INFORMATION TO USERS

This material was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again — beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

5. PLEASE NOTE: Some pages may have indistinct print. Filmed as received.

Xerox University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106

CLASS GROUPS OF REAL QUADRATIC NUMBER FIELDS

by

PAUL B. MASSELL

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1975

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

May 9, 1975
date

Professor Harvey Cohn
Chairman, Examining Committee

May 9, 1975
date

Professor Richard Sacksteder
Executive Officer

Professor Burton Randol

Professor Richard Sacksteder

Supervisory Committee

ACKNOWLEDGEMENTS

I wish to thank my advisor, Professor Harvey Cohn for the tremendous encouragement and the many hours of personal attention he gave me during the last four years. His enthusiasm for Number Theory was immediately transmitted to me during the first of those years and it never waned. He was extremely helpful in suggesting various areas ripe for research; indeed the topics discussed in this dissertation are a direct outgrowth of subjects discussed in his course on class field theory.

I would also like to thank Dr. David B. Cohen for some useful discussions on the group theory used in this dissertation.

TABLE OF CONTENTS

CHAPTER I. INTRODUCTION

§1. Historical Remarks

Algebraic Number Theory may be thought of as that branch of number theory where the mystery of prime numbers takes the form of questions about prime ideals. Many of the major theorems of this subject deal with the splitting properties of prime ideals in a higher field. Hilbert, for example, considered the problem of constructing an extension L of an algebraic number field K such that all the prime ideals in the unit class of the class group of K split completely in L. Later Weber considered more general types of ideal classes of K and conjectured that for each such ideal class there exists a unique abelian extension L of K such that all the prime ideals of the given ideal class split completely in K. Takagi, in 1920, proved Weber's conjecture and showed that the Galois group of such an extension is isomorphic to the corresponding ideal class group. Artin later proved this isomorphism was induced by the Frobenius automorphism. Thus, by 1927, the major results of class field theory, as these investigations were now called, were proved.

§2. This Dissertation

In this dissertation I do not attempt to add to the "grand structure" of class field theory. Rather I try to construct many of the objects of class field theory for special base fields, viz. the field of rationals and real quadratic fields. I do this for two reasons: a) to gain a better understanding of these objects and thus the theory as a whole, and b) to derive some results which though specialized are of interest in themselves.

The major emphasis in this paper is the construction of class groups (i.e., ideal groups) for the above-mentioned base fields. I use a known formula for calculating the order of ray class groups. This formula has only one factor that is difficult to determine for the case of real quadratic fields. The difficult factor involves the order of the fundamental unit modulo the modulus of the ray class group. We obtain values for this factor for various types of primes. Then knowing the order of the ray class group we find its structure for prime powers by reducing the problem as much as possible to the rational case where we can use primitive roots as generators. Then knowing the structure for prime powers we find a recurring pattern of subgroups among the sequence of ray class groups with successively higher powers of a prime power modulus. This allows us to calculate the number of ideal groups with prime power conductor in real quadratic fields.

Along the way to these results I give some examples of class fields and in so doing illustrate some of the major theorems of class field theory. I also derive necessary and sufficient conditions for solvability of some specific rational congruences using generators of class field extensions.

I assume the reader has a knowledge of Algebraic Number Theory, especially some knowledge of real quadratic fields.

CHAPTER II. BASIC DEFINITIONS, FACTS, AND THEOREMS OF CLASS FIELD THEORY

§1. Moduli, Ideal Groups, and Conductors

Note: For all of the definitions and many of the statements of theorems in this chapter I follow Janusz [12].

We consider an algebraic number field K and its ring of algebraic integers R. The ideal group I_K of K is the group of fractional R-ideals of K. It is the free abelian group with the finite primes as generators. The multiplicative group of nonzero elements in K is denoted by K^*. There is a natural map i which sends K^* into I_K by mapping an element α in K onto the principal ideal $(\alpha) = \alpha R = i(\alpha)$. The kernel of i is the group U_K of units in R. The structure of U_K is given by Dirichlet's unit theorem. The cokernel of i is by definition the class group of K, denoted by C_K. We know that C_K is a finite group. We summarize these facts with an exact sequence.

$$1 \to U_K \to K^* \to I_K \to C_K \to 1 \quad .$$

Definition: A modulus for K is a formal product $m = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ taken over all primes $\mathfrak{p}$ of K in which $n(\mathfrak{p})$ is a nonnegative integer and $n(\mathfrak{p}) > 0$ for only a finite number of $\mathfrak{p}$. Furthermore $n(\mathfrak{p}) = 0$ or 1 when $\mathfrak{p}$ is a real infinite prime and $n(\mathfrak{p}) = 0$ when $\mathfrak{p}$ is a complex infinite prime.

A modulus m may be considered a product $m_0 m_\infty$ with m_0 the product of the finite primes appearing with positive exponent in m and m_∞ the product of the real primes in m. Then m_0 is identified with an integral ideal; that is an ideal in R.

One can extend the notion of congruence between two elements of R modulo an ideal to a notion of congruence between elements of K^* modulo

a modulus.

Let $\mathfrak{p}$ denote a real prime of K. Then $\mathfrak{p}$ corresponds to a real conjugate $x \to x^i$ field of K.. For elements α,β in K^* we write $\alpha \equiv \beta \bmod \mathfrak{p}$ if $(\alpha/\beta)^i > 0$. If $\mathfrak{p}$ is a finite prime and α,β are in K^* then $\alpha = a/c$, $\beta = b/d$ where a,b,c,d are in R. Then we write $\alpha \equiv \beta \bmod \mathfrak{p}^n$ if $\alpha/\beta = ad/bc$ is in the valuation ring $R_{\mathfrak{p}}$ of $\mathfrak{p}$ (i.e., $V_{\mathfrak{p}}(\alpha/\beta) \geq 0$) and this elements is congruent to $1 \bmod \mathfrak{p}^n$; i.e., ad-bc/bc is in $\mathfrak{p}^n$.

Some care must be taken with congruences defined for elements of K^* because they can be multiplied but not added. By this we mean $\alpha_1 \equiv \beta_1$ and $\alpha_2 \equiv \beta_2 \bmod \mathfrak{p}^n$ implies $\alpha_1\alpha_2 \equiv \beta_1\beta_2 \bmod \mathfrak{p}^n$ but it need not follow that $\alpha_1 + \alpha_2 \equiv \beta_1 + \beta_2 \bmod \mathfrak{p}^n$. For example, with $K = Q$ and p a prime we take $\alpha = 1/p$, $\beta = p+1/p$. Then $\beta/\alpha = p+1 \equiv 1 \bmod p$ and so $\alpha \equiv \beta \bmod p$. However, we do not have $\alpha-\alpha \equiv \beta-\alpha \bmod p$ because $\beta-\alpha = 1 \not\equiv 0 \bmod p$.

<u>Definition</u>: For α,β in K^* we write $\alpha \equiv \beta \bmod \mathfrak{m}$ if $\alpha \equiv \beta \bmod \mathfrak{p}^{n(\mathfrak{p})}$ for all primes $\mathfrak{p}$ with $n(\mathfrak{p}) > 0$.

<u>Definition</u>: $K_{\mathfrak{m}} = \{a/b \mid a,b \text{ in } R,\ aR,\ bR \text{ relatively prime to } \mathfrak{m}_0\}$.

$$K_{\mathfrak{m},1} = \{\alpha \text{ in } K_{\mathfrak{m}},\ \alpha \equiv 1 \bmod \mathfrak{m}\}.$$

Notice that $K_{\mathfrak{m}}$ depends only upon the finite primes dividing $\mathfrak{m}_0$ and not upon their exponents.

