23}X_{123}.$$

Let $k_\alpha = \Omega(X_\alpha)$. Since any three non-identity elements, not contained in a proper subgroup, generate H, we may choose X_1 and X_2 so that $k_1 \le k_2 \le k_\alpha$ for $\alpha \ne 1, 2$. Then choose $X_3 \ne X_{12}$ so that k_3 is minimal among the remaining k_α.

Lemma 11. *Assume (x_0, y_0, z_0) is an admissible solution to (*) with $y = y_0$ maximal for $x = x_0$. If $x = x_1 = x_0 - 1$, $y = y_1$ and $z = z_1$ is another admissible solution, then $y_1 \le y_0 + 2$.*

Proof: Let F_1 in R' correspond to the solution (x_1, y_1, z_1). Suppose $y_1 > y_0 + 2$. If F_1 contains two different blocks of length 3, say $X_1X_2X_{12}$ and $X_1X_3X_{13}$, then applying

$$T_0(X_1X_2X_{12} + X_1X_3X_{13}) = X_2X_3X_{12}X_{13} + X_1^2$$

gives an F corresponding to an admissible solution with $x = x_0$ and $y = y_1 - 2 > y_0$, contradicting the choice of y_0. Hence, we may assume that F_1 contains only one type of irreducible block of length 3, say $X_1X_2X_{12}$.

Suppose now that F_1 contains at least two types of square terms disjoint from $X_1X_2X_{12}$, say X_{13}^2 and X_{23}^2. Applying

$$T_1(X_1X_2X_{12} + X_{13}^2 + X_{23}^2) = X_1X_2X_{13}X_{23} + X_{12}X_{13}X_{23}$$

gives an admissible solution with $x = x_0$ and $y = y_1 > y_0$, again contradicting the choice of y_0. Therefore we may assume that F_1 contains at most one such square term, say X_{23}^2.

If F_1 contains the block $X_3X_{13}X_{23}X_{123}$ then applying

$$T_2(X_3X_{13}X_{23}X_{123} + X_1X_2X_{12}) = X_1X_2X_3X_{123} + X_{12}X_{13}X_{123}$$

yields an element of R' with two types of blocks of length 3 corresponding to the admissible solution (x_1, y_1, z_1) which was seen to give a contradiction.

Now suppose that F_1 contains the block X_{23}^2 and a block of length 4 which does not contain X_{23}, say $X_1X_2X_3X_{123}$. Applying

$$T_3(X_1X_2X_3X_{123} + 2X_1X_2X_{12} + X_{23}^2) = X_2X_{12}X_{23}X_{123} + X_1X_3X_{12}X_{23} + X_1^2 + X_2^2$$

gives an admissible solution with $x = x_0$ and $y = y_1 - 2 > y_0$, again contradicting the maximality of y_0. Thus F_1 can contain only one type of block of length 3, one type of block of length 2 which is disjoint from the block of length 3, and no block of length 4 disjoint from either. Therefore, if F_1 contains an X_{23}^2 term, the only blocks of length 4 which can occur are:

$$X_1X_2X_{13}X_{23}, X_1X_3X_{12}X_{23}, \text{and} X_2X_{12}X_{23}X_{123}.$$

Since X_3, X_{13} and X_{123} can occur only in blocks of length 4, $x_1 = k_{13} + k_3 + k_{123}$. But every irreducible block of length 4 must contain at least one element of $\{X_{13}, X_3, X_{123}\}$, in particular, $x_0 \leq k_{13} + k_3 + k_{123} = x_1 = x_0 - 1$. Thus we may assume F_1 contains no X_{23}^2 block as well as no $X_3X_{13}X_{23}X_{123}$ block.

Now every block of length 4 in F_1 contains exactly two of the elements X_3, X_{13}, X_{23} and X_{123}. Moreover, since these elements can occur only in blocks of length 4, $x_1 = \frac{1}{2}(k_3 + k_{13} + k_{23} + k_{123})$. Label the irreducible blocks of length 4 as $A_1, \ldots, A_7$ and let a_i denote the maximum number of A_i which can occur in a partition of S. Then

$$a_1 + a_2 + a_3 + a_7 \leq k_3$$

$$a_3 + a_4 + a_5 + a_7 \leq k_{13}$$

$$a_2 + a_4 + a_6 + a_7 \leq k_{23}$$

$$a_1 + a_5 + a_6 + a_7 \leq k_{123}$$

where the blocks are labelled so that X_α for $\alpha \in \{3, 13, 23, 123\}$ occurs in block A_i if and only if a_i occurs in the inequality for k_α. Thus $2(a_1 + \cdots + a_6 + 2a_7) \leq k_3 + k_{13} + k_{23} + k_{123}$. In particular, $x_0 \leq a_1 + \cdots + a_7 \leq \frac{1}{2}(k_3 + k_{13} + k_{23} + k_{123}) = x_1$, a contradiction. Thus no F_1 can exist with $y_1 > y_0 + 2$.

Let $x = -s + u + v, y = s - 2u$ and $z = s + u - v$ be a parameterization of the solutions to (*) as in the proof of Lemma 9.

LEMMA 12. *Suppose $x = x_0, y = y_0$ and $z = z_0$ is an admissible solution to (*) with x_0 maximal and y_0 maximal with $x = x_0$. If $u = u_0$ and $v = v_0$ are the values of the parameters corresponding to this solution, then $v \leq v_0$ for all admissible solutions to (*).*

PROOF: Let (x_1, y_1, z_1) be an admissible solution with $x_0 - x_1 = t$. It follows from Lemma 11 that $y_1 \leq y_0 + 2t$ so that $u_0 - u_1 = \frac{1}{2}(y_1 - y_0) \leq t$. Thus, $t = x_0 - x_1 = (u_0 - u_1) + (v_0 - v_1) \leq t + v_0 - v_1$ and so $v_1 \leq v_0$.

LEMMA 13. *If $x = x_1, y = y_1$ and $z = z_1$ is an admissible solution with z_1 maximal, then the corresponding $v = v_1$ is minimal for the set of all admissible solutions.*

PROOF: Clearly $z_1 \leq \sum_\alpha \left[\frac{k_\alpha}{2}\right] = \sigma$. Since (β) is principal

$$k_1 + k_{12} + k_{13} + k_{123} \equiv 0(mod\ 2)$$

$$k_2 + k_{12} + k_{23} + k_{123} \equiv 0(mod\ 2)$$

$$k_3 + k_{13} + k_{23} + k_{123} \equiv 0(mod\ 2)$$

and so, exactly 0,3,4 or 7 of the k_α are even (odd). Moreover, if exactly 3 or 4 of the k_α are odd, the corresponding X_α's form an irreducible block of length 3 or 4 respectively. If all 7 k_α are odd, then clearly they can be partitioned into one block of length 3 and one of length 4. Hence there exists an admissible solution with $x_1 \leq 1, y_1 \leq 1$ and $z_1 = \sigma$. Since $y_1 = s - 2u_1$ and $x_1 = -s + u_1 + v_1$ with x_1 and y_1 minimal, u_1 maximizes u and v_1 minimizes v.

LEMMA 14. *Let $x = x_0, y = y_0$ and $z = z_0$ be the admissible solution to (*) with $x = x_0$ maximal and $y = y_0$ maximal with $x = x_0$. Let $x = x_1, y = y_1$ and $z = z_1$ be the admissible solution to (*) with z_1 maximal. Then $l(\beta) \leq x_0 - x_1 + \frac{y_0 - y_1}{2} + 1$. Moreover, $x_1 \leq 1, y_1 \leq 1$ and $x_1 = 1$ exactly when 4 or 7 k_α are odd and $y_1 = 1$ exactly when 3 or 7 k_α odd.*

PROOF: Let $f = x + y + z$ where $4x + 3y + 2z = s$. Then $f = \frac{s-y}{2} - x = s - v$. If (x, y, z) is an admissible solution to (*) then f is the weight of a corresponding F in R'. Now $l(\beta)$ is the number of weights of F in R'. Since $f = s - v$, the maximal and minimal weights are obtained when v is minimal and maximal, respectively. From Lemma 12 and Lemma 13, these values are given by $v = v_1$ and $v = v_0$ respectively. Hence

$$\begin{aligned} l(\beta) &\leq 1 + f_1 - f_0 \\ &= 1 + \frac{s - y_1}{2} - x_1 - \frac{s - y_0}{2} + x_0 \end{aligned}$$

$$= 1 + x_0 - x_1 + \frac{1}{2}(y_0 - y_1).$$

The exact values of x_1 and y_1 were determined in the proof of Lemma 13.

In order to determine x_0 and y_0, we construct an element F in R' of the form

$$F = m_1A_1 + m_2A_2 + m_3A_3 + m_4B + n_1C_1 + n_2C_2 + n_3C_3$$

where the A's and B's and C's represent blocks of length 4,3 and 2 respectively. Choose the A_i and m_i as follows: $A_1 = X_1X_{12}X_{13}X_{123}$, $m_1 = k_1$, $A_2 = X_2X_{12}X_{23}X_{123}$ and $m_2 = min\{k_2, k_{12} - m_1, k_{123} - m_1\}$. If $m_2 = k_{123} - m_1$, then $A_3 = X_2X_3X_{12}X_{13}$ and $m_3 = min\{k_2 - m_2, k_3, k_{12} - (m_1 + m_2), k_{13} - m_1\}$, otherwise $A_3 = X_3X_{13}X_{23}X_{123}$ and $m_3 = min\{k_3, k_{13} - m_1, k_{23} - m_2, k_{123} - (m_1 + m_2)\}$.

The choice for B depends on m_2 and m_3 as follows:

If $m_2 = k_2$ and $m_3 = k_3$ or $m_3 = k_{123} - (m_1 + m_2)$, then $B = X_{12}X_{13}X_{23}$ and

$$m_4 = min\{k_{12} - (m_1 + m_2), k_{13} - (m_1 + m_3), k_{23} - (m_2 + m_3)\}.$$

If $m_2 = k_2$ and $m_3 = k_{13} - m_1$ or $m_3 = k_{23} - m_3$, then $B = X_3X_{12}X_{123}$ and

$$m_4 = min\{k_3 - m_3, k_{12} - (m_1 + m_2), k_{123} - (m_1 + m_2 + m_3)\}.$$

If $m_2 = k_{12} - m_1$ and $m_3 = k_{13} - m_1$ or $m_3 = k_{123} - (m_1 + m_2)$, then $B = X_2X_3X_{23}$ and

$$m_4 = min\{k_2 - m_2, k_3 - m_3, k_{23} - (m_2 + m_3)\}.$$

If $m_2 = k_{12} - m_1$ and $m_3 = k_{23} - m_2$ or $m_3 = k_3$, then $B = X_2X_{13}X_{123}$ and

$$m_4 = min\{k_2 - m_2, k_{13} - (m_1 + m_3), k_{123} - (m_1 + m_2 + m_3\}.$$

If $m_2 = k_{123} - m_1$ and $m_3 = k_2 - m_2$ or $m_3 = k_3$, then $B = X_{12}X_{13}X_{23}$ and

$$m_4 = min\{k_{12} - (m_1 + m_2 + m_3), k_{13} - (m_1 + m_3), k_{23} - m_2\}.$$

If $m_2 = k_{123} - m_1$ and $m_3 = k_{12} - (m_1 + m_2)$ or $m_3 = k_{13} - m_1$, then $B = X_2X_3X_{23}$ and

$$m_4 = min\{k_2 - (m_2 + m_3), k_3 - m_3, k_{23} - m_2\}.$$

The C_i represent the remaining X_α in $S(\beta)$ which must occur in pairs.

LEMMA 15. *The polynomial F defined above has minimal weight in R'.*

PROOF: In each case F corresponds to an admissible solution of $4x + 3y + 2z = s$ with x maximal and y maximal for the value of x. By Lemma 12, the corresponding $v = v_0$ is maximal. Since $w(F) = x + y + z = s - v$ is minimal when v is maximal, the result follows.

Set $\epsilon_i \equiv m_i (mod\ 2)$ $\epsilon_i = 0$ or 1 for $1 \leq i \leq 4$. By Lemma 13, $F' = \epsilon A + \epsilon_4 B +$ squares has maximal weight in R', where $\epsilon = 1$ if exactly 4 or 7 k_α are odd and $\epsilon = 0$ if exactly 4 or 7 k_α are even, $\epsilon_4 = 1$ if exactly 3 or 7 k_α are odd and $\epsilon_4 = 0$ if exactly 3 or 7 k_α are even.

LEMMA 16. *Let F and F' be as above. If $k_{12} \neq 0$ then for any integer γ with $w(F) \leq \gamma \leq w(F')$ there exists an element F_1 in R' with $w(F_1) = \gamma$.*

PROOF: Suppose there is a series of transformations, which when applied to F yields F'. If each of these transformations increases the weight by at most one, then there is an F_1 with $w(F_1) = \gamma$. Thus we must show that such a series exists.

First assume $m_1 = m_2 = m_3 = 0$. Here $F = m_4B+$ squares. If $m_4 \leq 1$, then $F = F'$ and the lemma is trivially true. If $m_4 > 1$, then apply $T_4(2B) = C_1+C_2+C_3$, $\frac{m_4-\epsilon_4}{2}$ times. Observe that each application of T_4 increases the weight by one.

Now suppose at least two of m_1, m_2 and m_3 are positive, say $m_2 > 0$ and $m_1 > 0$ or $m_3 > 0$. Define $T_7(A_i + A_j) = A_{ij} + C + C'$; e.g., $T_7(A_1 + A_2) = X_1X_2X_{13}X_{23} + X_{12}^2 + X_{123}^2$.

Note that $T_7(A_i + A_{ij}) = A_j +$ squares and that T_7 increases the weight by one. One sequence of transformations taking F to F' is as follows:

Apply T_7 to $A_1 + A_2$ and then to $A_1 + A_{12}$ $\frac{m_1-\epsilon_1}{2}$ times, followed by T_7 to $A_2 + A_3$ and then to A_2+A_{23}, $\frac{m_2+\epsilon_2}{2}-1$ times and finally apply T_7 to A_2+A_3 and $A_3+A_{23}\frac{m_3-\epsilon_3}{2}$ times. This yields

$$F_2 = \epsilon_1 A_1 + (2-\epsilon_2)A_2 + \epsilon_3 A_3 + m_4 B + \text{ squares.}$$

If $\epsilon_1 = \epsilon_2 = \epsilon_3 = 0$, then $F_2 = 2A_2 + m_4B+$ squares and this can be dealt with as in the case of exactly one m_1, m_2 or m_3 being positive. Otherwise at least one $\epsilon_i \neq 0$ for some $i \leq 3$. Apply T_7 $\epsilon_1 + \epsilon_3 + 1 - \epsilon_2$ more times yielding $F_3 = A + m_4B+$ squares where A, the remaining block of length 4, depends on m_1, m_2 and m_3. Next apply T_4, $\frac{m_4-\epsilon_4}{2}$ times, yielding $F_4 = A + \epsilon_4 B+$ squares. If $\epsilon_4 = 0$ or A and B are disjoint, then no further transformations are possible. Otherwise, $T_6(A+B) = B'+$ squares can be applied one time. If $m_2 = 0$ and $m_1 > 0, m_3 > 0$, then interchanging A_2 and A_1 in the above sequence of transformations yields the desired result.

Now suppose exactly one of m_1, m_2 or m_3 is not zero, call it m. Then $F = mA + m_4B+$ squares. If $m = m_3$ and $m_4 = 0$, then since $k_{12} > 0, F$ contains a X_{12}^2 term, so the transformation

$$T_5(A_3 + X_{12}^2) = X_3X_{12}X_{123} + X_{12}X_{13}X_{23}$$

can be applied. If $m_4 = 0$ and $m \neq m_3$, then $k_2 > 0$, so $k_\alpha > 0$ for $\alpha > 2$. If $m_1 \neq 0$, then apply

$$T_5(A_1 + X_{23}^2) = X_1X_{23}X_{123} + X_{12}X_{13}X_{23} = B' + B.$$

If $m_2 \neq 0$, then apply

$$T_5(A_2 + X_{13}^2) = X_2X_{13}X_{123} + X_{12}X_{13}X_{23} = B' + B.$$

Thus there is always a polynomial F_2 in R' such that $w(F) = w(F_2)$ and F_2 contains a block of length 3. In fact,

$$F_2 = (m - \epsilon_5)A + (m_4 + \epsilon_5)B + \epsilon_5 B' + \text{ squares}$$

where $\epsilon_5 = 1$ if $m_4 = 0$ and $\epsilon_5 = 0$ otherwise. Now suppose that A and B are not disjoint. We can apply $T_6(A + B) = B'+$ squares followed by $T_6(A + B') = B+$ squares for a total of $m - \epsilon_5$ transformations. Next apply $T_4(2B) = C_1 + C_2 + C_3$ and $T_4(2B') = C_1' + C_2' + C_3'$ as many times as necessary to get a polynomial F_3 with the coefficients of the B and B' terms to be 0 or 1. If $F_3 = B + B'+$ squares, then by applying the inverse of T_5 we get $F_4 = A+$ squares. Since T_5 does not change the weight of a polynomial, $w(F_3) = w(F_4) = w(F')$.

Now we must consider the case where the A and B are disjoint. This can occur only when $A = A_1 = X_1X_{12}X_{13}X_{123}$ and $B = X_2X_3X_{23}$. If $m_1 = 1$, then 4 or 7 k_α are odd and $x_0 = x_1 = 1$. Thus no transformation involving A will increase $w(F)$ and applying T_4 $\frac{m_4-\epsilon_4}{2}$ times will yield F' as in the case $m_1 = m_2 = m_3 = 0$. If $m_1 > 1$, then by applying

$$T_2(A + B) = A_2 + B_1 = X_2X_{12}X_{23}X_{123} + X_1X_3X_{13} \text{ to } F \text{ gives}$$

$$F_2 = (m_1 - 1)A_1 + A_2 + (m_4 - 1)B + B_1 + \text{ squares.}$$

This is similar to the case where at least two of m_1, m_2 or m_3 are positive.

THEOREM 17. *If $k_{12} \neq 0$, then $l(\beta) = m_1 + m_2 + m_3 + \frac{m_4-\epsilon_4}{2} + \delta$ where $\delta = 1$ if 0 or 3 k_α are odd and $\delta = 0$ if 4 or 7 k_α are odd.*

If $k_{12} = 0$, then $l(\beta) = \frac{m_3-\epsilon_3}{2} + 1$.

PROOF: By Lemma 14 $l(\beta) \leq x_0 - x_1 + \frac{y_0-y_1}{2} + 1$. By Lemma XVI, factorizations of all lengths between $w(F)$ and $w(F')$ occur when $k_{12} \neq 0$ and equality holds. By our choice of $F, x_0 = m_1+m_2+m_3$ and $y_0 = m_4$. By Lemma 14 $x_1 = 1$ when 4 or 7 k_α are odd and $x_1 = 0$ otherwise, so $\delta = 1-x_1$. Since $y_1 = \epsilon_4, l(\beta) = m_1+m_2+m_3+\frac{m_4-\epsilon_4}{2}+\delta$.

Since $k_1 \leq k_2 \leq k_{12}, k_1 = k_2 = 0$ and $m_1 = m_2 = 0$ when $k_{12} = 0$. Also $B = X_{12}X_{13}X_{23}$ so $m_4 = 0$. Thus $F = m_3A_3+$ squares and the only transformation possible is $T_8(2A_3) =$ squares. T_8 increases the weight by two and can be applied $\frac{m_3-\epsilon_3}{2}$ times. Thus there are $\frac{m_3-\epsilon_3}{2} + 1$ weights of polynomials in R'.

Corollary 18. *If $k_{12} \neq 0$ then $l(\beta) = 1$ if and only if one of the following is true:*

(a) Either 0 or 3 k_α are odd, $k_1 = k_2 = k_3 = 0$ and $min\{k_{12}, k_{13}, k_{23}\} \leq 1$.

(b) Exactly 4 k_α are odd, $k_1 = k_2 = 0, k_3 = 1$ and either $k_{13} = 1$ or $k_{23} = 1$.

(c) All 7 k_α are odd, $k_1 = k_2 = k_3 = 1$ and at least two of k_{12}, k_{13} or k_{123} are 1.

Proof: (a) From Theorem 17 $l(\beta) = m_1 + m_2 + m_3 + \frac{m_4-\epsilon_4}{2} + 1$ when 0 or 3 k_α are odd. Thus if $l(\beta) = 1, m_1 = m_2 = m_3 = 0$ and so $k_1 = k_2 = k_3 = 0$. Also $m_4 = \epsilon_4$ and $B = X_{12}X_{13}X_{23}$ so $min\{k_{12}, k_{13}, k_{23}\} \leq 1$.