The group $K_{\mathfrak{m},1}$ is sometimes called the "ray mod $\mathfrak{m}$".

For a set S of primes, let I^S denote the part of the ideal group I_K generated by primes outside S. Let $I^{\mathfrak{m}}$ denote I^S where S is the set of primes dividing $\mathfrak{m}_0$. Thus $I^{\mathfrak{m}}$ does not depend upon the exponents of the primes dividing $\mathfrak{m}$. Clearly the image under i of $K_{\mathfrak{m}}$

or $K_{m,1}$ lands in I^m. The quotient $I^m/i(K_{m,1})$ is called the ray class group mod m and the cosets of $i(K_{m,1})$ in this quotient are the ray classes mod m.

Fact 1: Let $m_1,\ldots,m_n$ be pairwise relatively prime moduli and let m denote the product $m = m_1 \ldots m_n$. The natural map from K_m into the Cartesian product ΠK_{m_i} induces an isomorphism $K_m/K_{m,1} \cong \Pi K_{m_i}/K_{m_i,1}$.

Fact 2: Fact 1 is equivalent to the fact that given the relatively prime moduli $m_1,\ldots,m_n$ and β_i in K_{m_i} we can find an α in K_m to solve the congruences $\alpha \equiv \beta_i \bmod m_i$.

Fact 3: For any modulus m, the group $K_m/K_{m,1}$ is finite.

Fact 4: If $m = m_0 m_\infty$ and $n = r + 2s$ then $K_m/K_{m,1}$ has order

$$2^r N(m_0) \prod_{p \mid m_0} (1 - (1/N(p))) .$$

Fact 5: Each coset of $K_{m,1}$ in K_m contains an element relatively prime to any given ideal.

Fact 6: For any finite set of primes S, there is a natural isomorphism: $C_K \cong I^S/(I^S \cap i(K^*))$.

Fact 7: Let m be any modulus. Then the ray class group $I^m/i(K_{m,1})$ is a finite group.

Fact 8: h_K divides h_m for any modulus m.

Definition: A subgroup H of I_K is called a congruence subgroup if there is a modulus m such that $i(K_{m,1}) \subseteq H \subseteq I^m$. We say H is defined mod m. Suppose n is a modulus and $n \mid m$. Then I^m is a subgroup of I^n. There may (or may not) be a congruence subgroup H^n defined mod n such that $H = I^m \cap H^n$. When this does hold we say H is the restriction

of H^n to I^m. The first lemma shows H^n is uniquely determined by H and n.

Lemma 1: Let $n|m$ and H^m, H^n be congruence subgroups defined mod m and n. Suppose $H^m = I^m \cap H^n$. Then

(a) $I^m/H^m \cong I^n/H^n$ (b) $H^n = H^m i(K_{n,1})$.

Definition: We say H_1 is equivalent to H_2 (written $H_1 \sim H_2$) if $\exists\, m \ni H_1 \cap I^m = H_2 \cap I^m$.

It is easy to see this is an equivalence relation.

Lemma 2: Let H_1 be defined mod m_1, H_2 be defined mod m_2 and suppose they have a common restriction $H_3 = H_i \cap I^{m_3}$, $i = 1,2$. Let m be the greatest common divisor of m_1 and m_2. Then there is a congruence subgroup H defined mod m such that $H \cap I^{m_i} = H_i$, $i = 1,2$.

Definition: An equivalence class of congruence subgroups is called an ideal group. If H denotes an ideal group and m a modulus for which some congruence subgroup mod m belongs to H, we shall denote that (unique) subgroup by H^m.

Definition: Lemma 2 shows us whenever H^m and H^n belong to the ideal group H, then also $H^{m'}$ is in H for m' = greatest common divisor of m and n. This implies there is a unique modulus $\mathfrak{f}$ such that $H^{\mathfrak{f}}$ in H and H^m in H implies $\mathfrak{f}|m$. Clearly $\mathfrak{f}$ is the g.c.d. of all m for which H^m is in H. This modulus is called the conductor of H.

Fact 9: (From Holzer): If $H^{\mathfrak{f}_1} \cap I^m = H_a$ and $H^{\mathfrak{f}_2} \cap I^m = H_b$ and $H_a \subseteq H_b$ then $\mathfrak{f}_2 | \mathfrak{f}_1$.

Let K be any number field and H, J two ideal groups for K.

We say $H \subseteq J$ if for some modulus $\mathfrak{m}$, we have $H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}$.

Proposition: $H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}$ for one modulus $\mathfrak{m}$ implies the same inclusion for any modulus divisible by the conductor of H and the conductor of J.

Proof: First note (1) that if $H^y \in H$ and $y|x$ then $\exists\, H^x \in H$ (i.e., $H^x \sim H^y$) viz. $H^x = H^y \cap I^x$. Let $\mathfrak{f}, \mathfrak{f}'$ be the conductors of H, J respectively. The claim is that if for some $\mathfrak{n}$, $\mathfrak{f}|\mathfrak{n}$ and $\mathfrak{f}'|\mathfrak{n}$ then $H^{\mathfrak{n}} \subseteq J^{\mathfrak{n}}$. Let $\mathfrak{s}$ = l.c.m. $(\mathfrak{f}, \mathfrak{f}')$. Then $\mathfrak{s}|\mathfrak{m}$ (the l.c.m. divides all common multiples). Then by

(1) $\exists\, H^{\mathfrak{s}}, J^{\mathfrak{s}}$ (viz. $H^{\mathfrak{s}} = H^{\mathfrak{f}} \cap I^{\mathfrak{s}}$; $J^{\mathfrak{s}} = J^{\mathfrak{f}} \cap I^{\mathfrak{s}}$) $\ni H^{\mathfrak{s}} \sim H^{\mathfrak{m}}$, $J^{\mathfrak{s}} \sim J^{\mathfrak{m}}$.

So by Lemma 1(b) $H^{\mathfrak{s}} = H^{\mathfrak{m}}\, i(K_{\mathfrak{s},1})$; $J^{\mathfrak{s}} = J^{\mathfrak{m}}\, i(K_{\mathfrak{s},1})$. Since we are given $H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}$ we have $H^{\mathfrak{s}} \subseteq J^{\mathfrak{s}}$. Now if $\mathfrak{f}|\mathfrak{n}$ and $\mathfrak{f}'|\mathfrak{n}$ then $\mathfrak{s}|\mathfrak{n}$ so by (1) $\exists\, H^{\mathfrak{n}}, J^{\mathfrak{n}} \ni H^{\mathfrak{n}} \sim H^{\mathfrak{s}}$ and $J^{\mathfrak{n}} \sim J^{\mathfrak{s}}$, viz. $H^{\mathfrak{n}} = H^{\mathfrak{s}} \cap I^{\mathfrak{n}}$; $J^{\mathfrak{n}} = J^{\mathfrak{s}} \cap I^{\mathfrak{n}}$. Since $H^{\mathfrak{s}} \subseteq J^{\mathfrak{s}}$ we have $H^{\mathfrak{n}} \subseteq J^{\mathfrak{n}}$ //

§2. The Artin Reciprocity Theorem and the Classification Theorem

Let L/K be a finite-dimensional Galois extension with Galois group G. Let $\mathfrak{p}$ denote a prime ideal of K and let its decomposition in L be $\mathfrak{p} = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^e$. Set $\mathfrak{B} = \mathfrak{B}_1$ and $G(\mathfrak{B}) = \{\sigma \in G \,|\, \sigma(\mathfrak{B}) = \mathfrak{B}\}$. We call $G(\mathfrak{B})$ the decomposition group of $\mathfrak{B}$. Let q be the order of the residue field $R/\mathfrak{p}$.

Fact 10: There is a unique automorphism $\sigma \in G(\mathfrak{B})$ which satisfies $\sigma(x) \equiv x^q \bmod \mathfrak{B}$, $x \in R'$. This automorphism is called the Frobenius automorphism of $\mathfrak{B}$.

Fact 11: If L/K is abelian, then the Frobenius automorphism is the same for all the $\mathfrak{B}_i$ dividing $\mathfrak{p}$ and thus really depends only on $\mathfrak{p}$. Thus we denote it by $[L/K \,/\, \mathfrak{p}]$.

Definition: Let S denote a finite set of primes of K including all the primes which ramify in L. For each element $\mathfrak{A}$ in I^S we shall define an element $\varphi_{L/K}(\mathfrak{A})$ in G. First factor $\mathfrak{A}$ as $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ and then set $\varphi_{L/K}(\mathfrak{A}) = \prod_{\mathfrak{p}} \left[\frac{L/K}{\mathfrak{p}}\right]^{a(\mathfrak{p})}$. The product is well defined because G is abelian. The function $\varphi_{L/K}$ is a homomorphism from I^S into G and is called the Artin map for the extension L/K.

Definition: We say the reciprocity law holds for the triple $(L,K,\mathfrak{m})$ if $G(L/K)$ is abelian and $i(K_{\mathfrak{m},1}) \subseteq \ker \varphi_{L/K}$.

The Artin Reciprocity Theorem: Let L/K be an extension with abelian Galois group G. Let $\mathfrak{m}$ be a modulus for K divisible by all primes which ramify in L and assume the exponents of the prime divisors of $\mathfrak{m}$ are sufficiently large. Then the Artin map $\varphi_{L/K}$ maps $I_K^{\mathfrak{m}}$ onto G and the kernel is $N_{L/K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$.

Fact 12: A fundamental property of the Artin map is that $\varphi_{L/K}(\mathfrak{p}) = 1 \Leftrightarrow \mathfrak{p}$ splits completely in L. Thus the ideal group $N_{L/K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$ contains all primes that split completely in L.

Again suppose L/K is an abelian extension. Let $\mathfrak{m}$ be a modulus such that the reciprocity law holds for $(L,K,\mathfrak{m})$. Then the kernel of $\varphi_{L/K}$ acting on $I^{\mathfrak{m}}$ is a congruence subgroup which we shall denote by $H^{\mathfrak{m}}(L/K)$. If $\mathfrak{m}'$ is another modulus such that the reciprocity law holds for $(L,K,\mathfrak{m}')$ then $H^{\mathfrak{m}'}(L/K)$ and $H^{\mathfrak{m}}(L/K)$ have a common restriction in $I^{\mathfrak{m}\mathfrak{m}'}$. This is immediate because $\ker(\varphi_{L/K}|I^{\mathfrak{m}}) \cap I^{\mathfrak{m}\mathfrak{m}'} = \ker(\varphi_{L/K}|I^{\mathfrak{m}\mathfrak{m}'}) = \ker(\varphi_{L/K}|I^{\mathfrak{m}'}) \cap I^{\mathfrak{m}\mathfrak{m}'}$.

Definition: The above implies there is a unique ideal group -- denoted by $H(L/K)$ -- containing $H^{\mathfrak{m}}(L/K)$. This ideal group is called the class

group to L and L is called the class field to $H(L/K)$. The conductor of $H(L/K)$ is denoted by $\mathfrak{f}(L/K)$.

The Classification Theorem: Let K be any algebraic number field. The correspondence $L \to H(L/K)$ is a one-to-one inclusion reversing correspondence between the collection of finite dimensional abelian extensions L/K and the collection of ideals groups of K.

This is the main theorem in class field theory. It gives the classification of all abelian extensions of K in terms of objects defined by the internal structure of K.

CHAPTER III. CLASS GROUPS OF Q AND THEIR CORRESPONDING CLASS FIELDS

§1. Congruence Subgroups Defined mod 12^∞ and mod 20^∞

Now we will look at some examples of the concepts introduced in Chapter II. Throughout the remainder of this paper we will use slightly different notation from that in Chapter II. $\mathcal{J}_m^* \equiv I^m$, $\mathcal{J}_m^1 \equiv i(K_{m,1})$.

Note: In this chapter we consider extensions K/Q ($K = L$ of Chapter II). Q has 1 infinite real prime, denoted simply by ∞ .

$a \equiv b \bmod p^\infty \Leftrightarrow a \equiv b \bmod p$, $(ab,p) = 1$ and $a/b > 0$.

Example 1: $m = 12^\infty$. Step 1: Construct $\mathcal{J}_{12}^*/\mathcal{J}_{12^\infty}^1$. (Note that the "∞" is always dropped from $\mathcal{J}_m^*$ since $\mathcal{J}_{m^\infty}^* = \mathcal{J}_m^*$) . This will be a finite abelian group, indeed since $k = Q$, $\mathcal{J}_m^*/\mathcal{J}_{m^\infty}^1 \cong (\mathbb{Z}/(m))^*$. $\mathcal{J}_{12}^*/\mathcal{J}_{12^\infty}^1 = \{(1)(5)(7)(11)\}_{12^\infty}$. The subscript on the right-hand expression is the "preliminary" explanation modulus.

Step 2: In order to find the conductor of the ideal group to which $G = \{(1)(5)(7)(11)\}\,\mathcal{J}_{12^\infty}^1$ belongs we must find the congruence subgroup with the smallest explanation modulus which is equivalent to G . In this case it is easy; $G \cong \{(1)\}_1$ since $G \cap \mathcal{J}_{12^\infty}^* = \{(1)\}_1 \cap \mathcal{J}_{12^\infty}^*$. Thus $\mathfrak{f} = 1$ and since G is of index 1 in $\mathcal{J}_{12}^*/\mathcal{J}_{12^\infty}^1$ the class field K satisfies $|K/Q| = 1$ which implies $K = Q$. Similarly if $G = \{(1)(7)\}\,\mathcal{J}_{12^\infty}^1$, $G \cong \{(1)\}\,\mathcal{J}_{3^\infty}^1$ and G is not equivalent to any congruence subgroup with lower explanation modulus, therefore $\mathfrak{f} = 3^\infty$. Now we use some major theorems, viz.

Theorem A: The primes that divide the discriminant of an extension K/k are the primes that ramify; and

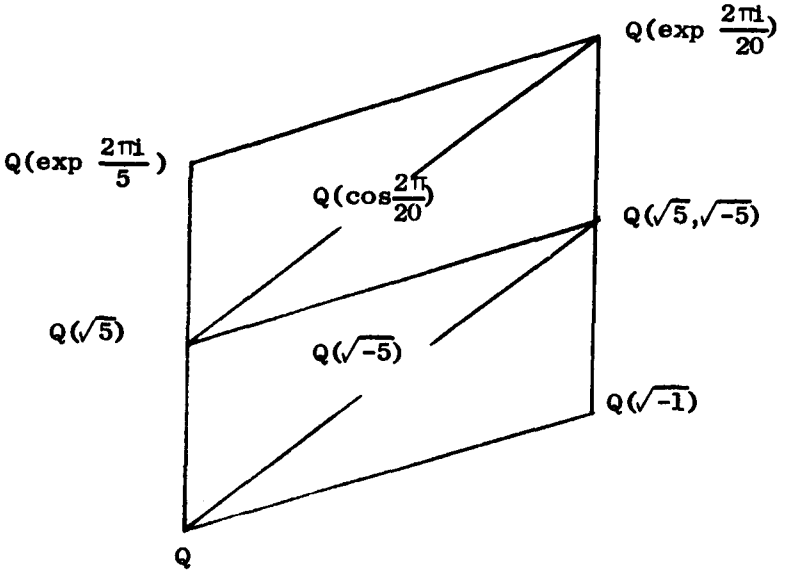
Theorem B: A prime divides $\mathfrak{f} \Leftrightarrow$ it divides the discriminant [12],p. 189. Thus the class field K has these properties; it is of degree 2 over Q, it is imaginary since ∞ ramifies, (cf.[12], p. 94) and 3 is the only

finite prime that ramifies (or equivalently, appears in d). Thus $K = Q(\sqrt{-3})$.