Conversely, if no k_α are odd with $k_1 = k_2 = k_3 = 0$, then m_4 is even and $min\{k_{12}, k_{13}, k_{23}\} = 0$. Thus $m_1 = m_2 = m_3 = m_4 = 0$ and $l(\beta) = 1$. If exactly 3 k_α are odd and $k_1 = k_2 = k_3 = 0$, then $min\{k_{12}, k_{13}, k_{23}\} = 1$. Thus $m_1 = m_2 = m_3 = 0$ and $m_4 = \epsilon_4 = 1$ and so $l(\beta) = 1$.

(b) Here Theorem 17 shows that $l(\beta) = m_1 + m_2 + m_3 + \frac{m_4-\epsilon_4}{2}$. If $l(\beta) = 1$, then $m_1 = m_2 = 0, m_3 = 1$ and $m_4 = \epsilon_4 = 0$. Since $A_3 = X_3X_{13}X_{23}X_{123}$ and $B = X_{12}X_{13}X_{23}$, it follows that $k_1 = k_2 = 0, k_3 = 1$ and $k_{13} = 1$ or $k_{23} = 1$. Conversely, the given conditions force $l(\beta) = 1$.

(c) As above $l(\beta) = m_1 + m_2 + m_3 + \frac{m_4-\epsilon_4}{2}$. If $l(\beta) = 1$, then $F = A_1 + B+$ squares. Thus $k_1 = 1$. Because $A_1 = X_1X_{12}X_{13}X_{123}$ and $m_2 = m_3 = 0$, at least two of k_{12}, k_{13} and k_{123} are one. Since $k_2 \leq k_3 \leq k_\alpha$ for $\alpha = 13$ or 123, $k_2 = k_3 = 1$. Conversely, the given conditions force $l(\beta) = 1$.

COROLLARY 19. *If $k_{12} = 0$, then $l(\beta) = 1$ if and only if $k_3 \leq 1$.*

PROOF: $l(\beta) = 1$ if and only if $m_3 = \epsilon_3$. Since $k_1 = k_2 = 0, m_3 = k_3$ and $k_3 = 0$ or $k_3 = 1$. Conversely, suppose $k_3 \leq 1$. Then $m_3 \leq 1$ and $m_3 = \epsilon_3$.

§6. Examples.

Let K be a number field with $h > 2$. Given any positive integer a, Sliwa [20] showed that it is possible to find an integer β such that $l(\beta) = a$ in K. In addition, Sliwa [18] has given asymptotic estimates for the number of non–associated integers β in K with $|N(\beta)| \leq x$ and $l(\beta) = a$. In this section, examples are given to illustrate how the results of this chapter may be used to determine such a β.

Example 1. $K = Q(\sqrt{-21})$, $F = Q(\sqrt{-1}, \sqrt{3}, \sqrt{7})$, and $H \approx Z_2 \times Z_2$. Let p be a rational prime such that $\left(\dfrac{-21}{p}\right) = 1$. Then $p = \mathfrak{p}_1\mathfrak{p}_2$ in K. Since every class has order 2, both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are in the same class. Thus we may talk about the class of the prime ideals above p without ambiguity. By class field theory, we see that the prime ideals above 5, 11 and 19 represent the three distinct nonprincipal classes. Let $n = 5 \cdot 11 \cdot 19$. Theorem 7 shows that $l(\beta) = a$ where $\beta = n^{a-1}$.

Example 2. $K = Q(\sqrt{-105})$, $F = Q(\sqrt{-1}, \sqrt{3}, \sqrt{5}, \sqrt{7})$, and $H \approx Z_2 \times Z_2 \times Z_2$. Again, every class has order 2, so we may refer to the class of the primes above a prime that splits in K. The primes: 11, 13, 19, 41, 43, 47 and 53 represent the seven non–principal classes of K. We will number the classes so that ideals with norms 11, 13 and 19 are in X_1, X_2 and X_3 respectively. Let $n = 41 \cdot 43 \cdot 47$. Then $k_1 = k_2 = k_3 = k_{123} = 0$ $k_{12} = k_{13} = k_{23} = 2$, $m_1 = m_2 = m_3 = 0$, $m_4 = 2$ and $\delta = 1$. Thus, Theorem 17 shows that $l(n^{a-1}) = a$.

Example 3. $K = Q(\sqrt{79})$ and $H \approx Z_3$. Let p be a rational prime such that $p = \mathfrak{p}_1\mathfrak{p}_2$ in K with neither $\mathfrak{p}_1$ nor $\mathfrak{p}_2$ principal. In this case, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are in distinct classes. Since the divisors of 3 are nonprincipal in K, if we set $n = p = 3$ then Theorem 7 shows that $l(n^{3a-3}) = a$.

Example 4. $K = Q(\sqrt{82})$ and $H \approx Z_4$. In this field we may choose the primes above the ramified prime 2 to represent the class of order 2 and the primes above 3 to represent the two classes of order 4. Thus, if $n = 2 \cdot 3^r$, $m = r$. It follows from Theorem 10 that $l(n) = a$ where $r = 2a - 2$.

Chapter III: Bicyclic Biquadratic Fields Which Contain Irreducible Rational Primes

§1. Introduction.

In an algebraic number field a rational prime may be irreducible, but still not generate a prime ideal. Proposition 9.6 of [13, p. 507] gives a necessary condition for a normal extension of the rational numbers to contain rational primes which do not ramify, but remain irreducible. Sliwa [19] gives a necessary and sufficient condition for the existence of irreducible rational primes in a normal extension K with Hilbert class field F, based on a characterization of the Galois group $G(F/Q)$. In this chapter we are primarily interested in the existence of rational primes which split completely in a given algebraic number field, but are irreducible. Such primes will be called sci primes.

It follows from Theorem 1 of §3 that a normal extension of the rationals of prime degree $l = 2, 3$ or 5 contains sci primes if and only if its class number is greater than 1. Moreover, any number field of degree greater than the Davenport constant of its class group does not contain sci primes.

In general, it seems to be difficult to characterize the normal extensions of the rational numbers that contain sci primes. The simplest case where this question is nontrivial is the bicyclic, biquadratic fields. In Theorem 2 of this chapter we give sufficient conditions for such fields to contain sci primes. The last two sections of this chapter are devoted to obtaining precise conditions for imaginary bicyclic biquadratic fields to contain sci primes.

If every ideal of a subfield $k \neq Q$ of a number field K becomes principal in K, then K contains no sci primes. However, the converse is not true even when K is an imaginary bicyclic biquadratic field. Assuming all imaginary quadratic fields with class numbers 2, 4 and 8 are known, see [3, 4, 7], we show there are exactly 88 imaginary bicyclic biquadratic fields such that the converse of the above statement is false. Such fields will be called exceptional fields.

§2. Notation.

Q:	Rational number field.
M, N, E, K:	Number fields.
k, k_i:	Subfields of K.
F:	Hilbert class field of K.
$H(k_i)$:	Class group of k_i.
h_i:	Class number of k_i.
Δ_i:	Discriminant of k_i.
t_i:	Number of distinct prime divisors of Δ_i.
p, q:	Rational primes.
$\mathfrak{p}, \mathfrak{q}, \mathfrak{p}_i, \mathfrak{q}_i$:	Primes of k, k_i.
P, Q:	Primes of K.
$\left[\dfrac{E/K}{\mathfrak{P}}\right]$:	Frobenius automorphism for the prime $\mathfrak{P}$ of E.
$\left(\dfrac{E/K}{P}\right)$:	Frobenius automorphism for all the primes in E lying above P in K. Here E/K must be abelian.
$N(\alpha) = N_{M/L}(\alpha)$:	The norm of α. We will drop the M/L when the extension is obvious.

The remaining notation is only defined when K is an imaginary bicyclic biquadratic field, k_0 its real quadratic subfield and k_1 and k_2 its imaginary quadratic subfields.

ρ:	Unit index of K/k_0.
ϵ:	Fundamental unit of k_0.
m_1, m_2:	Principal factors of the discriminant of k_0. We will take both values to be positive.
s:	Number of distinct prime divisors of (Δ_1, Δ_2).

2^{r_i}: Order of the subgroup of $H(k_i)$ which consists of the classes containing ideals that are principal in K.

2^{R_i}: Order of the subgroup of the genus group of k_i consisting of genera containing ideals that are principal in K. We will assume that the imaginary subfields of K are numbered so that $R_1 \geq R_2$.

$G_{k_i} = G_i$: Group of characters for the field k_i. Also the genus group for imaginary quadratic k_i.

$G'_{k_0} = G'_0$: Group of normalized characters for the real quadratic field k_0. Also the genus group of k_0.

$$\delta = \begin{cases} 1 & \text{if 2 is totally ramified in } K, \\ 0 & \text{otherwise.} \end{cases}$$

$$\lambda = \lambda(k_0) = \begin{cases} 0 & \text{if } p \mid \Delta_0 \text{ for some } p \equiv 3 \pmod 4, \\ 1 & \text{if } p \nmid \Delta_0 \text{ for all } p \equiv 3 \pmod 4. \end{cases}$$

§3. General results.

LEMMA 1. *Let K/k be a normal extension and N/k be an abelian extension. If E/K is an abelian extension with $N \subset E$ and E/k normal and if $\mathfrak{p} = P_1 \dots P_g$ is a prime of k which splits completely in K then $\left(\frac{E/K}{P_i}\right)\Big|_N = \left(\frac{N/k}{\mathfrak{p}}\right)$ for $i = 1, \dots, g$.*

PROOF: Let $\mathfrak{P}$ be a prime of E lying over P_1. Since $\mathfrak{p}$ splits completely in K, $\left(\frac{E/K}{P_1}\right)\Big|_N = \left[\frac{E/K}{\mathfrak{P}}\right]\Big|_N = \left[\frac{E/k}{\mathfrak{P}}\right]\Big|_N = \left(\frac{N/k}{\mathfrak{p}}\right)$.

LEMMA 2. *Let k, K, N, E be as in Lemma 1 with $[K : k] = n$. If $\mathfrak{p}$ is a prime of k which is unramified in E, then $\left(\frac{E/K}{\mathfrak{p}}\right)\Big|_N = \left(\frac{N/k}{\mathfrak{p}}\right)^n$.*

PROOF: Let $\mathfrak{p} = P_1 \dots P_g$ in K where each P_i has degree f over $\mathfrak{p}$, so $fg = n$. Let $\mathfrak{P}_i$

be a prime of E lying over P_i for each $i = 1, \ldots, g$. Then

$$\begin{aligned}
\left(\frac{E/K}{\mathfrak{p}}\right)\Big|_N &= \left(\frac{E/K}{P_1 \ldots P_g}\right)\Big|_N \\
&= \prod_{i=1}^{g} \left(\frac{E/K}{P_i}\right)\Big|_N \\
&= \prod_{i=1}^{g} \left[\frac{E/K}{\mathfrak{P}_i}\right]\Big|_N \\
&= \prod_{i=1}^{g} \left[\frac{E/k}{\mathfrak{P}_i}\right]^f\Big|_N \\
&= \prod_{i=1}^{g} \left[\frac{N/k}{\mathfrak{P}_i \cap N}\right]^f = \prod_{i=1}^{g} \left(\frac{N/k}{\mathfrak{p}}\right)^f \\
&= \left(\frac{N/k}{\mathfrak{p}}\right)^{fg} = \left(\frac{N/k}{\mathfrak{p}}\right)^n .
\end{aligned}$$

Lemma 3. *If K/k is an extension of degree n and I is an ideal of k which is principal in K, then every ideal in the class of I is principal in K. Moreover, I^n is principal in k.*

Proof: If $I = (\alpha)$ for some $\alpha \in K$ and $I \sim J$, then $J = (\beta)I$ for some $\beta \in k$, so $J = (\beta\alpha)$. Moreover, $I^n = N_{K/k}(I) = \big(N_{K/k}(\alpha)\big)$.

Theorem 1. *Let k/Q be a normal extension of prime degree $l = 2, 3$ or 5 and N be the Hilbert class field of k. Suppose K/k is a cyclic extension with $K \cap N = k$ and K/Q normal. If there exists a prime of k which does not become principal in K, then there are infinitely many rational primes which split into l primes in K and are irreducible.*

Proof: Let $\mathfrak{q}$ be a prime of k which does not become principal in K. Let $\tau = \left(\frac{N/k}{\mathfrak{q}}\right)$ and let σ generate $G(K/k)$. By assumption, $N \cap K = k$; thus $G(KN/k) \simeq G(K/k) \times G(N/k)$. By the Cebotarev Density Theorem, the set of primes $\mathfrak{P}$ of KN with $\left[\frac{KN/Q}{\mathfrak{P}}\right] = (\sigma, \tau)$ has positive density. We may assume that $\mathfrak{P}$ is unramified over Q.

Let $p = \mathfrak{P} \cap Q$ and $\mathfrak{p} = \mathfrak{P} \cap k$. Since $(\sigma, \tau) \in G(KN/k)$ and k/Q is normal, p splits completely in k, say $p = \mathfrak{p}_1 \ldots \mathfrak{p}_l$ where $\mathfrak{p}_1 = \mathfrak{p}$. Since $\left(\frac{K/k}{\mathfrak{p}}\right) = (\sigma, \tau)|_K = \sigma$, $\mathfrak{p}$ stays prime in K. Also, $\left(\frac{N/k}{\mathfrak{p}}\right) = (\sigma, \tau)|_N = \tau$ yielding $\mathfrak{p} \sim \mathfrak{q}$ in k. By Lemma 3, $\mathfrak{p}$ does not become principal in K. Since K/Q is normal, each $\mathfrak{p}_i$ stays prime in K and no $\mathfrak{p}_i$ becomes principal in K. If $l = 2$ or 3, it is clear that p is irreducible in K. Assume now $l = 5$ and $\mathfrak{p}_1\mathfrak{p}_2$ is principal in K. Since $G(k/Q)$ is transitive on the prime factors of p, there exists an automorphism σ of k/Q of the form $\sigma = (12abc)$ where $\{a, b, c\} = \{3, 4, 5\}$. Note σ^2 maps $\mathfrak{p}_1\mathfrak{p}_2$ to $\mathfrak{p}_a\mathfrak{p}_b$ so that $\mathfrak{p}_c$ is principal in K, contrary to assumption.

Corollary 1. *If K is a normal quartic number field with quadratic subfield k, such that $K \not\subseteq N$ and there is a prime of k which does not become principal in K, then there are infinitely many rational primes which split into two primes in K and are irreducible.*

Proof: Immediate from Theorem 1 with $l = 2$, since $K \not\subseteq N$ implies $K \cap N = k$.

For the remainder of this chapter, we specialize to the case where K is a bicyclic biquadratic field and k_0, k_1, and k_2 are its quadratic subfields.

Lemma 4. *Let p be a prime which splits completely in K. Then p is irreducible in K, if and only if, for each $i = 0, 1, 2$, the prime factors of p in k_i are not principal in K.*

Proof: Suppose $p = P_0P_1P_2P_3$ in K and $\mathfrak{p}_i = P_3 \cap k_i$ for $i = 0, 1, 2$. We may number P_0, P_1 and P_2 so that $\mathfrak{p}_i = P_iP_3$ for $i = 0, 1$ and 2. If p is irreducible in K, then no subproduct of P_0, P_1, P_2 and P_3 is principal in K, so in particular, $\mathfrak{p}_i$ is not principal in K for $i = 0, 1$, and 2.

Conversely, assume no $\mathfrak{p}_i$, $i = 0, 1$ and 2, is principal in K. Then no subproduct consisting of one or two P_i's can be principal, so no subproduct of the P_i's is principal. Thus p is irreducible in K.

LEMMA 5. *If in each $k_i, i = 1,2$ there exists a prime $\mathfrak{p}_i$ which splits completely and is nonprincipal in K, then there is a rational prime q which splits completely in K and has prime factors in both k_1 and k_2 which are not principal in K.*

PROOF: Let $\mathfrak{p}_i = P_i P_i'$ in K for $i = 1,2$, $\mathfrak{p}_1^* = P_2 \cap k_1$ and $\mathfrak{p}_2^* = P_1 \cap k_2$. If for either $i = 1$ or 2, $\left(\frac{F/K}{\mathfrak{p}_i^*}\right) \neq 1$, then set $q = \mathfrak{p}_i \cap Q = \mathfrak{p}_i^* \cap Q$. Thus we may assume that $\left(\frac{F/K}{\mathfrak{p}_1^*}\right) = \left(\frac{F/K}{\mathfrak{p}_2^*}\right) = 1$.

By hypothesis $\left(\frac{F/K}{\mathfrak{p}_1}\right) \neq 1$ and $\left(\frac{F/K}{\mathfrak{p}_2}\right) \neq 1$. Thus $\left(\frac{F/K}{\mathfrak{p}_1\mathfrak{p}_1^*}\right) \neq 1$ and so the ideal $\mathfrak{p}_1\mathfrak{p}_1^*$ is in a class of k_1 which does not become principal in K. Similarly, $\mathfrak{p}_2\mathfrak{p}_2^*$ belongs to a class of k_2 which does not become principal in K. Let $\tau = \left(\frac{F/K}{P_1P_2}\right) = \left(\frac{F/K}{P_1}\right)\left(\frac{F/K}{P_2}\right)$ and use the Cebotarev Density Theorem to obtain a prime ideal $\mathbb{Q}$ in F such that $\left[\frac{F/Q}{\mathbb{Q}}\right] = \tau$. Set $q = \mathbb{Q} \cap Q$ and $\mathfrak{q}_i = \mathbb{Q} \cap k_i$ for $i = 1,2$. Since $\tau|_K = 1$, q splits completely in K. By Lemma 1, $\tau|_{F_i} = \left(\frac{F_i/k_i}{\mathfrak{q}_i}\right)$ for $i = 1,2$. Since $\tau = \left(\frac{F/K}{P_1P_2}\right)$ it follows from Lemma 1 that $\tau|_{F_1} = \left(\frac{F_1/k_1}{\mathfrak{p}_1\mathfrak{p}_1^*}\right)$. Hence $\mathfrak{q}_1 \sim \mathfrak{p}_1\mathfrak{p}_1^*$. Similarly, $\mathfrak{q}_2 \sim \mathfrak{p}_2\mathfrak{p}_2^*$. Thus q splits completely in K and has prime factors in both k_1 and k_2 which do not become principal in K.

THEOREM 2. *Assume that k_1 and k_2 satisfy the conditions of the previous lemma. If, in addition, k_0 contains a prime ideal $\mathfrak{p}_0$ which splits completely in K and belongs to an ideal class whose square is not principal in K, then K contains an sci prime.*

PROOF: Let P be a prime divisor of $\mathfrak{p}_0$ in K, $\mathfrak{p}_1 = P \cap k_1$ and $\mathfrak{p}_2 = P \cap k_2$. If $\left(\frac{F/K}{\mathfrak{p}_1}\right) \neq 1 \neq \left(\frac{F/K}{\mathfrak{p}_2}\right)$ we are done. Thus we may assume $\left(\frac{F/K}{\mathfrak{p}_1}\right) = 1$. By Lemma 5, there exists a prime $\mathbb{Q}$ in K of degree 1 and index 1 over Q such that $\left(\frac{F/K}{\mathfrak{q}_1}\right) \neq 1 \neq \left(\frac{F/K}{\mathfrak{q}_2}\right)$ where $\mathfrak{q}_i = \mathbb{Q} \cap k_i$ for $i = 0,1,2$. If $\left(\frac{F/K}{\mathfrak{q}_0}\right) \neq 1$, then $\mathbb{Q} \cap Q$ is an sci prime. Assume $\left(\frac{F/K}{\mathfrak{q}_0}\right) = 1$ and let $\sigma = \left(\frac{F/K}{\mathbb{Q}}\right), \tau = \left(\frac{F/K}{P}\right)$. If

$\left(\frac{F/K}{\mathfrak{p}_2\mathfrak{q}_2}\right) = 1$, then set $\theta = \sigma\tau^2$. If $\left(\frac{F/K}{\mathfrak{p}_2\mathfrak{q}_2}\right) \neq 1$, then set $\theta = \sigma\tau$. By the Cebotarev Density Theorem, there exists a prime $\mathcal{L}$ of F with $\left[\frac{F/Q}{\mathcal{L}}\right] = \theta$. Let $l = \mathcal{L} \cap Q$ and $\mathfrak{l}_i = \mathcal{L} \cap k_i$ for $i = 0, 1, 2$. Since $\theta|_K = 1$, l splits completely in K.

We now show that l is irreducible in K. Let $j = 1$ or 2 so that $\theta = \sigma\tau^j$. By Lemma 1, $\left(\frac{F_i/k_i}{\mathfrak{l}_i}\right) = \theta|_{F_i} = \sigma\tau^j|_{F_i} = \left(\frac{F_i/k_i}{\mathfrak{q}_i\mathfrak{p}_i^j}\right)$ so $\mathfrak{l}_i \sim \mathfrak{q}_i\mathfrak{p}_i^j$ in k_i. Thus for $i = 1$,

$$\left(\frac{F/K}{\mathfrak{l}_1}\right) = \left(\frac{F/K}{\mathfrak{q}_1\mathfrak{p}_1{}^j}\right) = \left(\frac{F/K}{\mathfrak{q}_1}\right)\left(\frac{F/K}{\mathfrak{p}_1}\right)^j = \left(\frac{F/K}{\mathfrak{q}_1}\right) \neq 1.$$

For $i = 2$,

$$\left(\frac{F/K}{\mathfrak{l}_2}\right) = \left(\frac{F/K}{\mathfrak{q}_2\mathfrak{p}_2^j}\right) = \left(\frac{F/K}{\mathfrak{p}_2\mathfrak{q}_2}\right)\left(\frac{F/K}{\mathfrak{p}_2}\right)^{j-1} \neq 1.$$

For $i = 0$,

$$\left(\frac{F/K}{\mathfrak{l}_0}\right) = \left(\frac{F/K}{\mathfrak{q}_0}\right)\left(\frac{F/K}{\mathfrak{p}_0}\right)^j = \left(\frac{F/K}{\mathfrak{p}_0}\right)^j \neq 1.$$

By Lemma 4, l is irreducible in K.

<u>Example:</u> $K = Q(\sqrt{-13}, \sqrt{-14})$, $k_0 = Q(\sqrt{182})$, $k_1 = Q(\sqrt{-13})$ and $k_2 = Q(\sqrt{-14})$. Here $h_1 = h_2 = 2$ and $H(k_0)$ is cyclic of order 4. We will show in the next section that no nonprincipal class of any subfield becomes principal in K. It follows from Theorem 2 that K contains sci primes.

§4. Classes which become principal.

In this section we determine precisely which ideal classes of a quadratic subfield k of an imaginary bicyclic biquadratic field K become principal in K. Since only classes of order 1 or 2 in k can be principal in K, all classes which become principal are ambiguous for k/Q. When k is imaginary, all ambiguous classes contain an ambiguous ideal, i.e., an ideal whose prime factors are ramified over Q. When k is real, either all or half of the ambiguous classes contain ambiguous ideals. However, when k is real, it follows from Washington [13] that at most one nonprincipal class of k can become principal in K.

Since the problem is trivial unless $h(k) > 1$, we may assume that $K \neq Q(\sqrt{3}, \sqrt{-3})$ and $K \neq Q(\sqrt{2}, \sqrt{-2})$.

We shall adopt the following notation for the remainder of this chapter: $k_0 = Q(\sqrt{m}), k_1 = Q(\sqrt{n})$ and $k_2 = Q(\sqrt{n'})$ with $n < 0$, $m > 0$ and $n' = mn/d^2$. Here m, n, and n' are square free elements of Q and $d = (m, n)$. Also $<\tau> = G(K/k_0)$ and $<\sigma> = G(K/k_1)$.

LEMMA 6. *If $A = (\alpha)$ is a nonzero principal ideal of K which is ambiguous for K/k_0, then α can be chosen to have one of the following forms for some $\beta \in k_0$:*

(i) $\alpha = \beta$.

(ii) $\alpha = \sqrt{n}\beta$.

(iii) $\alpha = (1 + i)\beta$.

If, in addition, A is ambiguous for K/k_1, then there is a unit $\mu \in k_0$ such that $\alpha^\sigma = \mu\alpha$ when (i) or (ii) hold and $\alpha^\sigma = -i\mu\alpha$ when (iii) holds. Moreover, β can be chosen so that $\mu = \pm\epsilon^j$ with $j = 0$ or 1.

PROOF: Since A is ambiguous for K/k_0, $(\alpha) = A = A^\tau = (\alpha^\tau)$. Thus $\alpha^\tau = \mu\alpha$ for some unit μ in K. Since τ is complex conjugation on K, $\left|\dfrac{\alpha^\tau}{\alpha}\right| = |\mu| = 1$. Also K/Q is abelian, so all conjugates of $\dfrac{\alpha^\tau}{\alpha}$ have absolute value $+1$. Thus μ is a root of unity. By our assumptions on K, μ is a 2nd, 3rd, 4th or 6th root of unity.

If $\mu = 1$, then $\alpha = \alpha^\tau$ and $\alpha \in k_0$. If $\mu = -1$, then $\alpha = a\sqrt{n} + b\sqrt{n'} = \sqrt{n}\left(a + \dfrac{b}{d}\sqrt{m}\right)$, for some $a, b, \in Q$. When $\mu^3 = \pm 1, (\alpha^3)^\tau = \mu^3\alpha^3 = \pm\alpha^3$. Thus $\alpha^3 \in k_0$ or $\alpha^3 = \sqrt{n}\gamma$ where $\gamma \in k_0$. Since $[K : k_0] = 2$, either $\alpha = \beta$ or $\alpha = \sqrt{n}\beta$ for some $\beta \in k_0$.

If $\mu = \pm i$ and $\alpha = a + b\sqrt{-m} + c\sqrt{m} + ei$, then $a - b\sqrt{-m} + c\sqrt{m} - ei = \alpha^\tau = \pm i\alpha = \mp e \pm c\sqrt{-m} \mp b\sqrt{m} \pm ai$. Thus $e = \mp a$ and $b = \mp c$, yielding $\alpha = (1 \mp i)(a + c\sqrt{m})$. Since $(1 - i)i = i + 1$, we may write $\alpha = (1 + i)\beta$ with $\beta \in k_0$.

Now suppose that A is also ambiguous for K/k_1. Then $(\alpha) = (\alpha^\sigma)$ and $\alpha^\sigma = \omega\alpha$ for some unit $\omega \in K$. If $\alpha = \beta$ or $\alpha = \sqrt{n}\beta$, then $\beta^\sigma = \omega\beta$, so $\omega = \dfrac{\beta^\sigma}{\beta} \in k_0$. Here we set $\mu = \omega$. If $\alpha = (1+i)\beta$, then $(1-i)\beta^\sigma = \alpha^\sigma = \omega\alpha = \omega(1+i)\beta = i\omega(1-i)\beta$. Thus $\beta^\sigma = i\omega\beta$. Setting $\mu = i\omega = \dfrac{\beta^\sigma}{\beta}$, we have $\mu \in k_0$ and $\alpha^\sigma = -i\mu\alpha$.

Since $\mu \in k_0$, we may write $\mu = \pm\epsilon^{2i+j}$, where $j = 0$ or 1 and ϵ is the fundamental unit of k_0. Now $\beta^\sigma = \mu\beta$, so $(\epsilon^i\beta)^\sigma = (\epsilon^i)^\sigma\beta^\sigma = \pm(\epsilon^i)^\sigma\epsilon^{2i+j}\beta = \pm N_{k_0/Q}(\epsilon^i)\epsilon^j(\epsilon^i\beta)$. Hence, if β is replaced by $\epsilon^i\beta$, then $\mu = \pm\epsilon^j$.

LEMMA 7. *Let $A = (\alpha)$ be a principal ideal of K which is ambiguous for both K/k_1 and K/k_0. Let β and μ be determined as in Lemma 6. Then for some $c \in Q$:*

$$A = (c), (c\sqrt{n}) \text{ or } (c(1+i)) \text{ if } \mu = 1,$$

$$A = (c\sqrt{m}), (c\sqrt{n'}) \text{ or } (c(1+i)\sqrt{m}) \text{ if } \mu = -1 \text{ and}$$

$$A = (c(\epsilon^\sigma \pm 1)), (c\sqrt{n}(\epsilon^\sigma \pm 1)) \text{ or } (c(1+i)(\epsilon^\sigma \pm 1)) \text{ if } \mu = \pm\epsilon.$$

PROOF: When $\mu = 1, \beta^\sigma = \beta$ and $\beta \in k_1 \cap k_0 = Q$. Thus $\beta = c$ for some $c \in Q$. If $\mu = -1$, then $\beta = c\sqrt{m}$. When $\mu = \pm\epsilon$, let $\beta = a + b\sqrt{m}$ and $\epsilon = u + v\sqrt{m}$ with $a, b, u, v \in Q$. Then $a - b\sqrt{m} = \beta^\sigma = \mu\beta = \pm(u + v\sqrt{m})(a + b\sqrt{m}) = \pm\left[(ua + bvm) + (ub + av)\sqrt{m}\right]$ and $-b = \pm(ub + av)$ so $-av = b(u \pm 1)$. Hence $-v\beta = b(u \pm 1) - vb\sqrt{m} = b\left[(u - v\sqrt{m} \pm 1\right] = b(\epsilon^\sigma \pm 1)$. Setting $c = -b/v$ yields $\beta = c(\epsilon^\sigma \pm 1)$. The results follow from Lemma 6.

LEMMA 8. *If $\mu = \pm\epsilon$, then $N(\epsilon) = +1$.*

PROOF: Since $\beta^\sigma = \pm\epsilon\beta$, $\beta = \pm\epsilon^\sigma\beta^\sigma = (\pm\epsilon^\sigma)(\pm\epsilon)\beta$ and $\epsilon^{1+\sigma} = N(\epsilon) = +1$.

When $N(\epsilon) = +1$, there are two integers α_1 and α_2, unique up to associates, such that $\alpha_1\alpha_2 = \sqrt{m}\epsilon$ or $\sqrt{4m}\epsilon$ and $\epsilon = \alpha_1^2/N(\alpha_1) = -\alpha_2^2/N(\alpha_2)$, see Barrucand and Cohn [2]. Since $\epsilon(\epsilon^\sigma + 1) = \epsilon + 1$, $\epsilon = (\epsilon+1)/(\epsilon^\sigma + 1) = (\epsilon+1)^2/N(\epsilon+1)$. Similarly, $\epsilon = -(\epsilon-1)^2/N(\epsilon-1)$. Thus $(\epsilon+1) = (r_1)(\alpha_1)$ and $(\epsilon-1) = (r_2)(\alpha_2)$ for some rational integers r_1 and r_2. Set $m_1 = |N(\alpha_1)|$ and $m_2 = |N(\alpha_2)|$. Then m_1 and m_2 are called principal factors of the discriminant of k_0.

Let C be an ideal class of the imaginary quadratic subfield k_1 which becomes principal in K. By Lemma 3, C is an ambiguous class for k_1/Q. Since k_1 is imaginary, every ambiguous class is strongly ambiguous, so we may choose an ideal A in C such that A is an ambiguous ideal for k_1/Q. By removing rational factors, we may assume that A is square free and only divisible by prime ideals which are ramified over Q.

LEMMA 9. *Let A be a square free ideal of k_1, without rational factors, which becomes principal in K and is ambiguous for k_1/Q. If $\mu = \pm\epsilon$, then $N_{k_1/Q}(A) = m_1, -n/m_1, -4n/m_1, m_2, -n/m_2$ or $-4n/m_2$, except when $i \in K$, then $m_1/2$, $2m_1$, $m_2/2$, and $2m_2$ are also possible.*

PROOF: Set $a = N_{k_1/Q}(A)$ and note that a divides the discriminant of k_1 and that a is square free. It follows from Lemma 7 and the remarks preceding this Lemma that a is $c^2r^2m_0, -c^2r^2nm_0$ or $c^2r^22m_0$ where r is a rational integer and $m_0 = m_1$ or m_2. In the first case, $c^2r^2 = 1$ and $a = m_1$ or m_2. In the other cases, $c^2r^2d^2 = 1$ where $d = (n, m_0)$ or $d = (2, m_0)$. Hence $a = -nm_0/d^2$ or $a = 2m_0/d^2$. By assumption $a|n$ or $a|4n$. If $a|n, a = -nm_0/d^2$, and $i \notin K$, then m_0 also divides n and $m_0 = d$ yielding $a = -n/m_0$. Similarly, if $a|4n$ but $a \nmid n$, then $m_0 \equiv a \equiv 0 \pmod 2$ and $a = -4n/m_0$. If $i \in K$ and $a = 2m_0/d^2$, then $d = 1$ or 2, so $a = 2m_0$ or $m_0/2$.

LEMMA 10. *If $i \notin K$, then the unit index $\rho = 2$ if and only if $n = -m_1$ or $n = -m_2$. When $i \in K, \rho = 2$ if and only if 2 is a principal factor in k_0.*

PROOF: In Kuroda [12] it is shown that $\sqrt{\epsilon} = 1/2\left(\sqrt{N(\epsilon+1)} + \sqrt{-N(\epsilon-1)}\right) = 1/2(r_1\sqrt{m_1} + r_2\sqrt{m_2})$. In Satz 12 of [12], it is shown that $\rho = 2$ if and only if there exists a root of unity $\omega \in K$ with $\sqrt{\omega} \notin K$ such that $\sqrt{\omega\epsilon} \in K$. If $i \notin K$, take $\omega = -1$ and $\sqrt{-\epsilon} \in K$ if and only if $\sqrt{-m_1}$ and $\sqrt{-m_2} \in K$, i.e., if and only if $n = -m_1$ or

$-m_2$ and $n' = -m_2$ or $-m_1$. If $i \in K$, the result is immediate from Satz 13 of [12].

THEOREM 3. *Let D be the set of divisors of Δ_0 and let N be defined as follows:*

$$N = \begin{cases} \{1, -n\} & \text{if } i \notin K \text{ and } \rho = 1, \\ \{1, 2\} & \text{if } i \in K \text{ and } \rho = 1, \\ \{1\} & \text{if } \rho = 2. \end{cases}$$

Then $|D \cap N|$ is the number of classes of the real subfield k_0 which are principal in K.

PROOF: Let A be an ideal of k_0 which is principal in K. Then A is ambiguous for K/k_0. By Lemma 6, $A = (\alpha)$ where $\alpha = (a + b\sqrt{m}), \sqrt{n}(a + b\sqrt{m})$ or $(1 + i)(a + b\sqrt{m})$. In the first case A is principal in k_0. In the second and third cases $A = (a + b\sqrt{m})B$ where $N(B) = -n$ or $N(B) = 2$. If $N(B) = -n$, then in K, $B = (\sqrt{n})$. Since $(\sqrt{n})$ is an ambiguous ideal for K/Q, B is ambiguous for k_0/Q. Thus $-n \in D$. If $\rho = 1$ and $i \notin K$, then $-n \neq m, m_1$, nor m_2; hence, B is not principal in k_0. If $i \in K$ or $\rho = 2$, then B is principal in k_0.

Similarly if $i \in K$ and $N(B) = 2$, then $B = (1 + i)$ in K and B is ambiguous for K/Q. Thus $2 \in D$. If $\rho = 1$, then B is not principal in k_0, but the class containing B becomes principal in K. However, if $\rho = 2$, B is principal in k_0 and no nonprincipal class is principal in K.

THEOREM 4. *Let D be the set of divisors of the discriminant of the imaginary quadratic field $k = Q(\sqrt{n})$ and let M be defined as follows:*

$$M = \begin{cases} \{1, m\} & \text{if } i \notin K \text{ and } \rho = 2 \text{ or } N(\epsilon) = -1 \\ \{1, 2\} & \text{if } i \in K \text{ and } \rho = 2 \text{ or } N(\epsilon) = -1 \\ \{1, m_1, m_2, m\} & \text{if } i \notin K, \rho = 1 \text{ and } N(\epsilon) = +1 \\ \{1, m_1, 2, 2m_1\} & \text{if } i \in K, \rho = 1 \text{ and } N(\epsilon) = +1. \end{cases}$$

Then $|D \cap M|$ is the number of classes of k which are principal in K.

PROOF: Let C be a nonprincipal class of k which becomes principal in K. Since k is imaginary, we may choose an ambiguous ideal A in C such that A is square free, that is $N_{k/Q}(A) \in D$.

If $i \notin K$ and $N(\epsilon) = -1$, then it follows from Lemmas 7 and 8 that $\mu = -1$ and $A = (\sqrt{m})$ or $A = (\sqrt{n'})$ in K. Thus $N_{k/Q}(A) = m$ or $-n'$. Since $d^2n' = mn$, these norms represent ideals from the same class. It follows that one nonprincipal class of k becomes principal in K if and only if $m \in D$. If $i \in K$ and $N(\epsilon) = -1$, then $\mu = \pm 1$ and $A = (\sqrt{m}), A = (1+i)$, or $A = ((1+i)\sqrt{m})$ in K. But $n = -m$, so $(\sqrt{m}) = (\sqrt{-m})$ is principal in k. Since C is nonprincipal in k, $A = (1+i)$. Thus an ideal of k becomes principal if and only if k contains an ambiguous ideal with norm 2. If $N(\epsilon) = +1$ and $\rho = 2$, then as in Lemma 9, $N_{k/Q}(A)$ can also be m_1 or m_2, but this ideal is in the principal class of k by Lemma 10. Thus the only possibilities for a nonprincipal ideal A are the same as above.

If $N(\epsilon) = +1$ and $\rho = 1$, then by Lemma 10, neither principal factor of k_0 is the norm of a ramified principal ideal of k. If $i \notin K$, then Lemmas 7 and 9 give the possible values of $N_{k/Q}(A)$ as: $m, -n', m_1, m_2, -n/m_1, -n/m_2, -4n/m_1, -4n/m_2$. As above the ideals with norms m and $-n'$ are in the same class. Likewise, the ideals with norms m_1 and $-n/m_1$, m_2 and $-n/m_2, m_1$ and $-4n/m_1$, and m_2 and $-4n/m_2$ are in the same class. Thus the numbers m, m_1, and m_2 represent all of the possible distinct classes which become principal in K. Since the prime divisors of A are ramified over Q, each number occurs as the norm of A if and only if it is in D. It follows that $|D \cap M|$ is the number of classes of k which are principal in K.

If $i \in K$, then the ideal with norm m is principal in k. Since $\rho = 1$, Lemma 10 shows 2 is not a principal factor of k_0 so $2, m_1$, and m_2 are distinct. The possibilities for $N(A)$ are: $2, m/2, 2m, m_1, m_1/2, 2m_1, m_2, m_2/2$, and $2m_2$. The ideals of k having norms $2, m/2$, and $2m$ are necessarily in the same class. Also ideals of k having norms m_1 and m_2, or $m_1/2, m_2/2, 2m_1$, and $2m_2$ are in the same class. However, if they exist, ambiguous ideals with norms, $m_1, 2$, and $2m_1$ must be in distinct nonprincipal classes which become principal in K. Thus $|D \cap M|$ is the number of classes of k which are principal in K.

The order of the subgroup of $H(k_i)$ consisting of those classes which are principal in K will be denoted by 2^{r_i} for $i = 0, 1$ and 2. Theorems 3 and 4 tell us that $0 \leq r_0 \leq 1$ and $0 \leq r_i \leq 2$ for $i = 1, 2$. Relations between the r_i's with be obtained in the following corollaries. To simplify notation, we will number the imaginary quadratic subfields so that $r_2 \leq r_1$.

Corollary 1. *Suppose $r_1 = 2$. Then $r_0 = 1$ if and only if $n' = -1$ or -2, $h_0 > 1$, $\rho = 1$ and $2|\Delta_0$. If $h_2 > 1$, then $r_2 = 1$ if and only if 2 is totally ramified and 2 is a principal factor of k_0. Also $r_0 + r_2 \leq 1$.*

Proof: By Theorem 4, $r_1 = 2$ when there are nontrivial principal factors m_1 and m_2 such that $m_1 \cdot m_2|\Delta_1$. By Theorem 3, $r_0 = 1$ if and only if $\rho = 1$ and $n|\Delta_0$ when $i \notin K$ or $2|\Delta_0$ when $i \in K$. Since $m|\Delta_1$, if $n|\Delta_0$, then $n' = -1$ or $n' = -2$. Conversely, the conditions are sufficient to have $r_0 = 1$. However, when $k_2 = Q(i)$ or $k_2 = Q(\sqrt{-2})$, $h_2 = 1$ and $r_2 = 0$.

Suppose $r_2 = 1$, then $m_1|\Delta_2$. However $m_1|\Delta_1$ and $m_1|\Delta_0$, so $m_1 = 2$ is the only possibility. If $r_2 = 1$, then $h_2 > 1$ and $n' \neq -1$ or -2. Thus $r_0 + r_2 \leq 1$.

Corollary 2. *If $r_1 = 1$, then $r_2 = 1$ if and only if $h_2 > 1$ and one of the following conditions is satisfied:*

a) $m = 2$ or $m_1 = 2$ and 2 is totally ramified in K,

b) $m_1|\Delta_1$ and $m_2|\Delta_2$,

c) $m|\Delta_1, m_1 = 2, 2 \nmid \Delta_1$ but $2|\Delta_2$.

Proof: Suppose $h_2 > 1$ so $m \neq -n$. Since $r_1 = 1$, exactly one of m, m_1 or m_2 divides Δ_1. In order to have a class become principal from k_2 as well, $\rho = 1$ and one of these numbers must divide Δ_2. Up to renumbering the imaginary quadratic subfields, conditions a, b and c are the only way this can occur.