Next let $G = \{(1)(11)\}\mathcal{J}^1_{12\infty}$. We can lower the explanation modulus only from 12^∞ to 12, i.e., $\{(1)(11)\}\mathcal{J}^1_{12^\infty} \cong \{(1)(11)\}\mathcal{J}^1_{12}$ and $\mathfrak{f} = 12$. K then has the properties, $|K/Q| = 2$, it is real, and 2 and 3 are the only primes that ramify; which implies $K = Q(\sqrt{3})$. Next, let $G = \{(1)(5)\}\mathcal{J}^1_{12\infty}$. $G \cong \{(1)\}\mathcal{J}^1_{4\infty}$. Thus $\mathfrak{f} = 4^\infty$ and K has the properties $|K/Q| = 2$, it is imaginary and 2 is the only finite prime that ramifies; thus $K = Q(\sqrt{-1})$. Lastly, let $G = \{(1)\}\mathcal{J}^1_{12\infty}$. By Artin Reciprocity and the fact that $\{(1)\}\mathcal{J}^1_{12\infty}$ contains precisely those primes which split completely in $Q(\exp\frac{2\pi i}{12})$, [1], p. 327, we conclude that $K = Q(\exp\frac{2\pi i}{12})$.

Example 2: $m = 20^\infty$ $\mathcal{J}^*_{20}/\mathcal{J}^1_{20\infty} = \{(1)(3)(7)(9)(11)(13)(17)(19)\}_{20\infty} \cong \{(1)\}_1$ where $\cong$ denotes equivalence of congruence subgroups. These two congruence subgroups are equivalent since there exists a $\mathcal{J}^*_m$ (viz. $\mathcal{J}^*_{20}$) such that $\{(1)(3)(7)(9)(11)(13)(17)(19)\}\mathcal{J}^1_{20\infty} \cap \mathcal{J}^*_{20} = \{(1)\}_1\mathcal{J}^*_1 \cap \mathcal{J}^*_{20}$. Since $\{(1)\}\mathcal{J}^1_1$ is in the ideal group the conductor $\mathfrak{f} = 1$ and the class field is an extension of degree 1, viz. Q itself. Now we consider all the subgroups of $\mathcal{J}^*_{20}/\mathcal{J}^1_{20\infty}$ and ascertain their smallest explanation modulus, i.e., their conductor.
$\{(1)(9)(13)(17)\}\mathcal{J}^1_{20\infty} \cong \{(1)\}\mathcal{J}^1_{4\infty}$ since $\{(1)(9)(13)(17)\}\mathcal{J}^1_{20\infty} \cap \mathcal{J}^*_5 = \{(1)\}\mathcal{J}^1_{4\infty} \cap \mathcal{J}^*_5$. It can shown that $\mathfrak{f} = 4^\infty$ (i.e., $\{(1)\}\mathcal{J}^1_{4\infty}$ is not equivalent to any congruence subgroup with lower explanation modulus). Also by the Classification Theorem the class field K has degree $|\mathcal{J}^*_{20}/\{(1)(9)(13)(17)\}\mathcal{J}^1_{20\infty}| = 2$ over Q. The fact that $\mathfrak{f}$ contains the infinite prime of Q means K is imaginary, and the fact that 2

is the only finite prime that divides $\mathfrak{f}$ means that 2 is the only finite prime that ramifies. Thus $Q(\sqrt{-1})$. We now consider another subgroup of $\mathcal{J}^*_{20}/\mathcal{J}^1_{20\infty}$ of index 2; viz. $G = \{(1)(9)(11)(19)\}_{20\infty} \cong \{(1)(4)\}_5$. Here $\mathfrak{f} = 5$. (Notice that the infinite prime is not necessary since whenever $(x) \in G$, $(20 - x) \in G$). Thus K is real; 5 is the only prime that ramifies, therefore $K = Q(\sqrt{5})$. The last subgroup of index 2 to be considered is $G = \{(1)(3)(7)(9)\}\,\mathcal{J}^1_{20\infty}$. Since G is not equivalent to any congruence subgroups with smaller explanation modulus, $\mathfrak{f} = 20\infty$. Thus $|K/Q| = 2$, K is imaginary and 2 and 5 are the only finite primes that ramify. Thus $K = Q(\sqrt{-5})$. Now we consider subgroups of index 4. First $G = \{(1)(9)\}\,\mathcal{J}^1_{20\infty}$. Here $\mathcal{J}^*_{20\infty}/G$ is the Klein 4-group and $\mathfrak{f} = 20\infty$ which implies K is imaginary; 2 and 5 are the only finite primes which ramify and K/Q has Galois group isomorphic to the Klein 4-group. Thus $K = Q(\sqrt{5}, \sqrt{-5})$. For the final three subgroups $\{(1)(11)\}\,\mathcal{J}^1_{20\infty} \cong \{(1)\}\,\mathcal{J}^1_{5\infty}$, $\{(1)(19)\}\,\mathcal{J}^1_{20}$ and $\{(1)\}\,\mathcal{J}^1_{20\infty}$ we again refer to Artin Reciprocity and the fact that the sets of primes which split completely in $Q(\exp\frac{2\pi i}{m})$ and $Q(\cos\frac{2\pi}{m})$ are $\{(1)\}\,\mathcal{J}^1_{m\infty}$ and $\{(1)(m-1)\}\mathcal{J}^1_{m\infty}$ respectively, to conclude $K = Q(\exp\frac{2\pi i}{5})$, $Q(\cos\frac{2\pi}{20})$, $Q(\exp\frac{2\pi i}{20})$ respectively. Notice the lattice of class fields whose inclusion relations are inverse to the inclusion relations of the corresponding class groups.



§2. Number of Ideal Groups of Q with Conductor $\mathfrak{f}$

Next we give some general recursive formulas for calculating $A_{\mathfrak{f}}$, the number of ideal groups in Q with conductor $\mathfrak{f}$. Then we present a table which gives the first few congruence subgroups in all the ideal groups in Q with $\mathfrak{f} \leq 10^{\infty}$. Hasse, in [9], has a more extensive table with more emphasis on the inclusion relations among the subgroups and less emphasis on the explicit description of each ideal group.

RECURSIVE FORMULAS FOR CALCULATING $A_{\mathfrak{f}}$, THE NUMBER OF IDEAL GROUPS IN Q WITH CONDUCTOR $\mathfrak{f}$.

$$A_1 = 1 \quad A_{1\infty} = 0 \quad A_2 = 0 \quad A_{2\infty} = 0 \quad A_4 = 0 \quad A_{4\infty} = 1$$

if $t \geq 3$ $A_{2^t} = 1$ $A_{2^t{}_\infty} = 2$.