COROLLARY 3. *If* $r_0 = 1$ *and* $n' < -2$, *then* $r_1 \neq 2$. *Moreover,* $r_1 = 1$ *if and only if* $m_1|\Delta_1$. *Also* $r_1 = r_2 = 1$ *if and only if 2 is totally ramified in* K *and one of the following conditions is satisfied:*

a) $m_1 = 2$,

b) $m_1 = -2n$ *and* $m_2 = -n'/2$,

c) $m_1 = -n/2$ *and* $m_2 = -2n'$,

d) $m_1 = -n/2$ *and* $m_2 = -n'/2$.

PROOF: Suppose $r_0 = 1$ and $h_2 > 1$. It follows from Theorem 3 that $\rho = 1$ and $n|\Delta_0$ with $n \neq -m_1$ or $-m_2$. Since $n' < -2$ and $mn = d^2n'$, $m \nmid \Delta_1$. Hence $r_1 \neq 2$. From Theorem 4 we see that $r_1 = 1$ if and only if $m_1|\Delta_1$. Moreover, if $r_1 = r_2 = 1$, then either $m_1 = 2, 2|\Delta_1$ and $2|\Delta_2$ or $m_1|\Delta_1, m_1 \nmid \Delta_2$, but $m_2|\Delta_2$. In the first case, 2 is obviously totally ramified in K. Assume $m_1|\Delta_1$ and $m_2|\Delta_2$. Let p be an odd prime with $p|n$, then $p|m$ but $p \nmid n'$ so $p \nmid m_2$. It follows that $p|m_1$ if and only if $p|n$. Similarly, for an odd prime $q, q|m_2$ if and only if $q|n'$. Since $m_1 \neq -n$ and $m_2 \neq -n', m_1 = -2n$ or $-n/2$ and $m_2 = -2n'$ or $-n'/2$. In each case $2|\Delta_i$ for $i = 0, 1$ and 2. If $m_1 = -2n$ and $m_2 = -2n'$ then $m = m_1m_2/4 = nn' \equiv 3 \pmod 4$. But 2 is totally ramified in K, so $n \equiv n' \equiv 3 \pmod 4$ contradicting $m \equiv 3 \pmod 4$. Thus m_1 and m_2 cannot both be even, leaving conditions b, c and d.

Since $\rho = 1$, the converse follows immediately from Theorem 4.

§5 Applications of Genus Theory.

In many cases Theorems 2, 3 and 4 enable us to determine whether or not an imaginary bicyclic biquadratic field K contains sci primes. However, when the square of every ideal in each subfield is principal in K, these theorems do not apply. For example, we shall see that 53 is an sci prime in $K = Q(\sqrt{-15}, \sqrt{10})$ even though $h_0 = h_1 = h_2 = 2$. On the other hand, we shall see that $K = Q(\sqrt{-22}, \sqrt{-35})$

does not contain sci primes even though each subfield contains a prime which splits completely and remains nonprincipal in K. The genus structure of the quadratic subfields will be used to obtain these results and determine which imaginary K contain sci primes.

The genus of an ideal A of norm a in a quadratic field $k = Q(\sqrt{d})$ is determined by the values of Hilbert's norm residue symbols. If $l_1, \ldots, l_t$ are the prime divisors of the discriminant of k, then k has generic characters $\left(\frac{a,d}{l_i}\right)$ for $i = 1, \ldots, t$ (see Hancock [7] for details). When l_i is odd and $(a, l_i) = 1$, $\left(\frac{a,d}{l_i}\right) = \left(\frac{a}{l_i}\right)$ is the usual Legendre symbol. Similarly, if a is odd and $l_i = 2$

$$\left(\frac{a,d}{2}\right) = \begin{cases} \left(\frac{-1}{a}\right) & \text{if } d \equiv 3 \pmod 4, \\ \left(\frac{2}{a}\right) & \text{if } d/2 \equiv 1 \pmod 4, \\ \left(\frac{-2}{a}\right) & \text{if } d/2 \equiv 3 \pmod 4. \end{cases}$$

To simplify notation, define $\left(\frac{a}{2}\right) = \left(\frac{2}{|a|}\right)$.

If $l_i | (a, d)$, then $\left(\frac{a,d}{l_i}\right) = \left(\frac{-ad/l_i^2}{l_i}\right)$. Also $\left(\frac{|d|,d}{l_i}\right) = \left(\frac{a^2,d}{l_i}\right) = +1$.

The sequence $\left(\frac{a,d}{l_1}\right), \ldots, \left(\frac{a,d}{l_t}\right)$ is called the <u>character system of the integer a in k</u>. When a is the norm of an ideal in k, then $\prod_{i=1}^{t} \left(\frac{a,d}{l_i}\right) = +1$. The collection of all 2^{t-1} possible character systems with positive product form a group with the obvious multiplication. This group is called the <u>group of characters</u> for the field k and denoted by G_k.

When k is imaginary or when k is real and $\lambda = 1$, then the <u>character–system for the ideal A</u> is the character–system of $a = N_{k/Q}(A)$ in k. However, if k is real and $\lambda = 0$, then the character–system of A must be normalized. One way to accomplish this is as follows: Suppose $l_1 \equiv 3 \pmod 4$. Then for each $l_i \equiv 3 \pmod 4$ we replace

$\left(\frac{a,d}{l_i}\right)$ with the product $\left(\frac{a,d}{l_1}\right)\left(\frac{a,d}{l_i}\right)$ in the character–system. If $d \equiv 3$ or $d/2 \equiv 3 \pmod 4$, then the character at 2 is also normalized in the same manner. Since the normalized character at l_1 will be always positive, we need only consider the remaining $t-1$ characters. Again these $t-1$ values must have positive product when a is the norm of an ideal in k. The collection of all 2^{t-2} such possible normalized systems will be called the <u>group of normalized characters of k</u> and denoted by G'_k.

All ideals in a given class have the same normalized character–system and all classes with the same character–system belong to one genus. Thus there is a one–to–one correspondence between the genera of k and the group of (normalized) characters of k, with the genus of an ideal determined by its character–system. The principal class belongs to the principal genus which has a character–system consisting of only positive units. It is worthy of note that the square of every class is in the principal genus and every class in the principal genus is the square of some class.

In order for a rational prime p to split completely in k, the character–system of p in each subfield must have positive product. If, in addition, the character–system of p in each k_i places a prime factor $\mathfrak{p}_i$ of p in a genus which contains no class which becomes principal in k, then p is an sci prime. If for some $i, \mathfrak{p}_i$ is in a genus which only contains primes which become principal in K, then p is reducible in K.

In the first example, $K = Q(\sqrt{-15}, \sqrt{10})$, the primes above 53 belong to the nonprincipal genus in all three quadratic subfields while Theorems 3 and 4 show that all nonprincipal classes of each subfield remain nonprincipal in K. Thus 53 is an sci prime.

For $K = Q(\sqrt{-22}, \sqrt{-35})$ we number the subfields so that $k_0 = Q(\sqrt{770})$, $k_1 = Q(\sqrt{-22})$ and $k_2 = Q(\sqrt{-35})$. The possible character systems for ideals in each of the subfield are listed in the chart below.

k_0			k_1		k_2	
$\left(\frac{2}{x}\right)$	$\left(\frac{x}{5}\right)$	$\left(\frac{x}{7}\right)\left(\frac{x}{11}\right)$	$\left(\frac{2}{x}\right)$	$\left(\frac{x}{11}\right)$	$\left(\frac{x}{5}\right)$	$\left(\frac{x}{7}\right)$
+	+	+	+	+	+	+
+	−	−	+	+	−	−
−	+	−	−	−	+	+
−	−	+	−	−	−	−

Since $h_0 = 4$ and $h_1 = h_2 = 2$, each field has one class per genus. Thus K contains sci primes if and only if in each subfield the class belonging to the genus listed on the last line of the chart does not become principal in K. By Theorem 3 the ideals of k_0 with norm 22 and 35 become principal in K. However, an easy computation shows that these ideals are in the genus of k_0 which is listed on the bottom line. Thus every prime which splits completely in K belongs to an ideal class in some subfield that is principal in K. Hence K contains no sci primes.

THEOREM 5. *If each quadratic subfield of K contains primes that split completely in K, but do not become principal in K and if, for some j, there is a class in the principal genus of k_j that does not become principal in K, then K contains sci primes.*

PROOF: Since K/k is unramified for at most one subfield, we may assume that K/k_0 and K/k_2 are ramified extensions.

If $j = 0$ or 2, then the class group of this field has a cyclic factor of odd order or it contains an element of order 4 whose square is the element of the principal genus which does not become principal in K. Since K/k_j is ramified, every class contains primes which split in K. Thus Theorem 2 may be applied to show that K has sci primes.

Assume now that every class in the principal genus of k_0 and of k_2 is principal in K. Thus $j = 1$. If K/k_1 is ramified, the result follows as above. Hence we may assume that K/k_1 is unramified. This occurs only when G_0 and G_2 have no common characters so $G_0 \times G_2 \subseteq G_1$. Moreover, the elements of $G_0 \times G_2$ correspond to the genera of k_1 which contain primes that split completely in K. Here k_0 and k_2 must each have a genus which contains no ideals that become principal in K. There exists an element α in $G_0 \times G_2$ which corresponds to this genus in both k_0 and k_2. Since the principal genus of k_1 contains a class that does not become principal in K, every other genus of k_1 contains such a class. Let p be a rational prime whose divisors in k_1 belong to a class in α which does not become principal in k_1, then p must be an sci prime.

COROLLARY 1. *Assume $h_i > 2^{r_i}$ for $i = 0, 1, 2$ and that for some j there is a class in the principal genus of k_j which does not become principal in K. Then K contains sci primes if and only if one of the following holds:*

a) K/k_1 is ramified,

b) $h_1/|G_1| > 2^{r_1 - R_1}$,

c) $r_1 = 2$ and $\left(\dfrac{n'}{m_1}\right) + \left(\dfrac{n'}{m_2}\right) < 2$,

d) $r_1 = 2$, $\left(\dfrac{n'}{m_1}\right) = \left(\dfrac{n'}{m_2}\right) = 1$ and $h_1 > 8$,

e) $r_1 = 1$ and $\left(\dfrac{n'}{m}\right) = -1$,

f) $r_1 = 1$, $\left(\dfrac{n'}{m}\right) = +1$ and $h_1 > 4$.

PROOF: Suppose a) holds. Since K/k_i is ramified for $i = 0, 1$ and 2, every class in each subfield contains primes which split completely in K. There is a class in the principal genus of k_j which is not principal in K. Thus Theorem 5 applies to show that K contains sci primes.

Next suppose that b) holds. Since $h_1/|G_1|$ is the number of classes in each genus of k_1 and $2^{r_1 - R_1}$ is the number of classes in the principal genus which are principal in K, not all classes in the principal genus of k_1 can be principal in K. Thus k_1 contains primes which split completely in K and are not principal. Theorem 5 applies to show that K contains sci primes.

Assume for the remainder of the proof that $h_1/|G_1| = 2^{r_1-R_1}$ and that K/k_1 is unramified. This implies that $h_0/|G_0'| > 2^{r_0-R_0}$ or $h_2/|G_2| > 2^{r_2-R_2}$ and it follows from Theorem 4 that $r_1 > 0$. In order to use Theorem 5, we must show that each of conditions c), d), e), and f) implies the existence of classes in k_1 which do not become principal in K, but contain primes that split completely in K. If $r_1 = 2$ and $\left(\frac{n'}{m_1}\right) + \left(\frac{n'}{m_2}\right) < 2$, then only half of the classes of k_1 which become principal in K contain primes which split completely in K. Since $h_1/2 > 2^{r_1-1}$, k_1 contains classes which do not become principal yet split completely in K. If $\left(\frac{n'}{m_1}\right) = \left(\frac{n'}{m_2}\right) = +1$, then all the classes which become principal in K, split completely in K. Thus when $h_1 = 8$, all the classes which split in K become principal in K. It follows that K contains sci primes if and only if $h_1 > 8$.

If $r_1 = 1$ and $\left(\frac{n'}{m}\right) = -1$, the nonprincipal class of k_1 which becomes principal in K does not split in K. Thus $h_1 > 2^{r_1}$ implies that K contains sci primes. On the other hand, if $\left(\frac{n'}{m}\right) = +1$, then the nonprincipal class which becomes principal in K splits completely in K. Here k_1 contains primes which do not become principal in K and do split completely in K, if and only if $h_1 > 4$.

Since K contains sci primes only if, in each subfield there are primes which split completely in K and are not principal in K, it is necessary that one of the condition a), b), c), d), e), or f) holds.

Let G be a subgroup of $G_1 \times G_2$ such that $\alpha \in G$ if:

1) For each odd prime l dividing Δ_1 and Δ_2, the values of the common character at l are equal.
2) For $l = 2$ dividing Δ_1 and Δ_2 but not Δ_0, the values of the common character at 2 are equal.

If 2 is totally ramified in $K(\delta = 1)$, then an element of G will contain two distinct characters at 2 and they are not considered to be a common character. Thus $|G| = 2^{t_1+t_2-2-s+\delta}$, where $s-\delta$ is the number of common characters.

If l is a prime divisor of Δ_0 such that $l \nmid (\Delta_1, \Delta_2)$, then there is exactly one coordinate of $\alpha \in G$ corresponding to the prime l.

Define a function $f_1 : G \to G_0$ by $f_1(\alpha) = \beta$ where the coordinate at l in β is the coordinate at l in α. If 2 is totally ramified, then the character value at 2 in β in the product of the values for the characters at 2 in G_1 and G_2. Now, β is an element of G_0 if the product of the character values is $+1$. Since each element in G_1 and G_2 must satisfy the product condition, α has an even number of negative coordinates. The common coordinates are required to have the same sign, so the number of negative values in the non-common coordinates of α is also even. These are precisely the coordinates which determine the sign of the product in β.

Since we are interested in G_0' not G_0, we will define $f_0 : G_0 \to G_0'$ to be the normalization map and $f = f_1 \circ f_0 : G \to G_0'$. Notice that f_1 and f_0 are both homomorphisms in each coordinate. Thus f_1, f_0 and f are homomorphisms. While f_1 may not be onto, f_0 is clearly onto and we will show that f is onto as well.

Lemma 11. *If $(\Delta_1, \Delta_2) \neq 1$, then f_1 is onto.*

Proof: Let $\beta \in G_0$, then β has an even number of coordinates with negative values. If 2 is not totally ramified or if β has a positive 2–coordinate, then the negative coordinates of β may be partitioned into two subsets, those coordinates which occur in G_1 and those which occur in G_2. These sets have the same parity. If each has an even number of elements, then choose $\alpha_1 \in G_1$ and $\alpha_2 \in G_2$ such that all common characters, and the character at 2, if 2 is totally ramified, are positive. For all other coordinates set them equal to the values in β. If the parity is odd, then choose α_1 and α_2 such that the values at one common character or the characters at 2 are negative and all other common characters have positive values. Again set all other coordinates equal to the values in β. In this way we obtain $\alpha = (\alpha_1, \alpha_2)$ such that $f_1(\alpha) = \beta$.

If 2 is totally ramified and the 2–coordinate of β is negative, then the 2–coordinate of α_1 must be the negative of the 2–coordinate of α_2 and the partitioning as above of all the negative coordinates except that at 2 gives sets with opposite parity. Choose an $\alpha_1 \in G_1$ so that all common coordinates have positive value, the value of the 2–coordinate is the product of the values of the other coordinates of β from G_1, and the remaining coordinates have values identical to their values in β. Choose $\alpha_2 \in G_2$ in a similar manner. This gives an $\alpha \in G$ which maps to β.

LEMMA 12. *The function f is always onto.*

PROOF: If $(\Delta_1, \Delta_2) > 1$, then the result follows from Lemma 11 and the remarks proceeding it.

Suppose $(\Delta_1, \Delta_2) = 1$. Then either Δ_1 or Δ_2 is odd. Assume Δ_1 is odd. Then $|n| \equiv 3 \pmod 4$ and there is a prime $l_1 \equiv 3 \pmod 4$ such that $l_1 | \Delta_1$. Also $l_1 | \Delta_0$ and the character–system for k_0 must be normalized. Let u be the number of characters of k_0 which are normalized and note that u is even. Let $l_1, \ldots, l_u$ be the prime divisors of Δ_0 corresponding to these characters and use l_1 to normalize. Since $|n| \equiv 3 \pmod 4$, an odd number of these l_i must divide Δ_1, and hence, an odd number must divide Δ_2. For $\beta' \in G_0'$, choose $\beta \in G_0$ such that $f_0(\beta) = \beta'$. Partition the coordinates of β into two sets, one corresponding to the prime divisors of Δ_1, the other corresponding to the prime divisors of Δ_2. If each set has an even number of negative coordinates, then there is an $\alpha \in G_0$ with $f_1(\alpha) = \beta$ so $f(\alpha) = \beta'$. If both sets have an odd number of negative coordinates, then form a new β by changing the signs of the coordinates at $l_1, \ldots, l_u$. We now have a β with an even number of negatives in each set and $f_0(\beta) = \beta'$. As above choose $\alpha \in G$ with $f_1(\alpha) = \beta$.

LEMMA 13. *The kernel, K_f, of f has order $2^{s-\lambda}$.*

PROOF: $|G_1| = 2^{t_1-1}, |G_2| = 2^{t_2-1}$ and $|G_0'| = 2^{t_0-2+\lambda}$. Using the definition of s and δ we can write $t_0 = t_1 + t_2 - 2s + \delta$. From above, $|G| = 2^{t_1-1+t_2-1-(s-\delta)} = 2^{t_1+t_2-2-s+\delta} = 2^{t_0+s-2}$ so $|K_f| = \dfrac{|G|}{|G_0'|} = 2^{s-\lambda}$.

We will use f to determine if there is a rational prime p and a genus in each subfield containing a prime ideal $\mathfrak{p}_i$ above p which does not become principal in K. To this end we will call a genus of k_i <u>bad</u> or <u>good</u> depending on whether or not it contains a class of k_i which is principal in K. Let B_i be the set of bad genera of k_i. An element of G will be called <u>bad</u> if the restriction to G_1 or G_2 induces a bad genus; otherwise, it will be called <u>good</u>. The function f will be called <u>good</u> if there exists at least one good element of G which is mapped to a good element of G_0'. Obviously, if f is good, infinitely many sci primes exist.

Let 2^{R_i} denote the number of bad genera in k_i for $i = 0, 1, 2$. Since each class is contained in a genus and the bad classes form a subgroup of the class group, B_i is a subgroup of the genus group and $R_i \le r_i$ for $i = 0, 1, 2$. Thus the Corollaries to Theorem 4 can be used to determine the maximum values for R_0, R_1 and R_2 and under what conditions these values can occur. Since f is good only if each k_i contains a good genus, we may assume $R_i < t_i - 1$ for $i = 1$ and 2, $R_0 < t_0 - 2 + \lambda$, and that each discriminant has an odd prime divisor. We will also assume that $R_1 \ge R_2$, renumbering the imaginary fields if necessary.

LEMMA 14. *The number of bad elements of G is at most b where*

$$b = \begin{cases} 2^{\delta-s}\left(2^{R_1+t_2-1} + 2^{R_2+t_1-1}\right) - 1 & \text{if } t_1 \neq s-\delta \neq t_2. \\ 2^{\delta-s}\left(2^{R_1+t_2} + 2^{t_1-1}\right) - 1 & \text{if } t_2 = s-\delta. \end{cases}$$

PROOF: Suppose $t_1 \neq s-\delta$. Then $2^{t_1-1-(s-\delta)}$ elements of G induce a single element of G_2, and $2^{R_2}\left(2^{t_1-1-(s-\delta)}\right)$ elements of G induce elements of B_2. Similarly, if $t_2 \neq s-\delta$, then $2^{R_1}\left(2^{t_2-1-(s-\delta)}\right)$ elements of G induce elements of B_1. Since the principal element of G induces the principal element of G_1 and G_2, 1 is subtracted from the count and line 1 follows. However, if $t_2 = s-\delta$, then an element of G_1 is induced by at most one element of G and only half the elements of G_1 are induced by elements of G. Since the bad genera of k_1 form a subgroup of G_1, either all or half of the elements of B_1 are induced by elements of G. Thus, at most, 2^{R_1} elements of G induce elements of B_1. Since $t_2 = s-\delta$, $(\Delta_0, \Delta_2) = 1$. It follows from Theorem 4 that no nonprincipal ideal of k_2 becomes principal in K, i.e. $R_2 = 0$. Thus $2^{t_1-1-(s-\delta)}$ elements of G induce the bad element in G_2. Since this includes the principal element of G, 1 must be subtracted and line 2 follows.