If p is an odd prime we have

$$A_{p^t{}_\infty} = \left(\frac{1}{K+1}\right) \tau(p-1)$$

$$A_{p^t} = \left(\frac{K}{K+1}\right) \tau(p-1) - \delta_{1t}$$

where $\tau(n)$ = number of positive divisors of n

$\delta_{1t} = 1$ if $t = 1$; $\delta_{1t} = 0$ if $t > 1$.

$2^K \parallel (p-1)$.

$A_{2p^t} = A_{2p^t{}_\infty} = 0$.

For $\mathfrak{f}, \mathfrak{f}^\infty$ not of types given above we have

$$A_{\mathfrak{f}} + A_{\mathfrak{f}^\infty} = (\text{number of subgroups of } (\mathbb{Z}_{\mathfrak{f}})^*) - \sum_{\substack{n \mid \mathfrak{f}^\infty \\ n < \mathfrak{f}}} A_n + A_{n^\infty} .$$

TABLE OF IDEAL GROUPS OF Q WITH $\mathfrak{f} \leq 10^{\infty}$

CONDUCTOR	NUMBER OF IDEAL GROUPS	DESCRIPTION
1	1	$H_1 = \{\mathcal{J}_1^*, \mathcal{J}_2^*, \mathcal{J}_3^*, \ldots,\}$
1^{∞}	0	
2	0	
2^{∞}	0	
3	0	
3^{∞}	1	$H_{3^{\infty}} = \{\{(1)\}_{3^{\infty}}, \{(1)\}_{6^{\infty}}, \{(1)(4)(7)\}_{9^{\infty}}, \{(1)(7)\}_{12^{\infty}}, \{(1)(13)(4)(7)\}_{15^{\infty}}, \{(1)(7)(13)\}_{18^{\infty}}, \{(1)(4)(10)(13)(16)(19)\}_{21^{\infty}}, \{(1)(7)(13)(19)\}_{24^{\infty}}, \ldots\}$
4	0	
4^{∞}	1	$H_{4^{\infty}} = \{\{(1)\}_{4^{\infty}}, \{(1)(5)\}_{8^{\infty}}, \{(1)(5)\}_{12^{\infty}}, \{(1)(5)(9)(13)\}_{16^{\infty}}, \{(1)(9)(13)(17)\}_{20^{\infty}}, \{(1)(5)(13)(17)\}_{24^{\infty}}, \ldots\}$
5	1	$H_5 = \{\{(1)(4)\}_5, \{(1)(4)\}_{5^{\infty}}, \{(1)(9)\}_{10}, \{(1)(9)\}_{10^{\infty}}, \{(1)(4)(11)(14)\}_{15}, \{(1)(4)(11)(14)\}_{15^{\infty}}, \{(1)(9)(11)(19)\}_{20}, \{(1)(9)(11)(19)\}_{20^{\infty}}, \{(1)(4)(6)(9)(11)(14)(16)(19)(21)(24)\}_{25}, \ldots\}$
5^{∞}	1	$H_{5^{\infty}} = \{\{(1)\}_{5^{\infty}}, \{(1)\}_{10^{\infty}}, \{(1)(11)\}_{15^{\infty}}, \{(1)(11)\}_{20^{\infty}}, \{(1)(6)(11)(16)(21)\}_{25^{\infty}}, \ldots\}$
6	0	
6^{∞}	0	
7	1	$H_7 = \{\{(1)(6)\}_7, \{(1)(6)\}_{7^{\infty}}, \{(1)(13)\}_{14}, \{(1)(13)\}_{14^{\infty}}, \{(1)(8)(13)(20)\}_{21}, \ldots\}$

CONDUCTOR	NUMBER OF IDEAL GROUPS	DESCRIPTION
7^{∞}	2	$H_{7^{\infty}} = \{\{(1)\}_{7^{\infty}}, \{(1)\}_{14^{\infty}}, \{(1)(8)\}_{21^{\infty}}, \ldots\}$
		$H_{7^{\infty}} = \{\{(1)(2)(4)\}_{7^{\infty}}, \{(1)(9)(11)\}_{14^{\infty}},$ $\{(1)(2)(4)(8)(11)(16)\}_{21^{\infty}}, \ldots\}$
8	1	$H_{8} = \{\{(1)(7)\}_{8}, \{(1)(7)\}_{8^{\infty}},$ $\{(1)(7)(9)(15)\}_{16}, \{(1)(7)(9)(15)\}_{16^{\infty}}$ $\{(1)(7)(17)(23)\}_{24}, \ldots\}$
8^{∞}	2	$H_{8^{\infty}} = \{\{(1)\}_{8^{\infty}}, \{(1)(9)\}_{16^{\infty}}, \{(1)(17)\}_{24^{\infty}}, \ldots\}$
		$H_{8^{\infty}} = \{\{(1)(3)\}_{8^{\infty}}, \{(1)(3)(9)(11)\}_{16^{\infty}},$ $\{(1)(11)(17)(19)\}_{24^{\infty}}, \ldots\}$
9	1	$H_{9} = \{\{(1)(8)\}_{9}, \{(1)(8)\}_{9^{\infty}}, \{(1)(17)\}_{18}, \ldots\}$
9^{∞}	1	$H_{9^{\infty}} = \{\{(1)\}_{9^{\infty}}, \{(1)\}_{18^{\infty}}, \ldots\}$
10	0	
10^{∞}	0	

CHAPTER IV. CLASS GROUPS OF $Q(\sqrt{5})$ AND THEIR CORRESPONDING CLASS FIELDS

§1. Signature; Discussion of Ray Class Groups for $\mathfrak{m} = (2)^t$

Facts about $Q(\sqrt{5})$: Class number = 1, Fundamental Unit = $\epsilon = (1+\sqrt{5})/2$, $N\epsilon = -1$, $\mathfrak{O} = [1,\epsilon]_Z$. Powers are ϵ are Fibonaccian, i.e., $\epsilon^K = F_{K-1} + F_K\epsilon$ where F_K is the K^{th} Fibonacci number. Since most of the calculation involved in computing the order and structure of ray class groups involves powers of the fundamental unit, any simple rule for computing these powers is very helpful. Of course, recursive formulas exist for computing powers of ϵ for any real quadratic field; the Fibonacci formulas being the simplest.

Method for Finding the Order of Ray Class Groups: We use a formula from Cohn [4], p. 2.6, viz. $|\mathcal{J}^*_{\mathfrak{m}}/\mathcal{J}^1_{\mathfrak{m}}| = \frac{2^{r_1}\cdot\Phi(\mathfrak{m})}{[\mathfrak{O}^*:\mathfrak{O}^1_{\mathfrak{m}}]}$ where $\Phi(\mathfrak{m}) = N(\mathfrak{m})\cdot \prod_{\mathfrak{p}|\mathfrak{m}} (1 - (1/N(\mathfrak{p}))$. Here $\mathfrak{m}$ is an arbitrary modulus possibly containing infinite primes, and Φ (generalized Euler φ) and N (the norm) are functions from the group of ideals of $Q(\sqrt{d})$ to Z. Since we are dealing exclusively with real quadratic fields there are two real (infinite) primes; r_1 is 0,1, or 2 depending on whether the modulus $\mathfrak{m}$ contains no infinite primes, 1 infinite prime, or both. We shall abbreviate $\infty \equiv \infty_1 \cdot \infty_2$. Once a modulus is given we can readily calculate the two expressions in the numerator. However, to calculate the denominator we must look at successively higher powers of ϵ until we find the lowest power $Z \ni \epsilon^Z \equiv 1 \bmod \mathfrak{m}$. The only upper bound for Z is the cardinality of the numerator. ($\mathfrak{O}^*$ is the group of units; $\mathfrak{O}^1_{p^\infty}$ the group of units $\equiv 1 \bmod p^\infty$).