Define a function

$$g = \begin{cases} 2^{t_1+t_2-2} - 2^{t_2-1+R_1} - 2^{t_1-1+R_2} + 2^{s-\delta} - 2^{2s+R_0-(\delta+\lambda)} & \text{if } t_1 \neq s \neq t_2 \text{ or } \delta = 1 \\ 2^{t_1+t_2-2} - 2^{t_2+R_1} - 2^{t_1-1} + 2^{t_2} - 2^{2t_2+R_0-(\delta+\lambda)} & \text{if } t_2 = s \text{ and } \delta = 0. \end{cases}$$

THEOREM 6. *For a given field K, if $g \geq 0$, then f is good.*

PROOF: The number of good elements of G is at least $|G| - b$. Also f maps $2^{R_0}|K_f|$ elements of G to bad elements of G_0'. By Lemma 13, $|K_f| = 2^{s-\lambda}$. Since the principal element of G is counted in both b and $|K_f|$, $g = 2^{s-\delta}(|G| - b - 2^{R_0}|K_f|) \geq 0$ implies that there are more good elements in G than can be mapped to elements of B_0; thus f is good.

COROLLARY 1. *If $s-\delta = 0$, then f is good when $g \geq 1 - 2^{R_1+R_2}$.*

PROOF: Since $s-\delta = 0, B_1 \times B_2 \subset G$ and $2^{R_1+R_2}$ elements of G induce bad elements in both G_1 and G_2. Thus the estimate for b in Lemma 14 can be improved by $2^{R_1+R_2} - 1$ elements.

COROLLARY 2. *If $s-\delta = 1$, then f is good when $g \geq 2(1 - 2^{R_1+R_2-1})$.*

PROOF: Since $s-\delta = 1$, k_1 and k_2 have one common character χ. Because $\chi : B_i \rightarrow$

$\{\pm 1\}$ for $i = 1, 2$ is a group homomorphism, either all or exactly half the elements of B_i will have value $+1$ at χ. Thus $|B_1 \times B_2 \cap G| \geq 1/2|B_1 \times B_2| = 2^{R_1+R_2-1}$. Again the estimate for b can be improved and f is always good when $g \geq 2^{s-\delta}(1 - 2^{R_1+R_2-1}) = 2(1 - 2^{R_1+R_2-1})$.

Corollary 3. *If $|K_f| \geq |G_2|$ and $R_2 = 1$ or if $|K_f| \geq |G_1|$ and $R_1 \geq 1$, then f is good when $g \geq -2^{s-\delta}$.*

Proof: Suppose $|K_f| \geq |G_2|$. By looking at the inducement map to G_2 restricted to K_f, we see that either every element of G_2 is induced by an element in K_f or the principal element of G_2 is induced by two or more elements in K_f. Since $R_2 = 1$, at least one nonprincipal element of K_f induces an element in B_2. Thus f is good when $g \geq -2^{s-\delta}$.

The proof is identical for $|K_f| \geq |G_1|$.

Corollary 4. *If $t_2 = 2$ and $R_2 = 0$, then f is good when $g > -2^{R_1}$. If $s - \delta = t_2 = 2$, then $g > -2^{R_1+1}$ is sufficient. If $t_2 = 2$ and $R_0 = 1$, then $g > -2^{2s-\delta-\lambda}$ is sufficient.*

Proof: Let B_i' be the subgroup of G containing those elements which induce bad elements of G_i for $i = 1$ or 2. Since $t_2 = 2$, B_2' consists of those elements with positive values at both coordinates in G_2. Hence the product of any 2 elements of $G - B_2'$ is in B_2'. In particular, $[B_1' : B_1' \cap B_2'] \leq 2$. Thus f is good when $g > -2^{s-\delta-1}|B_1'|$. It follows from Lemma 14 that

$$|B_1'| = \begin{cases} 2^{R_1+t_2-1-(s-\delta)} & \text{if } t_2 \neq s - \delta. \\ 2^{R_1+t_2-(s-\delta)} & \text{if } t_2 = s - \delta. \end{cases}$$

Similarly, $[K_f : K_f \cap B_2'] \leq 2$. Thus f is good when $g > -2^{s-\delta-1+R_0}|K_f| = -2^{2s-\delta-1+R_0-\lambda} = -2^{2s-\delta-\lambda}$ when $R_0 = 1$.

Corollary 5. *If $t_0 + \lambda = 3$ and $R_1 = 2$, then f is good when $g > -2^{t_2}$.*

Proof: When $R_1 = 2$, Theorem 4 requires that $m|\Delta_1$. Since $t_0 + \lambda = 3$, there exists either a prime $p_1 \equiv 1 \pmod 4$ or two primes $p_2 \equiv p_3 \equiv 3 \pmod 4$ which divide m. In the first case, an element is in K_f if and only if its character value at p_1 is $+1$. Thus any two elements of B_1' which are not in K_f, have a product which is in K_f. In the second case, p_2 normalizes the character at p_3, so an element of G is in K_f if and only if the character value at p_2 equals the character value at p_3. Again, the product of two elements not in K_f is in K_f. Thus $[B_1' : B_1' \cap K_f] \leq 2$. It follows that $|B_1' \cap K_F| \geq 1/2|B_1'|$. Thus f is good when $g > -2^{s-\delta}\left(2^{t_2-(s-\delta)}\right)$.

Corollary 6. *If $t_2 = 2$, $t_0 + \lambda = 3$ and $R_1 = 2$, then f is good when $g \geq -8 + 2^{s-\delta+1}$.*

Proof: Corollary 4 estimates $|B_1' \cap B_2'|$ and Corollary 5 estimates $|B_1' \cap K_f|$. Since Lemma 14 assumed that only the principal element was in $B_1' \cap B_2' \cap K_f$, we may improve our estimate by $|B_1' \cap B_2'| + |B_1' \cap K_f| - 2$.

Corollary 7. *If $s = t_2$, then f is good when $g \geq -2^{s-\delta}\left(2^{1+R_2-\lambda} - 1\right)$.*

Proof: If $\delta = 0$, then $G \approx G_0 \times G_2$. If $\delta = 1$, then $G \approx G_0^* \times G_2$ where the 2–coordinate of G_0^* is the 2–coordinate of G_1 and the other coordinates of G_0^* are the remaining coordinates of G_0. Note that the 2–coordinate of G_0 is the product of the 2–coordinates of G_2 and G_0^*. Let $\alpha \in G_2$. If $\delta = 0$, then there exists $\beta \in G$ such that β has positive values for all coordinates of G_0 and the coordinates of G_2 have the same values as α. If $\delta = 1$, then there exists a $\beta \in G$ such that β induces α, the 2–coordinate of G_0^* equals the 2–coordinate of G_2 and all other coordinates have positive values. Since β belongs to K_f, the inducement map to G_2 is still surjective when restricted to K_f.

Since $s = t_2$, $|K_f| = 2^{s-\lambda} = 2^{s-1} \cdot 2^{1-\lambda} = |G_2| \cdot 2^{1-\lambda}$. Thus the inducement map restricted to K_f has kernel of order $2^{1-\lambda}$. It follows that $|B_2' \cap K_f| = 2^{1+R_2-\lambda}$. Since the principal element of G is included in $B_2' \cap K_f$, we may improve the estimate by $2^{1+R_2-\lambda} - 1$.

Corollary 8. *If $t_2 = s$, $t_0+\lambda = 3$ and $R_1 = 2$, then f is good when $g \geq -2^{s-\delta}\left(2^{1-\lambda+R_2}\right)$.*

Proof: Since $s = t_2$, an element of G_1 is induced by at most one element of G and either half or all the elements of G_1 are induced by elements of G. Thus either 2 or 4 elements of G induce elements of B_1. If 2 elements of B_1 are not induced, then we may improve the estimate of b by 2. If 4 elements of B_1 are induced, then as in Corollary 5, at least 2 of these are in K_f.

From the proof of Corollary 7, we see that every element of G_2 is induced by $2^{1-\lambda}$ elements of K_f. Thus $2^{1-\lambda+R_2}$ elements of K_f induce elements of B_2. Since the principal element was included in both improved estimates, b may be reduced by only $\left(2^{1-\lambda+R_2}\right)$.

Corollary 9. *If $t_1 = t_2 = 3$, $t_0 = 4$, $s-\lambda = 1$, $R_0 = R_1 = 1$ and $R_2 = 0$, then f is good.*

Proof: Here $t_1 + t_2 = t_0 + 2s - \delta$ implies $\delta = 0, s = 1, \lambda = 0, |G| = 8, |K_f| = 2$ and $|G_1| = |G_2| = |G_0'| = 4$. Hence each element of G_1 (respectively G_2) is induced by exactly 2 elements of G. If $B = B_1' \cup B_2'$, then $|B| \leq 4 + 2 - 1 = 5$ where the -1 is necessary because the principal element of G induces a bad element in both G_1 and G_2. If either $|B| < 5$ or $|B \cap K_f| > 1$, then there are at least $|G| - |B| - 2|K_f| + |B \cap K_f| \geq 1$ good elements of G mapped to good elements of G_0 and f is good. Thus we may assume $|B| = 5$ and $|B \cap K_f| = 1$. Now $|G| - |B| - |K_f| + |B \cap K_f| = 2$, so there are exactly two good elements α_1 and α_2 of $G - K_f$. If $f(\alpha_1) \neq f(\alpha_2)$, then either $f(\alpha_1)$ or $f(\alpha_2)$ is good. Thus we may assume $f(\alpha_1) = f(\alpha_2)$ or equivalently $\alpha_1\alpha_2 \in K_f$. Since $\alpha_1 \neq \alpha_2$ and $|B \cap K_f| = 1$, $\alpha_1 \cdot \alpha_2 \notin B$. Let C be the subgroup of G generated by α_1 and α_2. Then $|C| = 4$. Also B_1' is a subgroup of G of order 4. Since G is an elementary 2–group of order 8, $|B_1' \cap C| = 2$ or 4, contradicting the assumption that α_1, α_2 and $\alpha_1\alpha_2$ are good. Thus $f(\alpha_1) \neq f(\alpha_2)$.

Corollary 10. *If $R_0 = R_1 = 1, s = \lambda = 1, \delta = 0, t_0 \geq 3, t_1 \geq 3$ and $t_2 = 2$, then f is good.*

Proof: Since $R_0 = 1$ and $s - \delta = 1, 2$ is ramified in k_1 and k_2 and $m = nn'$. Thus $\left(\frac{-1}{x}\right)$ is the common character of k_1 and k_2. Since $R_1 = 1$, G_1 contains a nonprincipal bad element which is determined by m_1 or m_2. Since $\lambda = 1, m_1 \equiv m_2 \equiv 1 \pmod 4$, so $\left(\frac{-1}{m_1}\right) = \left(\frac{-1}{m_2}\right) = +1$ and all elements of B_1' have positive value for this character. Since $t_2 = 2$, all elements of B_2' also have positive value for this common character. Thus $|G| - |B_1' \cup B_2'| \geq 2$. However, G_0 has only one nonprincipal bad element and $|K_f| = 1$, so f is good.

Theorem 7. *If $R_0 = 0$, $t_0 \geq 3 - \lambda$ and $t_i \geq R_i + 2$ for $i = 1$ and 2, then f is good except possibly for the values listed below:*

	R_1	R_2	t_0	t_1	t_2	s	δ	λ
a)	2	1	2	4	3	3	1	1
b)	2	0	3	5	2	2	0	0
c)	2	0	3	4	2	2	1	0
d)	2	0	2	4	2	2	0	1
e)	1	1	2	3	3	2	0	1
f)	1	1	3	3	3	2	1	0
g)	1	0	2	4	2	2	0	1
h)	1	0	2	3	2	2	1	1
i)	1	0	3	3	2	1	0	0

Proof: Let $x = 2^{t_1 - 1}$ and $y = 2^{t_2 - 1}$ then

$$g = g(x,y) = \begin{cases} xy - 2^{R_2}x - 2^{R_1}y + 2^{s-\delta} - 2^{2s-(\delta+\lambda)} & \text{if } t_1 \neq s \neq t_2 \text{ or } \delta = 1, \\ xy - x - 2^{R_1+1}y + 2y - 2^{2-\lambda}y^2 & \text{if } t_2 = s, \delta = 0. \end{cases}$$

Here the values of x, y, and $2^{s-\delta}$ are related by $t_1 + t_2 = t_0 + 2s - \delta$.

If $R_1 = 2$, then it follows from Theorem 4 that either $s = t_2$ or $\delta = 0$ and $s = t_2 - 1$. The latter can occur only if $(\Delta_0, \Delta_2) = 4$. If, in addition, $R_2 = 1$, then it follows from Corollary 1 to Theorem 4 that $s = t_2, \delta = 1$ and $m_1 = 2$. In this case $g = xy - 2x - 3y - 2^{1-\lambda}y^2$ and $t_1 = t_2 + t_0 - 1$. Thus $t_1 \geq t_2 + 2 - \lambda$ and $x \geq 2^{2-\lambda}y$. Since

g is an increasing function of x on our domain, $g \geq 2^{2-\lambda}y^2 - 2^{3-\lambda}y - 3y - 2^{1-\lambda}y^2 = y(2^{1-\lambda}y - 2^{3-\lambda} - 3)$. If $\lambda = 0$, $x \geq 4y \geq 16$. Thus $g \geq 0$ except when $x = 16$ and $y = 4$. However, f is good at this point by Corollary 7 to Theorem 6. When $\lambda = 1, x \geq 2y \geq 8$. Thus $\lambda = 1, x = 8$ and $y = 4$ is the only case where f may be bad, yielding line (a) of the chart.

Next, suppose $R_1 = 2$ and $R_2 = 0$. If $s - \delta = t_2$, then $\delta = 0$ and $x \geq 2^{3-\lambda}y$. Thus

$$g = xy - x - 8y + 2y - 2^{2-\lambda}y^2 \geq 2^{3-\lambda}y^2 - \left(2^{3-\lambda} + 6\right)y - 2^{2-\lambda}y^2 \geq 0$$

when $y \geq 4 + \lambda$. However, when $\lambda = 1, x = 16$ and $y = 2$ or 4, then $g = -4$ or -8 and f is good by Corollaries 4 and 8 to Theorem 6, respectively. Also, $g \geq 0$ when $x > 16$. Thus $y = 2$ and $x = 2^{4-\lambda}$ are the only cases where f may be bad, yielding lines b) and d) of the chart.

If $s - \delta = t_2 - 1$, then $g = xy - x - 3y - 2^{\delta-\lambda}y^2$. Hence $x \geq 2^{1+\delta-\lambda}y$ and $g \geq 0$ except when $\delta - \lambda = 1, x = 8, y = 2$ or $\delta - \lambda = 0, x = 8, y = 2$ or 4. However, when $\delta = \lambda$ Corollaries 2 and 5 to Theorem 6 show f is good. When $\delta = 1, \lambda = 0, x = 8$, and $y = 2$, line (c) is obtained.

Since $R_1 = 2$, $n'|\Delta_1$. Thus $s - \delta \geq t_2 - 1$.

Next, consider the case $R_1 = R_2 = 1$. By Theorem 4 and its first two Corollaries, $s - \delta \neq t_2$. Thus if $s = t_2$, then $\delta = 1$, and $t_1 = t_0 - \delta + t_2 \geq 2 - \lambda + t_2$. If $\lambda = 0$, then $x \geq 4y$, and $g \geq y(2y - 9) \geq 0$ except when $x = 16, y = 4$. Here $g = -4$ and f is good by Corollary 3 to Theorem 6. When $\lambda = 1, x \geq 2y$, so $g \geq 0$ except when $x = 8, y = 4$. By Corollary 7 to Theorem 6, f is good in these circumstances.

If $s = t_2 - 1$, then $t_1 \geq 1 - (\delta + \lambda) + t_2$. Thus when $\lambda = \delta = 0$, $g = xy - 2x - y - y^2$, $x \geq 2y$ and $g \geq 0$ except when $x = 8, y = 4$. Here $g = -4$ and f is good by Corollary 3 to Theorem 6. If $\delta + \lambda = 1$, then $x \geq y$ so $g \geq y\left(1/2y - 4 + 2^{-\delta}\right) \geq 0$ when $y \geq 8$. If $y = 4$, then $g = 2x - 16 + 2^{2-\delta} \geq 0$ for $x \geq 8$. Hence $t_1 = t_2 = 3$, $t_0 = 3 - \lambda$ and

$\delta + \lambda = 1$, yields lines e) and f) of the chart. Let $\delta + \lambda = 2$ and by renumbering k_1 and k_2 if necessary, assume $x \geq y$. Thus $g \geq 0$ except when $x = y = 4$. Here $g = -2$ and f is good by Corollary 2 to Theorem 6.

Let $s = t_2 - 2$ and $t_1 \geq t_2$. If $\delta + \lambda = 0$ then $g \geq 0$ except when $x = y = 4$. Here again $g = -2$ and Corollary 2 to Theorem 6 tells us that f is good. If $\delta + \lambda \geq 1$, then

$$g \geq xy - 2x - 2y + 1/4y - 1/8y^2 \geq 7/8y^2 - 15/4y \geq 0$$

when $y > 4$. If $x = y = 4$, $\delta = 1$ and $\lambda = 0$, then $g = -1$, but $s - \delta = 0$ and Corollary 1 to Theorem 6 shows that f is good. If $\lambda = 1$, then $g \geq 0$ on our domain. Since g is a decreasing function of s, $g \geq 0$ for $x, y \geq 4$ and $s < t_2 - 2$.

Finally, let $R_1 = 1, R_2 = 0$. Here the numbering of k_1 and k_2 is fixed, so we must consider the cases $t_1 \geq t_2$ and $t_1 < t_2$ separately. First let $t_1 \geq t_2$ and $s = t_2$. As above, $t_1 \geq t_2 + 3 - (\delta + \lambda)$. If $\delta + \lambda = 0$, then $x \geq 8y$ so $g = xy - x - 4y + 2y - 4y^2 \geq 2y(2y - 5) \geq 0$ except when $y = 2$ and $x = 16$. In this case $g = -4$ and f is good by Corollary 7 to Theorem 6. If $\delta = 1$ and $\lambda = 0$, then $g \geq 0$ except when $x = 8, y = 2$. Here f is good by Corollary 7 to Theorem 6. If $\lambda = 1$, then $g \geq 0$ except when $\delta = 0$, $x = 8$ and $y = 2$ or $\delta = 1, x = 4$ and $y = 2$. This yields lines g) and h) of the chart.

When $s = t_2 - 1, x \geq 2^{1-(\delta+\lambda)}y$ and $g = xy - x - 2y + 2^{-\delta}y - 2^{-(\delta+\lambda)}y^2$. If $x \geq 2y$, then $g \geq 0$ unless $x = 4$ and $y = 2$. If $\delta + \lambda = 0$ this yields line (i) of the chart. When $\delta = 1$ and $\lambda = 0$, then $s - \delta = 0$ and $g = -1$ so Corollary 1 to Theorem 6 shows f is good. If $\lambda = 1$, then $g \geq 0$ on our domain. Suppose now $x = y$, so $\delta + \lambda > 0$. Thus $g \geq 0$ except when $\lambda = 0, \delta = 1$ and $x = y = 4$. Here $g = -2$. Since $|G_1| = |K_f|$, Corollary 3 to Theorem 6 shows that f is good.

If $s \leq t_2 - 2$ and $x \geq y$, then $g \geq xy - x - 2y + 2^{-1-\delta}y - 2^{-2-\delta-\lambda}y^2 \geq 0$ for $x \geq 4$ and $y \geq 2$.

Assume now $t_2 > t_1 \geq 3$. Then $y \geq 2x$ and $g \geq 2x^2 - 5x + 2^{s-\delta} - 2^{2s-(\delta+\lambda)}$. Hence $g \geq 0$ for $s \leq t_1 - 1$. Thus we may assume $s = t_1$. Since $R_1 = 1$, 2 is totally ramified in K, so $\delta = 1$. Hence $t_2 = t_0 + 2s - \delta - t_1 \geq t_1 + 2 - \lambda$, so $y \geq 2^{2-\lambda}x$. Therefore,

$$g \geq 2^{2-\lambda}x^2 - x - 2^{3-\lambda}x + x - 2^{(1-\lambda)}x^2 = x\left(2^{1-\lambda}x - 2^{3-\lambda}\right) \geq 0$$

for $x \geq 4$.

If $R_1 = R_2 = 0$, then $g \geq 0$ on our domain.

Corollary 1. *Lines a), b), c), d), f) and g) of Theorem 7 are always good. (The proof for lines a), c) and d) assumes the list of imaginary quadratic fields with one class per genus is complete.)*

Proof: In line (a) $R_1 = 2$ and $R_2 = 1$, thus by Theorem 4 and Corollary 1 to it, m and n' must divide Δ_1 and 2 is a principal factor in k_0. Since $\lambda = \delta = 1$, $t_0 = 2$ and $t_1 = 4, m = 2p_1$ with $p_1 \equiv 1 \pmod 4$, and $n = -2^c p_1 p_2 p_3$ with $p_1 p_2 p_3 \equiv 1 \pmod 4$ and $c = 0$ or 1. Here $R_1 = r_1$ and $R_2 = r_2$ so each of k_1 and k_2 must have at most one bad class in a given genus. Thus if either k_1 or k_2 has more than one class per genus, then there exists a good class in the principal genus of that field. Since K/k_1 is ramified, Corollary 1 to Theorem 5 shows that K contains sci primes. Thus we may assume that both k_1 and k_2 have only one class per genus. From the list of such fields the only possible example is $m = 2 \cdot 17, n = -3 \cdot 7 \cdot 17$ and $n' = -2 \cdot 3 \cdot 7$. Since $\left(\frac{2}{17}\right) = \left(\frac{-1}{17}\right) = +1$ and $\left(\frac{17}{3}\right) = \left(\frac{17}{7}\right) = -1$, it follows that the elements of G corresponding to 2, 17 and 34 are distinct elements of the kernel of f. Since $|G| = 8$ and $|K_f| = 4$, there are three elements of $G - K_f$ which induce nonprincipal elements in G_2. Since only one of these is bad, K must contain sci primes.

In line (b), $t_0 = 3, t_1 = 5, t_2 = s = 2$ and $\lambda = \delta = 0$. Thus there are five distinct primes with $p_1p_2p_3|\Delta_0, p_1p_2p_3p_4p_5|\Delta_1$ and $p_4p_5|\Delta_2$. In order to have $\lambda = \delta = 0$ the following congruences must hold: $p_1 \equiv p_2 \equiv p_5 \equiv 3 \pmod 4), p_3 \equiv p_4 \equiv 1 \pmod 4$ or any p_i may be 2. Here $G \approx G_0 \times G_2 \subseteq G_1$ as shown in the chart below:

	G_0			G_2		G'_0	
	p_1	p_2	p_3	p_4	p_5	p_1p_2	p_3
1	+	+	+	+	+	+	+
2	−	−	+	+	+	+	+
3	+	+	+	−	−	+	+
4	−	−	+	−	−	+	+
5	+	−	−	+	+	−	−
6	−	+	−	+	+	−	−
7	+	−	−	−	−	−	−
8	−	+	−	−	−	−	−

Thus only lines 7 and 8 of $G - K_f$ are possibly good. Hence, if K has no sci primes, then lines 7 and 8 of G must correspond to classes of k_1 which become principal in K. Since the elements which become principal in K form a group, line 2 must contain the third nonprincipal class that becomes principal. Thus we assume that these three lines must be the character system in k_1 for the principal factors m_1, m_2 and m_1m_2.

Since no nonprincipal classes of k_0 or k_2 can become principal in K, Theorem 5 applies to show K has sci primes whenever any quadratic subfield has more than one class per genus. Thus we may assume that all three quadratic subfields have one class per genus. Since p_1 and p_2 are symmetric, we may number these primes so that p_2 is not a principal factor of k_0. Thus, $\left(\frac{p_4}{p_5}\right) = \left(\frac{p_2}{p_3}\right) = -1$.

First, assume that $m_1 = p_3$ and $m_2 = p_1p_2$. Then $\left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = -1$ and since $p_3 \not\equiv 3 \pmod 4$ $\left(\frac{p_3}{p_1}\right) = \left(\frac{p_3}{p_2}\right) = -1$. Hence neither m_1 nor m_2 can be on lines 7 or 8, so K must contain sci primes in this case.

Next, assume that $m_1 = p_1$ and $m_2 = p_2p_3$, so $\left(\frac{p_1}{p_3}\right) = +1$. Thus we may assume that p_1 is on line 2. Let us assume for the moment that all p_i are odd. Thus $p_1 \equiv p_5 \equiv 3 \pmod 4$ so $\left(\frac{p_4p_5}{p_1}\right) = -\left(\frac{p_1}{p_4}\right)\left(\frac{p_1}{p_5}\right) = -1$. Since m_1m_2 and p_4p_5 are on the same line, they must be on line 8, so $m_2 = p_2p_3$ is on line 7. Thus $\left(\frac{p_4p_5}{p_3}\right) = \left(\frac{p_2p_3}{p_4}\right) =$

$\left(\frac{p_2p_3}{p_5}\right) = \left(\frac{p_2}{p_4p_5}\right) = -1$, which implies that $\left(\frac{p_5}{p_3}\right) = \left(\frac{p_2}{p_4}\right) \neq \left(\frac{p_3}{p_4}\right) = \left(\frac{p_2}{p_5}\right)$. If $\left(\frac{p_2}{p_5}\right) = +1$ then p_3 and p_4 are in the same genus of k_1 so p_3p_4 is in the principal genus. If $\left(\frac{p_2}{p_5}\right) = -1$, then p_2 and p_4 are in the same genus so p_2p_4 is in the principal genus. This contradicts k_1 having only one class per genus.

Now assume $p_5 = 2$. If n is even, then the character at p_5 is $\left(\frac{-2}{x}\right) = (-1)^{\frac{x-1}{2}}\left(\frac{2}{x}\right)$, so the above computations are still valid, and either p_3p_4 or p_2p_4 will be in the principal genus of k_1. Similar results are obtained with $p_i = 2$ for $i = 1, 2, 3$ or 4 and n even. Assume now n is odd. If $p_5 = 2$, then the character at p_5 is $(-1/x)$. Since $m_1 = p_1$, $\left(\frac{p_1}{p_3}\right) = +1$ but $\left(\frac{-1}{p_1}\right) = -1$, so p_1 is not on any of lines 2, 7 or 8. Similarly, if $p_2 = 2$, then $(-1/x)$ is the character at p_2. Also $m = p_1p_3$, so $m_2 = p_3$. But $\left(\frac{p_3}{p_1}\right) = +1$ while $\left(\frac{-1}{p_3}\right) = +1$, so p_3 is not on line 2, 7 or 8. If $p_1 = 2$, then $(-1/x)$ is the character at p_1. Since $\left(\frac{p_1}{p_3}\right) = +1$, we may assume that p_1 belongs on lines 2. Since $p_2p_3 \equiv p_4p_5 \equiv 3 \pmod 4$, we may assume both p_2p_3 and p_4p_5 belong on line 8. Thus $\left(\frac{p_4}{p_2}\right) = \left(\frac{p_5}{p_2}\right)$, $\left(\frac{p_4}{p_3}\right) = -\left(\frac{p_5}{p_3}\right)$ and $\left(\frac{p_2}{p_4}\right) = -\left(\frac{p_3}{p_4}\right)$. It follows that $\left(\frac{p_5}{p_2}\right) = \left(\frac{p_4}{p_2}\right) = -\left(\frac{p_3}{p_4}\right) = \left(\frac{p_3}{p_5}\right)$. Also, $\left(\frac{p_2}{p_3}\right) = \left(\frac{p_4}{p_5}\right) = -1$. If $\left(\frac{p_4}{p_2}\right) = +1$ then we have the following character values:

	$\left(\frac{-1}{x}\right)$	$\left(\frac{x}{p_2}\right)$	$\left(\frac{x}{p_3}\right)$	$\left(\frac{x}{p_4}\right)$	$\left(\frac{x}{p_5}\right)$
p_2	$-$	$-$	$-$	$+$	$-$
p_4	$+$	$+$	$-$	$+$	$-$

Thus p_2p_4 is on line 2, so $2p_2p_4$ is on line 1, contradicting that there is only one class per genus in k_1. Similarly, if $\left(\frac{p_4}{p_2}\right) = -1$ we have the following character values:

	$\left(\frac{-1}{x}\right)$	$\left(\frac{x}{p_2}\right)$	$\left(\frac{x}{p_3}\right)$	$\left(\frac{x}{p_4}\right)$	$\left(\frac{x}{p_5}\right)$
p_3	$+$	$-$	$+$	$+$	$-$
p_4	$+$	$-$	$+$	$+$	$-$

so p_3p_4 is on line 1, contradicting that there is only one class per genus in k_1.

Suppose now $m_1 = 2p_2$ and $m_2 = 2p_3$. Here both m and n must be odd and $p_1 = 2$. Since $\left(\frac{2p_2}{p_3}\right) = +1$, $2p_2$ can not be on line 7 or 8. Also, $\left(\frac{-1}{p_2p_3}\right) = \left(\frac{-1}{p_4p_5}\right) = -1$. Thus if K contains no sci primes, $2p_2$ is on line 2 and p_2p_3 and p_4p_5 are on line 8. It follows that the character systems for p_2, p_3, p_4 and p_5 will be as above.

In line (c) there are three distinct odd primes p_1, p_2 and p_3 with $2p_1p_2|\Delta_0$, $2p_1p_2p_3|\Delta_1$ and $2p_3|\Delta_2$ where $p_2 \equiv 3 \pmod 4$. We have the following character tables:

G_1				G_2		$G_0,\ p_1 \equiv 1 \pmod 4$		$G_0,\ p_1 \equiv 3 \pmod 4$	
2	p_1	p_2	p_3	2	p_3	$2p_2$	p_1	p_1p_2	2
+	+	+	+	+	+	+	+	+	+
−	+	−	+	+	+	+	+	−	−
+	+	−	−	−	−	+	+	−	−
−	+	+	−	−	−	+	+	+	+
+	−	−	+	+	+	−	−	+	+
−	−	+	+	+	+	−	−	−	−
+	−	+	−	−	−	−	−	−	−
−	−	−	−	−	−	−	−	+	+

If $p_1 \equiv 1 \pmod 4$, then K will contain no sci primes only if lines 2, 7 and 8 of G_1 are bad and k_0 and k_1 have only one class per genus. If 2 is not a principal factor of k_0, then $\left(\frac{2}{p_1}\right) = -1$. Here we assume k_2 has one class per genus, hence $\left(\frac{2}{p_3}\right) = -1$. Thus, 2 is on line 7 or 8 and f is good. If 2 is a principal factor of k_0, then $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_3}\right) = +1$ and 2 is on line 2. However, $k_1 = Q(\sqrt{-357})$ is the only known imaginary quadratic field where this occurs. Here $p_1 = 17$, $p_2 = 3$ and $p_3 = 7$ so $\left(\frac{-1}{p_3}\right) = -1$, $\left(\frac{p_3}{p_2}\right) = +1$. Thus p_3 is not on line 7 or 8 and f is good.

If $p_1 \equiv 3 \pmod 4$, then f is good only if line 3 or 7 is good in G. If 2 is not a principal factor of k_0, then $\left(\frac{2}{p_1p_2}\right) = -1$ so $\left(\frac{2}{p_1}\right) \neq \left(\frac{2}{p_2}\right)$. Since k_2 has one class per genus, $\left(\frac{2}{p_3}\right) = -1$. Thus 2 is on line 3 or 7 and f is good. If 2 is a principal factor of k_0, then since p_1 and p_2 are not principal factors of k_0, $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = -1$.

Also $\left(\frac{2}{p_3}\right) = +1$, so 2 is on line 5. However, there is no known imaginary quadratic field with one class per genus meeting these conditions.

In line (d) there are four distinct primes such that $p_1p_2|\Delta_0, p_1p_2p_3p_4|\Delta_1$ and $p_3p_4|\Delta_2$. Since $\lambda = 1, p_1 \not\equiv 3 \not\equiv p_2 \pmod 4$. Also $R_1 = 2$ implies $N(\epsilon) = +1$, $m_1 = p_1$ and $m_2 = p_2$. The following chart shows the genus structure:

G_0		G_2	
p_1	p_2	p_3	p_4
$+$	$+$	$+$	$+$
$+$	$+$	$-$	$-$
$-$	$-$	$+$	$+$
$-$	$-$	$-$	$-$

If the last line is good, then K will contain sci primes. Since $m_1 = p_1$, $\left(\frac{p_1}{p_2}\right) = +1$. This implies that neither p_1 nor p_2 is on line 4. However, the product p_1p_2 will be on line 4 exactly when $\left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_4}\right) \neq \left(\frac{p_1}{p_4}\right) = \left(\frac{p_2}{p_3}\right)$. Note that either line 3 or 4 of G_1 is good, so Theorem 5 applies to show sci primes exist whenever any quadratic subfield has more than one class per genus. Since $p_3 \equiv p_4 \equiv 3 \pmod 4$ is not possible, assuming the list of imaginary quadratic fields with one class per genus is complete, no such fields exist.

In line (f) there exist three odd primes such that $2p_1p_2|\Delta_0$, $2p_1p_3|\Delta_1$ and $2p_2p_3|\Delta_2$ where $p_2 \equiv 3 \pmod 4$. Since $r_1 \neq 2$, if any quadratic subfield has more than one class per genus, then Theorem 5 applies. We consider the cases $p_1 \equiv 1 \pmod 4$ and $p_1 \equiv 3 \pmod 4$ separately.

G_1			G_2			G_0' case I		G_0' case II	
2	p_1	p_3	2	p_2	p_3	$2 \cdot p_2$	p_1	$p_1 \cdot p_2$	2
+	+	+	+	+	+	+	+	+	+
+	+	+	−	−	+	+	+	−	−
−	+	−	−	+	−	+	+	+	+
−	+	−	+	−	−	+	+	−	−
−	−	+	+	+	+	−	−	−	−
−	−	+	−	−	+	−	−	+	+
+	−	−	−	+	−	−	−	−	−
+	−	−	+	−	−	−	−	+	+

Case I: $p_1 \equiv 1 \pmod 4$. Here $m = p_1p_2$ or $2p_1p_2$. In order for f to be bad, lines 7 and 8 must be bad in G_1 and line 6 bad in G_2. If $m_1 = 2$, then $(\frac{2}{p_1}) = +1$, so 2 is not on lines 7 and 8 in G_1. If 2 is not a principal factor of k_0, then $(\frac{2}{p_1}) = -1$. If $(\frac{2}{p_3}) = -1$, then 2 is on lines 7 and 8 in G_1, making them good. Otherwise, $(\frac{2}{p_3}) = +1$ implies 2 is on line 6 in G_2, making it good.

Case II: $p_1 \equiv 3 \pmod 4$. Here $m = 2p_1p_2$, $p_3 \equiv 3 \pmod 4$ and the character of 2 in k_0 is $(\frac{2}{x})$. Without loss of generality, $n = -p_1p_3$ and $n' = -2p_2p_3$. Here f will be bad if and only if lines 4 and 7 of G are bad. Suppose $m_1 = 2$ and $m_2 = p_1p_2$, then the primes above p_1 and p_2 are not in the principal genus of k_0, so $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$. If K contains no sci primes, then 2 must be on lines 7 and 8 in G_1, yielding $(\frac{2}{p_3}) = -1$. Since $(\frac{-2}{p_3}) = -(\frac{2}{p_3}) = +1$, p_3 is either on line 1 or 4 of G_2. Thus k_2 has more than one class per genus.

If $m_1 \neq 2$, then $(\frac{2}{p_1}) \neq (\frac{2}{p_2})$. Suppose $(\frac{2}{p_1}) = +1$, then since 2 is not the norm of a principal ideal of k_1, $(\frac{2}{p_3}) = -1$. Thus 2 is on line 4 of G_1, making that line good. Similarly, if $(\frac{2}{p_1}) = -1$ and $(\frac{2}{p_2}) = +1$, then from G_2, $(\frac{2}{p_3}) = -1$. Thus 2 is on line 7 of G, making it good.

In line (g) there exist four primes with $p_1p_2 \mid \Delta_0$, $p_1p_2p_3p_4 \mid \Delta_1$ and $p_3p_4 \mid \Delta_2$. Since $\lambda = 1$, $m = p_1p_2$ with $p_1 \not\equiv 3$, $p_2 \not\equiv 3 \pmod 4$. Moreover, $p_3 \not\equiv p_4 \pmod 4$. The structure of $G \approx G_0 \times G_2$ is given below:

G_0		G_2	
p_1	p_2	p_3	p_4
$+$	$+$	$+$	$+$
$+$	$+$	$-$	$-$
$-$	$-$	$+$	$+$
$-$	$-$	$-$	$-$

Here f is good if line 4 of G is good. If $N(\epsilon) = +1$, then $m_1 = p_1$ and $m_2 = p_2$ with $(\frac{p_1}{p_2}) = +1$. Since $r_1 = 2$ and $R_1 = 1$, k_1 has a nonprincipal bad class in the principal genus. Hence m, m_1 or m_2 is on line 1 of G. Since neither m_1 nor m_2 can be on line 4, it is good.

Assume now that $N(\epsilon) = -1$, so $R_1 = r_1 = 1$. Whenever any quadratic subfield has more than one class per genus, Theorem 5 applies to show that K contains sci primes. Thus we may assume $(\frac{p_1}{p_2}) = (\frac{p_3}{p_4}) = -1$. If $n' = -p_3p_4$ is one line 4, then $(\frac{p_3}{p_2}) = (\frac{p_1}{p_4}) \neq (\frac{p_2}{p_4}) = (\frac{p_3}{p_1})$. If $(\frac{p_3}{p_1}) = +1$, then the primes above p_1 and p_3 are in distinct classes of k_1 but are in the same genus. If $(\frac{p_3}{p_1}) = -1$, then p_2 and p_3 have the same character system in k_1, contrary to one class per genus. If $n' = -p_4$ and $p_3 = 2$, then the character at p_3 is $(\frac{-1}{x})$. Since $(\frac{-1}{p_4}) = +1$, line 4 is good and K contains sci primes.

THEOREM 8. *If $t_i \geq R_i + 2$ for $i = 1, 2$ and $t_0 \geq 4 - \lambda$ with $R_0 = 1$, then f is good except possibly for the values listed below:*

	R_1	R_2	t_0	t_1	t_2	s	δ	λ
(a)	1	0	4	3	2	1	1	0
(b)	0	0	4	2	2	0	0	0
(c)	0	0	3	2	2	1	1	1
(d)	0	0	4	3	2	1	1	0

PROOF: Since $R_0 = 1$, Theorem 3 shows that $n \mid \Delta_0$. Thus $\delta \leq s \leq 1$ and $s - \delta = 1$ if and only if 2 is ramified in k_1 and k_2 but n and n' are odd. If $\lambda = 1$, then every prime dividing Δ_0 is congruent to 1 or 2 $\pmod 4$ so $n \not\equiv 1 \pmod 4$, $n' \not\equiv 1 \pmod 4$, and 2 is ramified in k_1 and k_2. Thus $\lambda = 1$ implies $s = 1$.

Suppose $s = 1$ and $\delta = 0$. Here $R_1 = R_2 = 1$ is impossible by Corollary 3 to Theorem 4; hence, we may assume $R_2 = 0$. Each element of G_1 is induced by 2^{t_2-2} elements of G. Hence, G has at least

$$|G| - |B_1'| - |B_2'| + |B_1' \cap B_2'| \geq 2^{t_1+t_2-3} - 2^{R_1+t_2-2} - 2^{t_1-2} + 1 = g_1$$

good elements. If g_1 is at least $2|K_f| = 2^{2-\lambda}$, then f is good. By hypothesis, $t_1 + t_2 = t_0 + 2s - \delta \geq 6 - \lambda$, $t_1 \geq R_1 + 2$ and $t_2 \geq 2$. By direct computation it is seen that $g_1 \geq 2^{2-\lambda}$ when $t_1 + t_2 = 6 + R_1 - \lambda$. Since g_1 is an increasing function of $t_1 + t_2$, we need only consider the case $t_1 + t_2 = 6 - \lambda$ and $R_1 = 1$. If $\lambda = 0$, then Corollary 9 to Theorem 6 applies when $t_1 = t_2 = 3$ and Corollary 4 to Theorem 6 applies when $t_1 = 4$, $t_2 = 2$ to show f is good. If $\lambda = 1$, then $t_0 = t_1 = 3$, $t_2 = 2$ and Corollary 10 to Theorem 6 applies to show f is good.

Assume now that $s - \delta = 0$, so $G = G_1 \times G_2$. Here there are exactly $g_2 = (2^{t_1-1} - 2^{R_1})(2^{t_2-1} - 2^{R_2})$ good elements of G. Since at most $2^{1+s-\lambda} - 1$ good elements of G can map to bad elements of G_0', f will be good whenever $g_2 \geq 2^{1+s-\lambda}$. By hypothesis, $t_1 + t_2 = t_0 + 2s - \delta \geq 4 - \lambda + s$ and $t_i \geq R_i + 2$ for $i = 1, 2$. By direct computation, $g_2 \geq 2^{1+s-\lambda}$ whenever $t_1 + t_2 = 5 - \lambda + s$. Since g_2 is an increasing function of $t_1 + t_2$, we need only consider the cases where $t_1 + t_2 = 4 - \lambda + s$. Since $4 - \lambda + s = 3$, 4 or 5 and $t_1 + t_2 \geq 4 + R_1 + R_2$, equality can only occur when $R_1 = 1$, $R_2 = 0$ and $t_1 + t_2 = 5$, or $R_1 = R_2 = 0$ and $t_1 + t_2 = 4$ or 5. These values where equality holds are exactly those listed in the statement of the Theorem.