Method for Constructing Ray Class Groups: Let us suppose that $\mathfrak{m} = (p)^t$ where (p) is an inert prime ideal. Then first we must find a set of representatives of $\mathfrak{O}/(p)$. There will be $\Phi(p)$ cosets. Then following

Ribenboim [15], P. 120 we can easily find a system of representatives of $\mathcal{O}/(p)^t$. For example if $m = (2)^2$, $\phi(2) = 3$ and $\mathcal{O}/(2) = \{1, \epsilon, 1+\epsilon\}$. $\mathcal{O}/(4)$ has $\phi(4) = 12$ elements; $\mathcal{O}/(4) = \{1, 3, \epsilon, 1+\epsilon, 2+\epsilon, 3+\epsilon, 1+2\epsilon, 3+2\epsilon, 3\epsilon, 1+3\epsilon, 2+3\epsilon, 3+3\epsilon\}$. The most difficult part comes now; we try to find the number of distinct rays generated by elements of $\mathcal{O}/(4)$. For example since $-3 \equiv 1 \bmod 4$, $(-3)\mathcal{J}_4^1 = (1)\mathcal{J}_4^1$. Obviously since $\epsilon, 1+\epsilon, 1+2\epsilon, 2+3\epsilon$ are units $(\epsilon)\mathcal{J}_4^1 = (1)\mathcal{J}_4^1 = (1+\epsilon)\mathcal{J}_4^1 = (1+2\epsilon)\mathcal{J}_4^1 = (2+3\epsilon)\mathcal{J}_4^1$. Since $2+\epsilon \equiv -(2+3\epsilon) \bmod 4$, $(2+\epsilon)\mathcal{J}_4^1 = (1)\mathcal{J}_4^1$. Also since $3\epsilon \equiv -\epsilon \bmod 4$, $3+\epsilon \equiv \epsilon^5 \bmod 4$, $(3\epsilon)\mathcal{J}_4^1 = (3+\epsilon)\mathcal{J}_4^1 = (1)\mathcal{J}_4^1$. Similarly for the remaining elements. Thus $\mathcal{J}_4^*/\mathcal{J}_4^1 = \{1\}$

Signature: If the modulus m contains one or both of the real infinite primes the situation becomes more complicated. For example, $(-3)\mathcal{J}_{4\infty}^1 \neq (1)\mathcal{J}_{4\infty}^1$ because $-3 \not\equiv 1 \bmod 4^\infty$ and there does not exist a unit $\pm \epsilon^Z \ni (-3)(\pm \epsilon^Z) \equiv 1 \bmod 4^\infty$. More generally, $(x)\mathcal{J}_{4\infty}^1 = (y)\mathcal{J}_{4\infty}^1 \Leftrightarrow \exists\, Z \ni x\cdot(\pm \epsilon^Z) \equiv y \bmod 4^\infty$. If x,y are in $\mathcal{O}$ then $x \equiv y \bmod 4^\infty \Leftrightarrow x \equiv y \bmod 4$ and x and y have the same signature, i.e., the same sign pattern for the two conjugates of $Q(\sqrt{5})$. Thus if $x = (a+b\sqrt{5})/2 > 0$ and $x' = (a-b\sqrt{5})/2 > 0$ we say x is totally positive, written either $x \gg 0$ or x is $++$. If $x > 0$ and $x' < 0$, x is $+-$. If $x < 0$ and $x' > 0$, x is $-+$. Finally, if $x < 0$ and $x' < 0$ x is $--$. Note that if $N(x) = xx' > 0$ then x is either $++$ or $--$ and if $N(x) < 0$ then x is either $+-$ or $-+$.

Subgroups of the Ray Class Group: Let us now examine a ray class group for $m = (2)^{3\infty} = (8)^\infty$. One can easily calculate $|\mathcal{J}_8^*/\mathcal{J}_{8\infty}^1| = 8$ and $\mathcal{J}_8^*/\mathcal{J}_{8\infty}^1 = \{(1)(1+4\epsilon)\} \times \{(1)(-7)\} \times \{(1)(1+8\epsilon)\}$. This group has structure $Z_2 \oplus Z_2 \oplus Z_2$. The last two cycles are present only because of the infinite primes contained in m , i.e., $\mathcal{J}_8^*/\mathcal{J}_8^1 = \{(1)(1+4\epsilon)\}$. Let us

consider some congruence subgroups of $\mathcal{J}_8^*$ and the class fields corresponding to their class groups. Let $G = \{(1)(-7)(1+8\epsilon)(1-8\epsilon)\}\mathcal{J}_{8\infty}^1$. G is of index 2 in $\mathcal{J}_{8\infty}^*$ thus the class group to which G belongs (the equivalence class of congruence subgroups) corresponds to a class field K of degree 2 over the base field $Q(\sqrt{5})$. In order to determine K we should first determine the conductor of the class group to which G belongs. The conductor $\mathfrak{f}$ is a divisor of $8\infty = 8\infty_1\infty_2$. If we look closely at the ideals contained in G we see G is the group of ideals generated by elements $1+(8)$ which have all possible signatures. Since all possible signatures are represented no infinite primes will appear in $\mathfrak{f}$. And because this group of ideals could not possibly be defined mod (1),(2), or (4), $\mathfrak{f} = 8$. Since (2) is the only prime which divides $\mathfrak{f}$ it is only prime which divides $d = \text{disc } K/Q(\sqrt{5})$ and thus the only prime which ramifies in that extension. Since $\mathfrak{f}$ contains no infinite primes K must be real. Thus $K = Q(\sqrt{5},\sqrt{2})$. Let us now consider $H = \{(1)(9+4\epsilon)\}\mathcal{J}_{8\infty}^1$. H is of index 4 in $\mathcal{J}_{8\infty}^1$, thus the class group which contains H corresponds to a field of degree 4 over $Q(\sqrt{5})$. Since H contains all ideals generated by $++$ elements from the coset $1+(8)$ and by $++$ elements from the coset $1+4\epsilon+(8)$, we see immediately that $\mathfrak{f}$ must contain the two infinite primes and since H can be defined mod (4) but not mod (2), $\mathfrak{f} = 4\infty_1\infty_2$. Thus K must be imaginary for both conjugates of $\sqrt{5}$ and (2) must be the only prime that ramifies in $K/Q(\sqrt{5})$. Also since $\mathcal{J}_8^*/H \cong Z_2 \oplus Z_2$ the Galois group of $K/Q(\sqrt{5}) \cong Z_2 \oplus Z_2$. Thus $K = Q(\sqrt{5},\sqrt{\epsilon},\sqrt{-\epsilon})$. For a complete table of all subgroups of $\mathcal{J}_{8\infty}^*$ and their conductors and corresponding class field, see below. We have constructed class fields here only to illustrate the

connection between the major structures of class field theory. For the remainder of the paper we will concentrate on describing the class groups for real quadratic fields.

The Pattern of Subgroups of $\mathcal{J}^*_{2^{K_\infty}}$: When dealing with moduli m which are powers of a given prime (p) we can find the number of class groups with $\mathfrak{f} = (p)^K$ by starting with $K = 1$ and working up. That is, first we look at congruence subgroups defined mod p^∞, then mod $p^{2\infty}$, then mod $p^{3\infty}$, etc. Some of those defined mod $p^{K\infty}$ may be explained by a smaller modulus and by starting with $K = 1$ we can determine exactly how many congruence subgroups can be explained by lower moduli. We discovered something quite surprising (to us) for $(m) = (2)^{t\infty}$. After conjecturing that $\mathcal{J}^*_{2^{t+2}}/\mathcal{J}^1_{2^{t+2_\infty}} \cong Z_{2^t} \oplus Z_2 \oplus Z_2$, $t \geq 1$ we found that this sequence of groups has the following nice property:

Theorem: $Z_{2^t} \oplus Z_2 \oplus Z_2$ for $t \geq 2$ has 7 subgroups of index 2; 11 subgroups of index $4,\ldots,2^t$; 7 subgroups of index 2^{t+1}, and 1 subgroup of index 2^{t+2}.

Proof: Consider a subgroup G of index 2. Then G is of the form $Z_{2^{t-1}} \oplus Z_2 \oplus Z_2$ or $Z_{2^t} \oplus Z_2$. We use a counting argument found in Carmichael [2], p. 108. The number of groups of the first form is $\frac{(2^{t-2}\cdot 4)\cdot 6\cdot 4}{(2^{t-2}\cdot 4)\cdot 6\cdot 4} = 1$; of the second form there are $\frac{(4\cdot 2^{t-1})\cdot 6}{(2\cdot 2^{t-1})\cdot 2} = 6$. If $t = 1$ there are $\frac{7\cdot 6}{3\cdot 2} = 7$ subgroups of form $Z_2 \oplus Z_2$. We now consider subgroups G of index 4. G can have either the form $Z_{2^{t-2}} \oplus Z_2 \oplus Z_2$, $Z_{2^{t-1}} \oplus Z_2$, or Z_{2^t}. There is $\frac{(2^{t-3}\cdot 4)\cdot 6\cdot 4}{(2^{t-3}\cdot 4)\cdot 6\cdot 4} = 1$ subgroup of the first type; $\frac{4\cdot 2^{t-2}\cdot 6}{2\cdot 2^{t-2}\cdot 2} = 6$ of the second type and

$\frac{4\cdot 2^{t-1}}{2^{t-1}} = 4$ of the third type. If $t = 1$ there are no groups of the first type, and 7 of type Z_2. If $t = 2$ there are 7 groups $Z_2 \oplus Z_2$ and 4 of type Z_4. More generally for index $4,\ldots,2^{t-1}$ there is one subgroup of type $Z_{2^n} \oplus Z_2 \oplus Z_2$, 6 of type $Z_{2^{r+1}} \oplus Z_2$ and 4 of type $Z_{2^{r+2}}$, $1 \le r \le t-2$. There are always 7 subgroups of order 2. //

From this theorem, it follows, assuming our conjecture, that $\mathcal{J}^*_{2^{t+2}_\infty}$ has 4 congruence subgroups of index 2^t with $\mathfrak{f}^* = 2^{t+2}$, 6 of index 2^{t+1} with $\mathfrak{f}^* = 2^{t+2}$, and 1 of index 2^{t+2} with $\mathfrak{f}^* = 2^{t+2}$, where $\mathfrak{f}^*$ = finite part of $\mathfrak{f}$. More precisely $\mathcal{J}^*_{2^{t+2}_\infty}$ has 1 congruence subgroup of type $Z_2 \oplus Z_2$ for $\mathfrak{f} = 2^{t+2}$, $2^{t+2}\infty_1, 2^{t+2}\infty_2, 2^{t+2}\infty_1\infty_2$, 4 of type Z_2 with $\mathfrak{f} = 2^{t+2}\infty_1\infty_2$, 1 of type Z_2 for $\mathfrak{f} = 2^{t+2}\infty_1$, $2^{t+2}\infty_2$, and 1 of type $\{1\}$ with $\mathfrak{f} = 2^{t+2}\infty_1\infty_2$. The first statement becomes clear by simply looking at the diagram below:

Number of Subgroups of Index I

I =	32	16	8	4	2	
	1 ⊆	7 ⊆	11 ⊆	11 ⊆	7 ⊆	$\mathcal{J}^*_{32}$
		1 ⊆	7 ⊆	11 ⊆	7 ⊆	$\mathcal{J}^*_{16}$
			1 ⊆	7 ⊆	7 ⊆	$\mathcal{J}^*_{8}$

The last statement follows from the fact that if the signature subgroup is denoted by $\{(1)(b)\} \times \{(1)(c)\}$ with $b = -(2^t-1)$ and $c = 1+2^t\epsilon$, then if (c) belongs to a congruence subgroup that subgroup will not have an ∞_2 in its conductor; if (bc) belongs to a congruence subgroup there will be no ∞_1.

Congruence Subgroups of $\mathcal{J}_8^*/\mathcal{J}_{8\infty}^1$ and Their Class Fields

$\mathcal{J}_8^*/\mathcal{J}_{8\infty}^1 = \{(1)(1+4\epsilon)\} \times \{(1)(-7)\} \times \{(1)(1+8\epsilon)\} \longleftrightarrow Q(\sqrt{5})$, $\mathfrak{f} = 1$

7 subgroups of index 2 :

$\{(1)(1+4\epsilon)(-7)(1-4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-2})$, $\mathfrak{f} = 8^{\infty}{}_1{}^{\infty}{}_2$

$\{(1)(1+4\epsilon)(1+8\epsilon)(9+4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-\epsilon})$, $\mathfrak{f} = 4^{\infty}{}_1$

$\{(1)(1+4\epsilon)(1-8\epsilon)(-7-4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{2\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_2$

$\{(1)(-7)(1+8\epsilon)(1-8\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{2})$, $\mathfrak{f} = 8$

$\{(1)(1-4\epsilon)(1+8\epsilon)(-7-4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-2\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_1$

$\{(1)(9+4\epsilon)(-7)(-7-4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-1})$, $\mathfrak{f} = 4^{\infty}{}_1{}^{\infty}{}_2$

$\{(1)(1-8\epsilon)(1-4\epsilon)(9+4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{\epsilon})$, $\mathfrak{f} = 4^{\infty}{}_2$

7 subgroups of index 4 :

$\{(1)(1+4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-2},\sqrt{-\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_1{}^{\infty}{}_2$

$\{(1)(-7)\} \longleftrightarrow Q(\sqrt{5},\sqrt{2},\sqrt{-1})$, $\mathfrak{f} = 8^{\infty}{}_1{}^{\infty}{}_2$

$\{(1)(1+8\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{2},\sqrt{-\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_1$

$\{(1)(1-4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-2},\sqrt{\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_1{}^{\infty}{}_2$

$\{(1)(9+4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{\epsilon},\sqrt{-\epsilon})$, $\mathfrak{f} = 4^{\infty}{}_1{}^{\infty}{}_2$

$\{(1)(1-8\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{2},\sqrt{\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_2$

$\{(1)(-7-4\epsilon)\} \longleftrightarrow Q(\sqrt{5},\sqrt{-1},\sqrt{2\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_1{}^{\infty}{}_2$

1 subgroup of index 8 :

$\{(1)\} \longleftrightarrow Q(\sqrt{5},\sqrt{2},\sqrt{\epsilon},\sqrt{-\epsilon})$, $\mathfrak{f} = 8^{\infty}{}_1{}^{\infty}{}_2$

Subgroups of $\mathcal{J}^*_{16}/\mathcal{J}^1_{16\infty}$

$\mathcal{J}^*_{16}/\mathcal{J}^1_{16\infty} = \{(1)(1+4\epsilon)(1+8\epsilon)(1+12\epsilon)\} \times \{(1)(-15)\} \times \{(1)(1+16\epsilon)\}$.