Corollary 1. *Line (d) of Theorem 8 is always good.*

Proof: Here $s = \delta = 1$, $\lambda = 0$ and three odd primes divide the discriminant of K. Let $2p_1p_2 \mid \Delta_1$ and $2p_3 \mid \Delta_2$. The structure of G is given below:

G_1			G_2	
2	p_1	p_2	2	p_3
+	+	+	+	+
+	−	−	+	+
−	+	−	+	+
−	−	+	+	+
+	+	+	−	−
+	−	−	−	−
−	+	−	−	−
−	−	+	−	−

Since $R_1 = R_2 = 0$, the last three lines of G are good. Hence f is good if it maps one of these lines to a good element of G'_0. Thus it is sufficient to show that f maps two of these lines to distinct nonprincipal elements of G'_0. Since $\lambda = 0$, $p_i \equiv 3 \pmod 4$ for some $i = 1, 2$ or 3. Also $|K_f| = 2^{s-\lambda} = 2$. If $p_3 \equiv 1 \pmod 4$, or $p_1 \equiv p_2 \equiv 1 \pmod 4$, then no good element of G is in K_f, thus f is good. If $p_3 \equiv 3 \pmod 4$, then $n' = -2p_3$ and either $n \equiv 3$ or $m \equiv 3 \pmod 4$. Either way, $p_1 \equiv p_2 \pmod 4$. Thus the only remaining case to consider is $p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod 4$. There line 6 corresponds to an element of K_f, but lines 7 and 8 give distinct elements of G'_0. Thus f is good.

THEOREM 9. *Assume that K/k_1 is ramified and that $h_i > 2^{r_i}$ for $i = 0, 1, 2$. Then K contains sci primes unless all classes in the principal genus of each k_i ($i = 0, 1, 2$) are principal in K and one of the following conditions holds:*

7,e,1. $m = p_1p_4$, $n = -p_1p_2p_3$, $n' = -p_2p_3p_4$ *with* $p_1 \not\equiv 3$, $p_4 \equiv 1$, $p_2 \not\equiv p_3 \pmod 4$, $(\frac{p_1}{p_4}) = +1$, $(\frac{p_2}{p_3}) = -1$, $(\frac{p_1}{p_2}) = (\frac{p_3}{p_4}) \neq (\frac{p_2}{p_4}) = (\frac{p_1}{p_3})$, *and* $r_1 = r_2 = 1$.

7,h,1. $m = 2p_2$, $n = -2^c p_1p_2$, $n' = -2^{1-c}p_1$, *with* $p_1 \equiv p_2 \equiv 1 \pmod 4$, $(\frac{2}{p_1}) = (\frac{2}{p_2}) = +1$, $(\frac{p_1}{p_2}) = -1$, $N(\epsilon) = +1$, $r_1 = 2$, *and* $r_2 = 1$.

7,i,1. $m = p_1p_2p_4$, $n = -p_1p_2p_3$, $n' = -p_3p_4$ *with* $p_1 \not\equiv 1 \not\equiv p_4$, $p_2 \not\equiv 3$, $p_3 \not\equiv p_4 \pmod 4$, $(\frac{p_4}{p_2}) = (\frac{p_1}{p_3}) = (\frac{p_4}{p_3}) = +1$, $(\frac{p_1}{p_2}) = (\frac{p_2}{p_3}) = -1$, *and* $r_1 = r_2 = 1$.

7,i,2. $m = p_2p_4$, $n = -p_2p_3$, $n' = -p_3p_4$ *with* $p_2 \equiv p_3 \equiv 1$, $p_4 \equiv 3 \pmod 4$, $(\frac{p_2}{p_4}) =$

$(\frac{p_4}{p_3}) = +1$, $(\frac{p_2}{p_3}) = -1$, *and* $r_1 = r_2 = 1$.

7,i,3. $m = p_1p_2$, $n = -p_1p_2p_3$, $n' = -p_3$ *with* $p_1 \equiv 3$, $p_2 \equiv p_3 \equiv 1 \pmod 4$, $(\frac{p_1}{p_3}) = +1$, $(\frac{p_2}{p_3}) = -1$, $(\frac{2}{p_2}) = (\frac{2}{p_3})$, *either* $(\frac{p_1}{p_2}) = +1$ *and* $(\frac{2}{p_2}) = -1$ *or* $(\frac{p_1}{p_2}) = -1$, *and* $r_1 + r_2 \leq 2$.

8,a,1. $m = 2^c p_1p_2p_3$, $n = -2p_1p_2$, $n' = -2^{1-c}p_3$, *with* $p_1 \equiv 3$, $p_2 \equiv p_3 \equiv 1 \pmod 4$, $(\frac{p_3}{p_1}) = (\frac{2}{p_2}) = (\frac{2}{p_3}) = +1$, $(\frac{2}{p_1}) = (\frac{p_1}{p_2}) = (\frac{p_3}{p_2}) = -1$, *and* $r_0 = r_1 = r_2 = 1$.

8,a,2. $m = 2p_1p_2p_3$, $n = -p_1p_2$, $n' - 2p_3$ *with* $p_1 \equiv p_2 \equiv 3$, $p_3 \equiv 1 \pmod 4$, $(\frac{2}{p_3}) = +1$, $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$, *and* $r_0 = r_1 = r_2 = 1$.

8,a,3. $m = 2^c p_1p_2p_3$, $n = -2^{1-c}p_1p_2$, $n' = -2p_3$ *with* $p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod 4$, $(\frac{2}{p_3}) = +1$, $(\frac{p_3}{p_1}) = (\frac{p_3}{p_2}) = -1$, $(\frac{p_1}{p_2}) = (\frac{2}{p_1}) \neq (\frac{2}{p_2})$, $r_0 = r_1 = r_2 = 1$.

8,b,1. $m = p_1p_2p_3{p_4}^c$, $n = -p_1p_2$, $n' = -p_3{p_4}^c$ *with* $p_1 \equiv 3$, $p_2 \equiv 1$, $p_3 \not\equiv 3$, $p_4 \not\equiv 1 \pmod 4$, $(\frac{p_1}{p_3}) = (\frac{p_4}{p_2}) = +1$, $(\frac{p_3}{p_2}) = -1$, $(\frac{p_1}{p_2}) + (\frac{p_4}{p_3}) < 2$, $r_0 = 1$, *and* $r_1 + r_2 < 2$.

8,c,1. $m = 2p_1p_2$, $n = -2p_1$, $n' = -p_2$, *with* $p_1 \equiv p_2 \equiv 1 \pmod 4$, $(\frac{2}{p_1}) = (\frac{2}{p_2}) = +1$, $(\frac{p_1}{p_2}) = -1$, *and* $r_0 = r_1 = r_2 = 1$.

Here $c = 0$ *or 1 and* $c = 0$ *can only occur as an exponent of the prime 2. Also the number of each condition signifies the line of Theorem 7 or 8 that yielded it. For example, the quadratic fields given on line 8,c,1 have the* R_i, t_i, s, δ *and* λ *values listed on line (c) of Theorem 8.*

Proof: Since K/k_1 is ramified, we may apply Theorem 5 to show that if for some j, k_j has a good class in the principal genus, then K contains sci primes. Thus we may assume that for each k_i, $2^{r_i - R_i}$ is the number of classes per genus. Under this assumption, $h_i > 2^{r_i}$ is equivalent to each k_i containing a good genus, i.e., $t_i \geq 2 + R_i$ for $i = 1$ and 2 and $t_0 \geq 3 - \lambda + R_0$. Thus Theorems 7 and 8 and their Corollaries list all possible cases where K does not contain sci primes.

First, assume that line (e) of Theorem 7 holds. Since $t_0 = 2$ and $\lambda = 1$, $m = p_1p_4$

with $p_1 \not\equiv 3$ and $p_4 \equiv 1 \pmod 4$. Since $t_1 = t_2 = 3$ and $s = 2$, $n = -p_1p_2$ with $p_1 \equiv p_2 \equiv 1 \pmod 4$ or $n = -p_1p_2p_3$ with $p_2 \not\equiv p_3 \pmod 4$. The fields have the genus structure shown below:

G_1			G_2			G_0	
p_1	p_2	p_3	p_2	p_3	p_4	p_1	p_4
+	+	+	+	+	+	+	+
+	−	−	−	−	+	+	+
−	+	−	+	−	−	−	−
−	−	+	−	+	−	−	−

On line (e) we have $R_1 = R_2 = 1$, so we must have $N(\epsilon) = +1$. Hence $m_1 = p_1$, $m_2 = p_4$ and $(\frac{p_1}{p_4}) = +1$. Thus K contains no sci primes if and only if p_1 belongs to line 3 or 4 in G_1 and p_4 belongs to line 4 or 3 in G_2.

If $n = -p_1p_2$, then $p_3 = 2$ and the character at p_3 is $(\frac{-1}{x})$. Since $p_1 \equiv p_4 \equiv 1 \pmod 4$, neither p_1 nor p_4 can be on line 3. In this case, K must contain sci primes. Thus we may assume $n = -p_1p_2p_3$. If $(\frac{p_1}{p_2}) = (\frac{p_3}{p_4}) \neq (\frac{p_2}{p_4}) = (\frac{p_1}{p_3})$, then p_1 is on line 3 or 4 in G_1 and p_4 is on the other in G_2. Since k_1 has one class per genus, p_1, p_2 and p_3 are on distinct nonprincipal lines of G_1. Thus $(\frac{p_2}{p_3}) = -1$. This is consistent with k_2 containing one class per genus.

Next assume that line (h) of Theorem 7 holds. Since $\delta = \lambda = 1$ and $t_0 = 2$, $m = 2p_2$ with $p_2 \equiv 1 \pmod 4$. In addition, $t_1 = 3$ and $t_2 = s = 2$ so $n = -2^c p_1 p_2$ and $n' = -2^{1-c}p_1$ with $c = 0$ or 1 and $p_1 \equiv 1 \pmod 4$. This leads to the genus structure shown below:

G_1			G_2		G_0	
2	p_1	p_2	2	p_1	2	p_2
+	+	+	+	+	+	+
−	−	+	−	−	+	+
−	+	−	+	+	−	−
+	−	−	−	−	−	−

If $N(\epsilon) = -1$, then $r_1 = 1$ and $r_0 = r_2 = 0$. Thus k_0, k_1, and k_2 have one class per genus. It follows that $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$. Hence, 2 is one line 4 of G_1. But the prime divisors of 2 in k_1 do not become principal in K, so line 4 is good. Thus we may assume $N(\epsilon) = +1$. Since $m_1 = 2$, the prime divisor of 2 in k_2 becomes principal in K and must be in the principal genus of k_2. Since $(\frac{2}{p_1}) = (\frac{2}{p_2}) = +1$, the prime divisors of 2 belong to the principal genus in k_1. Thus p_2 determines the bad element of G_1. Thus K contains no sci primes when $(\frac{p_1}{p_2}) = -1$. Part 7,h,1 of the Theorem follows.

Assume line (i) of Theorem 7 holds. Since $t_0 = t_1 = 3$, $t_2 = 2$, $s = 1$ and $\delta = \lambda = 0$, there are exactly four primes dividing the discriminant of K/Q. We may number these primes so that $p_1p_2p_4 \mid \Delta_0$, $p_1p_2p_3 \mid \Delta_1$ and $p_3p_4 \mid \Delta_2$ with $p_3 \not\equiv p_4 \pmod 4$.

The genus structure is given below:

G_1			G_2		G_0'		G_0'	
					$p_1 \not\equiv 1 \not\equiv p_2 \pmod 4$		$p_1 \not\equiv 1 \not\equiv p_4 \pmod 4$	
p_1	p_2	p_3	p_3	p_4	p_1p_2	p_4	p_1p_4	p_2
+	+	+	+	+	+	+	+	+
−	−	+	+	+	+	+	−	−
−	+	−	−	−	−	−	+	+
+	−	−	−	−	−	−	−	−

If $p_1 \not\equiv 1 \not\equiv p_2 \pmod 4$ and $p_4 \not\equiv 3 \pmod 4$, then the character at p_1 normalizes the character at p_2. Since k_1 has only one bad nonprincipal genus and k_0 and k_2 have none, f will always be good.

Now assume that the character at p_4 in G_0' is normalized. This occurs when $p_1 \not\equiv 1 \not\equiv p_4$ and $p_2 \not\equiv 3 \pmod 4$. Here f will be good only if line 4 of G_1 is good. Since $r_0 = 0$, we may assume that k_0 has one class per genus. Also $R_2 = 0$ implies $(\frac{p_4}{p_3}) = +1$ if and only if p_4 is a principal factor in k_0.

First assume that $m = p_1p_2p_4$. Here $n = -p_1p_2p_3$, $m_1 = p_1$, p_2 or p_1p_2 and

$m_2 \nmid \Delta_1$. If $m_1 = p_1$, then $(\frac{p_1}{p_2}) = +1$, so p_1 is not on line 4. If p_1 is not a principal factor of k_0, then $(\frac{p_1}{p_2}) = -1$. Thus p_2 cannot be on line 4. However, when $m_1 = p_1 p_2$ and $m_2 = p_4$, m_1 can be on line 4. This occurs when $(\frac{p_4}{p_2}) = (\frac{p_1}{p_3}) = +1$ and $(\frac{p_2}{p_3}) = (\frac{p_1}{p_2}) = -1$.

Next let $m = p_2 p_4$, $n = -p_2 p_3$, $p_1 = 2$ and the character at p_1 be $(\frac{-1}{x})$. Since $m \nmid \Delta_1$, k_1 has one class per genus and p_2 cannot be on line 1 of G_1. Thus $(\frac{-1}{p_2}) = +1$ implies p_2 belongs on line 4 of G_1. Thus K contains no sci primes if and only if p_2 is a principal factor of k_0. This occurs when $(\frac{p_2}{p_4}) = +1$. As above $(\frac{p_4}{p_3}) = +1$ and $(\frac{p_2}{p_3}) = -1$.

Finally let $m = p_1 p_2$, $n = -p_1 p_2 p_3$, $n' = -p_3 \equiv 3 \pmod 4$ and the character at p_4 be $(\frac{-1}{x})$. If $m_1 = p_1$ and $m_2 = p_2$, then $r_1 = 2$, so k_1 has two classes per genus. Since $(\frac{p_1}{p_2}) = +1$, line 4 is bad only if p_2 is on it. Hence $(\frac{p_2}{p_3}) = -1$. Also $R_1 = 1$ implies $(\frac{p_1}{p_3}) = +1$. Since the prime divisors of 2 in k_0 and k_2 are not in the principal genus, $(\frac{2}{p_2}) = (\frac{2}{p_3}) = -1$. If $m_1 \neq p_1$, then $(\frac{p_1}{p_2}) = -1$. Also $m_1 \nmid \Delta_1$ so line 4 of G_1 is bad if and only if m and p_3 belong on line 4. Hence $(\frac{p_3}{p_1}) = +1$ and $(\frac{p_3}{p_2}) = (\frac{p_1}{p_2}) = -1$. Since $R_2 = 0$, k_2 has two classes per genus exactly when 2 is a principal factor of k_0. Thus $(\frac{2}{p_2}) = (\frac{2}{p_3})$. Line 7,i,3 follows.

Assume now that line (a) of Theorem 8 holds. Since $t_0 = 4$, $t_1 = 3$, $t_2 = 2$, $s = \delta = 1$ and $\lambda = 0$, there exist exactly three odd primes dividing the discriminant of K/Q. These primes can be numbered so that $2p_1p_2p_3 \mid \Delta_0$, $2p_1p_2 \mid \Delta_1$ and $2p_3 \mid \Delta_2$. Note, at least one $p_i \equiv 3 \pmod 4$ and we have four cases depending on which primes satisfy this congruence.

The following genus structures result:

G_1			G_2		G'_0, case I			G'_0, case II			G'_0, case III			G'_0, case IV		
2	p_1	p_2	2	p_3	$2p_1$	p_2	p_3	p_1p_2	p_3	2	$2p_1$	p_1p_2	p_1p_3	$2p_3$	p_1	p_2
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	−	−	+	+	−	−	+	+	+	+	−	+	−	+	−	−
−	+	−	+	+	−	−	+	−	+	−	−	−	+	−	+	−
−	−	+	+	+	+	+	+	−	+	−	+	−	−	−	−	+
+	+	+	−	−	−	+	−	+	−	−	−	+	−	+	+	+
+	−	−	−	−	+	−	−	+	−	−	+	+	+	+	−	−
−	+	−	−	−	+	−	−	−	−	+	+	−	−	−	+	−
−	−	+	−	−	−	+	−	−	−	+	−	−	+	−	−	+

Here $p_1 \equiv 3,\ p_2 \equiv p_3 \equiv 1 \pmod 4$ in case I; $p_1 \equiv p_2 \equiv 3,\ p_3 \equiv 1 \pmod 4$ in case II; $p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod 4$ in case III; and $p_1 \equiv p_2 \equiv 1,\ p_3 \equiv 3 \pmod 4$ in case IV.

First consider Case I. Since $p_1p_2 \equiv 3 \pmod 4$, $n = -2p_1p_2$ and $m = 2^c p_1p_2p_3$. In order for K to have no sci primes, the character system for m_1 must be line 8 of G_1 and lines 6 and 7 must be bad in G'_0. If $m_1 = 2$, then $(\frac{2}{p_2}) = (\frac{2}{p_3}) = +1$. Thus K contains no sci primes if and only if $(\frac{2}{p_1}) = (\frac{p_3}{p_2}) = -1$ and $(\frac{p_3}{p_1}) = +1$. Since the primes above p_1 in k_1 do not become principal in K, $(\frac{p_1}{p_2}) = -1$ yielding line 8,a,1. Suppose $m_2 = p_3 \neq -n'$, then the prime above 2 in k_2 becomes principal in K. Thus 2 determines a bad class in each k_i. Since $R_2 = 0$, $(\frac{2}{p_3}) = +1$. Thus 2 cannot be on line 6 and 7 of G'_0, so K has sci primes. Hence we may assume that the prime divisors of 2 in each k_i are not principal in K. From G_2 we see that $(\frac{2}{p_3}) = -1$. If $(\frac{2}{p_2}) = +1$, then 2 is on line 8 of G_1 showing that it is good. On the other hand, if $(\frac{2}{p_2}) = -1$, then 2 is on lines 6 and 7 in G'_0, so these lines are good.

Next consider case II. Here $m = 2p_1p_2p_3$ and if K contains no sci primes, then line 6 must be bad in G_1 and lines 7 and 8 be bad in G'_0.

If $m_1 = 2$, then $(\frac{2}{p_1p_2}) = (\frac{2}{p_3}) = +1$. Since 2 is not the norm of a principal ideal of k_1, $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$, placing 2 on line 6 of G_1. If $n = -2p_1p_2$, then the character at 2 in G_1 is $(\frac{-2}{x})$ and $(\frac{-2}{p_1}) = (\frac{-2}{p_2}) = +1$. Since $(\frac{p_1}{p_2}) = -(\frac{p_2}{p_1})$, either p_1 or p_2 is on line 1 of G_1. Therefore, one class per genus in k_1 implies $n = -p_1p_2$. Thus p_1p_2

determines the nonprincipal bad element of G_0'. Since $(\frac{2}{p_1p_2}) = +1$, p_1p_2 is on lines 7 and 8 of G_0', yielding line 8,a,2.

Assume now that 2 is not a principal factor of k_0. If 2 determines a bad element in the genus group of each k_i, then 2 must be on line 1 of G_2, i.e., $(\frac{2}{p_3}) = +1$. Since 2 can not be on lines 7 and 8 of G_0', they are good. If the primes above 2 in the quadratic subfields do not become principal in K, then any line corresponding to 2 is good. From G_2, we see that $(\frac{2}{p_3}) = -1$. Thus 2 is either on line 6 of G_1 or it is on lines 7 and 8 of G_0'.

Next consider case III. Here $n' = -2p_3$, $m = 2^c p_1p_2p_3$ and the character at 2 in G_0 is either $(\frac{-1}{x})$ or $(\frac{-2}{x})$. K contains sci primes if line 7 or 8 is good in both G_1 and G_0'. If $m_1 = 2$, then $(\frac{2}{p_1}) = (\frac{2}{p_2}) = (\frac{2}{p_3})$, so 2 is not on line 7 or 8 of G_1. However, if $m_2 = p_3$, the prime above 2 is each k_i becomes principal in K. Since $(\frac{2}{p_3}) = +1$, f is bad when $(\frac{2}{p_1}) \neq (\frac{2}{p_2})$. In order to have neither p_1 nor p_2 on the same line as 2 in G_1, $(\frac{p_1}{p_2}) \neq (\frac{2}{p_2})$. Since $m_2 = p_3$ and $(\frac{2}{p_3}) = +1$, it follows that $(\frac{p_3}{p_1}) = (\frac{p_3}{p_2}) = -1$, yielding line 8,a,3.

For the remaining possible principal factors of k_0, we need to consider the cases where n is odd and even separately. First let $n = -p_1p_2$. Here the character at 2 in G_1 is $(\frac{-1}{x})$ and in G_0 it is $(\frac{-2}{x})$. In order to have $m_1 = p_1$, $(\frac{-2}{p_1}) = (\frac{p_1}{p_2}) = (\frac{p_1}{p_3})$ is necessary. If p_1 is on line 7 in G_1, then $(\frac{p_1}{p_2}) = -1$. Thus $(\frac{2}{p_1}) = -(\frac{-2}{p_1}) = +1$, so 2 is on line 1 or 7 of G_1. Either way, k_1 has two classes per genus and K contains sci primes. If p_1 is on line 8 in G_1, then f is bad if and only if p_2 (and $2p_3$) are on line 7 of G_0'. Since $(\frac{-2}{p_2})(\frac{p_2}{p_1}) = +1$ and $(\frac{p_1}{p_2}) = +1$, $(\frac{2}{p_2}) = +1$ and $(\frac{2}{p_1}) = -1$. Thus 2 is also on line 8 in G_1. Again k_1 contains a good class in each genus.

If $m_1 = 2p_1$ and f is bad, then $2p_1$ must be on line 7 or 8 of G_1. Since $(\frac{-1}{p_1}) = -1$,

p_1 is on the other. This puts 2 on line 6, so $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$. Also, k_2 has one class per genus, so $(\frac{2}{p_3}) = -1$. Thus the prime above 2 in k_0 is in the principal genus contradicting one class per genus.

Now let $n = -2p_1p_2$ and $m = p_1p_2p_3$. Here the characters at 2 in G_0 and G_1 are $(\frac{-1}{x})$ and $(\frac{-2}{x})$, respectively. If $m_1 = p_1$, then $(\frac{p_1}{p_2}) = (\frac{p_1}{p_3}) = (\frac{-1}{p_1}) = -1$, so p_1 is not on line 8 of G_1. Suppose p_1 is on line 7 of G_1. Then $(\frac{p_2}{p_1}) = -(\frac{p_1}{p_2}) = +1$, so p_2 is on line 1 or 7 of G_1. Either way, k_1 has a good class in each genus.

If $m_1 = 2p_1$ and $m_2 = 2p_2p_3$, then 2 is not the norm of an ideal in any k_i which becomes principal in K. Thus we may assume that $(\frac{2}{p_3}) = -1$ and 2 is not on line 1 in G_1 or G_0'. If f is bad then $2p_1$ and p_2 are on line 7 or 8 in G_1. Thus $(\frac{2}{p_2}) = -(\frac{-2}{p_2}) = +1$ placing 2 on line 8 in G_1. This yields $(\frac{2}{p_1}) = -1$, so 2 is on line 8 of G_0' also. Hence K contains sci primes.

Finally assume that $p_1 \equiv p_2 \equiv 1$ and $p_3 \equiv 3 \pmod 4$. Since $R_0 = R_1 = 1$, there is always at least one good line of G that maps to a good line of G_0', so f is good.

Next we assume line (b) of Theorem 8 holds. Since $t_0 = 4$, $t_1 = t_2 = 2$, and $s = \delta = 0$, there exist four primes dividing the discriminant of K/Q with $p_1p_2p_3p_4 \mid \Delta_0$, $p_1p_2 \mid \Delta_1$, and $p_3p_4 \mid \Delta_2$. Note that neither $p_1 \equiv p_2$ nor $p_3 \equiv p_4 \pmod 4$ is possible. Thus we may assume $p_1 \equiv 3$, $p_2 \equiv 1$, $p_3 \not\equiv 3$ and $p_4 \not\equiv 1 \pmod 4$. The following chart shows the genus structure:

G_1		G_2		G_0'		
p_1	p_2	p_3	p_4	p_1p_4	p_2	p_3
+	+	+	+	+	+	+
+	+	−	−	−	+	−
−	−	+	+	−	−	+
−	−	−	−	+	−	−

If K contains no sci primes, then $-n$ and $-n'$ must be on line 4 of G_0'. Since every bad class of k_1 must be in the principal genus, p_1 or p_2 is a principal factor of

k_0 if and only if $(\frac{p_1}{p_2}) = +1$. Similarly, p_3 or p_4 is a principal factor of k_0 if and only if $(\frac{p_4}{p_3}) = +1$. Thus $(\frac{p_1}{p_2}) + (\frac{p_3}{p_4}) < 2$.

Suppose first that $n' = -p_3$ and $p_4 = 2$. Then K contains no sci primes exactly when p_3 is on line 4 of G_0'. Thus $(\frac{p_3}{p_1}) = +1$ and $(\frac{p_3}{p_2}) = -1$. If $m_1 = 2$, then $(\frac{2}{p_2}) = +1$. If 2 is not a principal factor of k_0, then $(\frac{2}{p_3}) = -1$. Since 2 is not on line 4 of G_0', $(\frac{2}{p_2}) = +1$. Line 8,b,1 with $c = 0$ follows.

Suppose now that $n' = -p_3p_4$. Then n and n' are on line 4 of G_0' if and only if $(\frac{p_1p_2}{p_3}) = (\frac{p_3p_4}{p_2}) = -1$ or equivalently $(\frac{p_1}{p_3}) = (\frac{p_4}{p_2}) = -(\frac{p_3}{p_2})$. If $(\frac{p_1}{p_2}) = +1$, then from above p_1 or p_2 is a principal factor of k_0. Thus either $(\frac{p_1}{p_3}) = +1$ or $(\frac{p_2}{p_4}) = (\frac{p_4}{p_2}) = +1$. Assume $(\frac{p_1}{p_2}) = -1$. If $(\frac{p_1}{p_3}) = -1$, then $(\frac{p_2}{p_1p_4}) = +1$ and $(\frac{p_2}{p_3}) = +1$ implying p_2 is a principal factor of k_0, contradicting that $(\frac{p_1}{p_2}) = -1$. Thus $(\frac{p_1}{p_3}) = +1$, yielding line 8,b,1 with $c = 1$.

Finally, assume line (c) of Theorem 8 occurs. Since $t_1 = t_2 = 2$, $t_0 = 3$ and $s = \delta = \lambda = 1$, $m = 2p_1p_2$, $2p_1 \mid \Delta_1$ and $2p_2 \mid \Delta_2$ with $p_1 \equiv p_2 \equiv 1 \pmod 4$. Without loss of generality, $n = -2p_1$ and $n' = -p_2$. This gives the following genus structure:

G_1		G_2		G_0'		
2	p_1	2	p_2	2	p_1	p_2
+	+	+	+	+	+	+
+	+	−	−	−	+	−
−	−	+	+	−	−	+
−	−	−	−	+	−	−

Again K contains no sci primes if and only if p_2 is on line 4 of G_0'. If $N(\epsilon) = -1$, then $r_1 = r_2 = 0$, so $(\frac{2}{p_2}) = -1$. Hence, p_2 is not on line 4 of G_0'. Similarly, if $N(\epsilon) = +1$ and 2 is not a principal factor of k_0 then $(\frac{2}{p_2}) = -1$, so line 4 of G_0' is good. However, if $m_1 = 2$ and $m_2 = p_1p_2$, then $(\frac{2}{p_1}) = (\frac{2}{p_2}) = +1$. Hence, p_2 is on line 4 of G_0' if and only if $(\frac{p_1}{p_2}) = -1$.

Lemma 15. *If $h_i > 2^{r_i}$ for $i = 0, 1, 2$ and K/k_1 is unramified, then K contains sci* *primes except possibly when* $h_1/|G_1| = 2^{r_1 - R_1}$ *and* R_1, r_1, t_0, t_1, t_2 *have the values listed below:*

	R_1	r_1	t_0	t_1	t_2
(a)	2	2	3	4	1
(b)	2	2	2	4	2
(c)	1	2	2	3	1
(d)	1	1	1	3	2
(e)	1	1	2	3	1
(f)	0	1	1	2	1

In line (b) we also require $\lambda = 0$.

PROOF: If $h_1/|G_1| > 2^{r_1 - R_1}$ or $h_1 > 2^{r_1+1}$, then K has sci primes by Corollary 1 to Theorem 5. Since K/k_1 is unramified, $\delta = 0$ and $s = t_2$, so $t_1 = t_0 + t_2$. If $t_0 \geq 3 - \lambda$ and $t_2 \geq 2$, then by Theorem 7 and its Corollary, K contains sci primes. Thus we may assume $h_1/|G_1| = 2^{r_1 - R_1}$ and $h_1 = 2^{r_1+1}$. Since $|G_1| = 2^{t_1 - 1}$, $t_1 = R_1 + 2$. If $r_1 = 2$, then by Theorem 4, $t_0 \geq 2$, so $t_1 \geq 3$. If $r_1 = 1$, then $t_1 \geq 2$. The values listed in the chart follow.

LEMMA 16. *Lines (a), (b), (d) and (e) of Lemma 15 are always good assuming that the known list of imaginary quadratic fields containing one class per genus is complete.*

PROOF: In each of lines (a), (b), (d) and (e), k_1 must contain one class per genus. In lines (d) and (e), $t_1 = 3$. In all known cases where $t_1 = 3$ and k_1 has one class per genus, either k_0 or k_2 has class number one.

In lines (a) and (b), $t_1 = 4$ and $r_1 = 2$, so $N(\epsilon) = +1$. In line (a), $t_2 = 1$ and for all known cases, $h_2 = 1$ except when $k_0 = Q(\sqrt{15})$, $k_1 = Q(\sqrt{-345})$ and $k_2 = Q(\sqrt{-23})$. In this case $m_1 = 6$ and $m_2 = 10$. Since $\left(\frac{-23}{10}\right) = -1$, Corollary 1(c) to Theorem 5 shows that K contains sci primes. For line (b) all known cases with $t_0 = t_2 = 2$, $\lambda = 0$ and k_1 containing one class per genus have $h_0 = 1$ for all choices of k_0.

THEOREM 10. *If* $h_i > 2^{r_i}$ *for* $i = 0, 1, 2$ *and* K/k_1 *is unramifed, then* K *contains sci* *primes except when* $h_1/|G_1| = 2^{r_1-R_1}$ *and* m*,* n *and* n' *meet one of the following conditions:*

i) $m = p_1{}^c p_2$, $n = -p_1{}^c p_2 p_3$, $n' = -p_3$ *with* $N(\epsilon) = +1$, $c = 0$ *or 1,* $(c = 0$ *only if* $p_1 = 2$ *and* $p_2 \equiv 3 \pmod 4)$*), either* $p_1 = 2$ *or* $p_1 \equiv p_2$, $p_3 \equiv 3 \pmod 4$ $(\frac{p_1}{p_3}) = (\frac{p_2}{p_3}) = +1$*, and* $(\frac{\pm p_1}{p_2}) = -1$*, or*

ii) $m = p_1$, $n = -p_1 p_2$, $n' = -p_2$ *with* $p_1 \equiv 1$, $p_2 \equiv 3 \pmod 4$ *and* $(\frac{p_1}{p_2}) = +1$.

PROOF: We need only consider the fields where $h_1/|G_1| = 2^{r_1-R_1}$ and the discrimants of k_0, k_1 and k_2 have the number of prime divisors listed in lines (c) and (f) of Lemma 15.

In line (c) k_1 has the genus structure shown below:

G_1		
p_1	p_2	p_3
$+$	$+$	$+$
$-$	$-$	$+$
$+$	$-$	$-$
$-$	$+$	$-$

Moreover, $m = p_1{}^c p_2$, $n = -p_1{}^c p_2 p_3$ and $n' = -p_3$ where $p_3 \equiv 3 \pmod 4$ and either $p_1 = 2$ or $p_1 \equiv p_2 \pmod 4$. Since $r_1 = 2$, $N(\epsilon) = +1$ with $m_1 = p_1$ and $m_2 = p_1{}^{1-c} p_2$. We may assume k_1 has two classes per genus. Here the first two lines of G_1 correspond to the classes containing primes which split completely in K. Thus K contains no sci primes if and only if $(\frac{m_1}{p_3}) = (\frac{m_2}{p_3}) = +1$. If $c = 0$, then $p_1 = 2$, $p_2 \equiv 3 \pmod 4$, $m_1 = 2$ and $m_2 = 2p_2$. The above statement is equivalent to $(\frac{2}{p_3}) = (\frac{p_2}{p_3}) = +1$. Since $p_2 \equiv 3 \pmod 4$, p_2 is on line 2. Thus each of the genera corresponding to the top two lines of G_1 contains two bad classes. If $c = 1$, then the above condition becomes $(\frac{p_1}{p_3}) = (\frac{p_2}{p_3}) = +1$. When $p_1 = 2$ and $p_2 \equiv 3 \pmod 4$, the character at p_1 is $(\frac{-2}{x})$. Since $(\frac{-2}{p_2}) \neq (\frac{2}{p_2})$, 2 and p_2 are not both on line 1. Again, each of the top two lines of G_1 contains two bad classes. Similarly if $p_1 \equiv p_2 \equiv 3$

(mod 4), then $(\frac{p_1}{p_2}) \neq (\frac{p_2}{p_1})$ and the result follows. If $p_2 \equiv 1 \pmod 4$, then we need $(\frac{p_1}{p_2}) = (\frac{p_2}{p_1}) = -1$ to ensure that exactly two bad classes belong to each of these genera.

If line (f) of Lemma 15 holds, then $m = p_1$, $n = -p_1p_2$ and $n' = -p_2$ with $p_1 \equiv 1$ and $p_2 \equiv 3 \pmod 4$. Here only the principal genus of k_1 contains primes which split in K. Thus K contains no sci primes when k_1 has two classes per genus and $(\frac{p_1}{p_2}) = +1$.

§6 Conclusions and Numerical Results.

In this section it is our objective to determine all imaginary bicyclic biquadratic fields K such that $h_i > 2^{r_i}$ for $i = 0, 1, 2$ and K contains no sci primes, i.e. to determine all exceptional fields. It follows from Theorems 9 and 10 that if $h_1 > 8$ or K/k_1 is ramified and $h_2 > 4$, then K is not an exceptional field. A well known result of Heilbronn [10] shows that there are only finitely many imaginary quadratic fields with bounded class number. Therefore, there are only finitely many exceptional fields K.

If K is an exceptional field, then Theorem 9 and 10 show $r_i - R_i \leq 1$ for $i = 1, 2$, i.e. k_1 and k_2 have at most two classes per genus. Dickson [7, p. 85] listed 65 imaginary quadratic fields containing one class per genus. It is a long standing conjecture that this list is complete. Chowla and Briggs [6] and Grosswald [8], among others, give results in support of this conjecture. We need to know only those imaginary quadratic fields with two classes per genus having class number 4 or 8. In [3], Buell showed that for imaginary quadratic fields with discriminant greater than -4×10^6, 54 have class number 4 and 131 have class number 8. Those fields with class number 4 are listed in [4]. Of the fields with class number 8, 13 have one class per genus while 54 have two classes per genus.

The real quadratic subfield has one class per genus in all cases listed in Theorem 9. For $m < 24572$, the class number is given in [17]. However, for larger values of m satisfying the hypotheses of Theorem 9, the class number of $Q(\sqrt{m})$ was computed using Dirichlet's class number formula, see [13, p. 440]. The value of $\log \epsilon$ was computed using an ordinary continued fraction algorithm. The class numbers of the real quadratic fields which were computed are listed below.

Class number of $Q(\sqrt{m})$			
m	h_0	m	h_0
26751	4	58174	4
33370	20	62665	4
34210	4	70737	28
43505	4	75905	20
43945	4	81838	4
44473	2	117273	12
45399	4	118105	4
45991	4	136565	2
46345	4	159505	4
49569	4	178585	4
51531	28	235705	4
52207	20	274209	4
52745	4	384865	4

Assuming that the lists in [3, 4, 7] are complete, there are no exceptional fields with K/k_1 unramified and $\underline{88}$ with K/k_1 ramified.

Exceptional fields $K = Q(\sqrt{n}, \sqrt{n'})$ with conductor f					
f	$-n$	$-n'$	f	$-n$	$-n'$
780	195	13	24072	177	34
2184	91	6	24648	1027	78
2220	555	37	24860	1243	5
2860	715	5	27676	187	37
3080	35	22	27740	1387	5
3740	187	5	29784	102	73
5304	102	78	29784	102	146
5576	82	17	30140	1507	5
5576	697	82	31240	355	22
5655	435	95	37596	723	13
5772	1443	13	39372	193	51
5772	1443	37	39516	267	37
6045	403	15	39576	102	97
6216	259	6	39576	102	194
6460	323	5	40120	1003	10
6460	323	85	43068	291	37
7480	187	10	43505	1243	35
7548	51	37	43945	235	187
7752	57	34	47724	123	97
8140	2035	5	49569	403	123
8140	2035	37	49720	1243	10
9672	403	6	52745	1507	35
10120	115	22	53960	355	190
10248	427	6	55480	1387	10
11388	219	13	58056	177	82
12920	323	10	63304	193	82
13640	155	22	63804	1227	13
13884	267	13	78744	386	102
14168	253	14	84040	955	22
14892	73	51	107004	723	37
15132	291	13	118105	1027	115
15405	1027	195	136565	955	715
15405	1027	15	136840	1555	22
16744	91	46	159505	1387	115
17112	93	46	178585	955	187
18312	763	6	181596	1227	37
19788	97	51	183964	1243	37
19880	142	70	222365	1555	715
20060	1003	5	232696	1003	58
20060	1003	85	235705	1003	235
20680	235	22	274209	1027	267
20805	1387	15	327352	1411	58
22792	259	22	384865	955	403
23560	190	155	626665	1555	403

Works Cited

[1] S. Allen and P. A. B. Pleasants, The number of different lengths of irreducible factorization of a natural number in an algebraic number field, Acta Arithmetica 36 (1980), 59–86.

[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] D. H. Buell, Small class numbers and extreme values of L–functions of quadratic fields, Math. Comp. 31 (1977), 786–796.

[4] D. H. Buell, H. C. Williams and K. S. Williams, On the imaginary bicyclic biquadratic fields with class–number 2, Math. Comp. 31 (1977), 1034–1042.

[5] L. Carlitz, A characterization of algebraic number fields with class number two, Proceedings of the American Mathematical Society 11 (1960), 391–392.

[6] S. Chowla and W. E. Briggs, On discriminants of binary quadratic forms with a single class in each genus, Canadian J. of Math. 6 (1954).

[7] L. E. Dickson, Introduction to the Theory of Numbers, Univ. of Chicago Press, Chicago, 1929.

[8] E. Grosswald, Negative discriminants of binary quadratic forms with one class in each genus, Acta Arith. VIII (1963), 295–306.

[9] H. Hancock, Foundations of the Theory of Algebraic Numbers, Macmillan Co., New York, 1931.

[10] H. Heilbronn, On the class number in imaginary quadratic fields, The Quarterly Journal of Mathematics 5 (1934), 150–160.

[11] E. L. Ince, Cycles of Reduced Ideals in Quadratic Fields, Mathematical Tables, IV, British Association for the Advancement of Science, London, 1934.

[12] S. Kuroda, Über den Dirichletschen Körper, J. Fac. Sci. Imp. Univ. Tokyo, Sec. I, Vol. IV, Part 5 (1943), 383–406.

[13] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd ed., Springer–Verlag, Berlin, 1990.

[14] W. Narkiewicz, On algebraic number fields with non–unique factorization, Colloquium Mathematicum 12 (1964), 59–68.

[15] W. Narkiewicz and J. Sliwa, Normal orders for certain functions associated with factorizations in number fields, Colloquium Mathematicum 38 (1978), 323–328.

[16] J. E. Olson, A combinatorial problem on finite abelian groups, Journal of Number Theory 1 (1969), 8–10.

[17] B. Oriat, Theorie Des Nombres (fasciculez) Années 1986/87–1987/88, Publications Mathematiques de la Faculté des Sciences de Besancon, Besacon.

[18] J. Sliwa, Factorizations of distinct lengths in algebraic number fields, Acta Arith. XXI (1976), 399–417.

[19] J. Sliwa, Primes which remain irreducible in a normal field, Colloquium Mathematicum 37 (1977), 159–165.

[20] J. Sliwa, Remarks on factorizations in algebraic number fields, Colloquium Mathematicum 46 (1982), 123–130.

[21] L. Washington, Introduction to Cyclotomic Fields, Springer–Verlag, New York, 1982.

VITA

Daisy Cox McCoy was born on May 15, 1951 in Atlanta, Georgia, the daughter of Anne and Albert Cox. She graduated from Druid Hills High School in 1969. She attended Emory and Henry College and received her Bachelor's degree in Mathematics from Douglass College in 1975. After becoming interested in a teaching career, she returned to school in 1984 and received the M.S. degree in Mathematics from Virginia Tech in 1986. She is currently an instructor of Mathematics at Union College, Barbourville, Kentucky. She is a member of the American Mathematical Society and the Association for Women in Mathematics.

Daisy C McCoy