Let $a = (1+4\epsilon)$, $a^2 = (1+8\epsilon)$, $a^3 = (1+12\epsilon)$, $b = (-15)$, $c = (1+16\epsilon)$.

Then this group can be represented as $Z_4 \oplus Z_2 \oplus Z_2 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3, c, ca, ca^2, ca^3, bc, bca, bca^2, bca^3\}$.

7 subgroups of index 2 :

$\{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$	$Z_4 \oplus Z_2$	$\bar{f} = 8^\infty{}_1{}^\infty{}_2$
$\{1, a, a^2, a^3, c, ca, ca^2, ca^3\}$	$Z_4 \oplus Z_2$	$\bar{f} = 4^\infty{}_1$
$\{1, a^2, ca^2, ba^2, c, b, bc, bca^2\}$	$Z_2 \oplus Z_2 \oplus Z_2$	$\bar{f} = 8$
$\{1, a, a^2, a^3, bc, bca, bca^2, bca^3\}$	$Z_4 \oplus Z_2$	$\bar{f} = 8^\infty{}_2$
$\{1, ba, a^2, ba^3, c, cba, ca^2, cba^3\}$	$Z_4 \oplus Z_2$	$\bar{f} = 8^\infty{}_1$
$\{1, ca, a^2, ca^3, b, cba, ba^2, cba^3\}$	$Z_4 \oplus Z_2$	$\bar{f} = 4^\infty{}_1{}^\infty{}_2$
$\{1, ca, a^2, ca^3, bc, ba, bca^2, ba^3\}$	$Z_4 \oplus Z_2$	$\bar{f} = 4^\infty{}_2$

11 subgroups of index 4 :

$\{1, a, a^2, a^3\}$	Z_4	$\bar{f} = 8^\infty{}_1{}^\infty{}_2$
$\{1, b, c, bc\}$	$Z_2 \oplus Z_2$	$\bar{f} = 16$
$\{1, ba^2, ca^2, bc\}$	$Z_2 \oplus Z_2$	$\bar{f} = 8^\infty{}_2$
$\{1, ba, a^2, ba^3\}$	Z_4	$\bar{f} = 8^\infty{}_1{}^\infty{}_2$
$\{1, ca, a^2, ca^3\}$	Z_4	$\bar{f} = 4^\infty{}_1{}^\infty{}_2$
$\{1, b, a^2, a^2b\}$	$Z_2 \oplus Z_2$	$\bar{f} = 16^\infty{}_1{}^\infty{}_2$
$\{1, c, a^2, a^2c\}$	$Z_2 \oplus Z_2$	$\bar{f} = 8^\infty{}_1$
$\{1, bca, a^2, bca^3\}$	Z_4	$\bar{f} = 8^\infty{}_1{}^\infty{}_2$
$\{1, a^2b, c, a^2bc\}$	$Z_2 \oplus Z_2$	$\bar{f} = 16^\infty{}_1$
$\{1, a^2c, b, a^2bc\}$	$Z_2 \oplus Z_2$	$\bar{f} = 8^\infty{}_1{}^\infty{}_2$
$\{1, bc, a^2, a^2bc\}$	$Z_2 \oplus Z_2$	$\bar{f} = 16^\infty{}_2$

7 subgroups of index 8 :

$\{1,a^2\}$ $\mathfrak{f} = 16\infty_1\infty_2$

$\{1,b\}$ $\mathfrak{f} = 16\infty_1\infty_2$

$\{1,ba^2\}$ $\mathfrak{f} = 16\infty_1\infty_2$

$\{1,c\}$ $\mathfrak{f} = 16\infty_1$

$\{1,ca^2\}$ $\mathfrak{f} = 8\infty_1\infty_2$

$\{1,bc\}$ $\mathfrak{f} = 16\infty_2$

$\{1,bca^2\}$ $\mathfrak{f} = 16\infty_1\infty_2$

1 subgroup of index 16 :

$\{1\}$ $\mathfrak{f} = 16\infty_1\infty_2$

§2. Ray Class Fields Over $Q(\sqrt{5})$ For Primes p and Solvability of Congruences

Example A: $p = (11) = pp'$ in $Q(\sqrt{5})$; $p = (3+2\epsilon)$, $p' = (5-2\epsilon)$, $|\mathfrak{J}_p^*/\mathfrak{J}_p^1| = 1$ and $|\mathfrak{J}_p^*/\mathfrak{J}_{p\infty_1}^1| = 2$. (See Chapter V for relationship between $x_{1,p}$ and $x_{1,p}$) . Since the extension K corresponding to the latter class group is quadratic we can try to find a simple generator for it, say $\sqrt{\xi}$ where $(\xi) = p = (3+2\epsilon)$ and $\xi \equiv \alpha^2 \bmod 4$. The latter condition is necessary since otherwise a factor of (4) would enter the discriminant; [cf. Hilbert [10], p. 374]. Because of the ∞_1 , ξ must be negative but ξ' must be positive. Thus we look for a unit such that $(3+2\epsilon)\cdot\text{unit} \equiv \alpha^2 \bmod 4$. The squares of the residue classes mod 4 have as representatives 1, ϵ^2, and ϵ^4 . Thus we need only solve $(3+2\epsilon) \equiv \text{unit} \bmod 4$. Unit $= -(1+2\epsilon) = -\epsilon^3$ is a unique solution mod 4. Thus $\xi = -(3+2\epsilon)/\epsilon = -3/\epsilon - 2 = 1 - 3\epsilon = (-1-3\sqrt{5})/2$. We see that

$\xi < 0$ and $\xi' > 0$. Thus $K = Q\left(\sqrt{5}, \sqrt{\frac{-1-3\sqrt{5}}{2}}\right)$. We can now obtain an interesting result regarding the solvability of congruences if we recall that by Artin Reciprocity the prime ideals $\mathfrak{p}$ which split in a class field extension are those which are $\equiv 1 \bmod \mathfrak{f}$. Since the ring of integers $\mathfrak{O}$ for $Q(\sqrt{5})$ is a principal ideal domain we can represent $\mathfrak{p}$ as (π). Let us assume that we have a rational prime p such that $(p/5) = 1$ so that there exist a,b in $Z \ni p = ((a+b\sqrt{5})/2)((a-b\sqrt{5})/2)$. We would like to find conditions on a and b such that $((a+b\sqrt{5})/2) \equiv 1 \bmod (3+2\epsilon)\infty_1$. Since $\epsilon^5 \equiv 1 \bmod (3+2\epsilon)\infty_1$ we have 5 possibilities.

(1) $\frac{a+b\sqrt{5}}{2} \cdot 1 \equiv (a-b)/2 + b\epsilon \equiv 1 \bmod (3+2\epsilon)\infty_1$. Equivalently $\frac{a-b-2}{2} + b\epsilon$ is an element of $(3+2\epsilon)$. But the elements of the ideal $(3+2\epsilon)$ have the form $(c+d\epsilon)(3+2\epsilon) = (3c+2d) + (2c+5d)\epsilon$ where c and d are in Z. Thus we must solve the linear system $\frac{(a-b-2)}{2} = 3c+2d$; $b = 2c+5d$.

$c = ((5/2)(a-b-2)-2b)/11$ and c in $Z \Rightarrow (5/2)(a-b-2) - 2b \equiv 0 \bmod 11 \Leftrightarrow a-4b \equiv 2 \bmod 11$. d in Z implies the same condition.

(2) $\frac{(a+b\sqrt{5})}{2} \cdot \epsilon \equiv 1 \bmod (3+2\epsilon)\infty_1 \Leftrightarrow (a-b)/2 + b\epsilon \equiv -\epsilon' \equiv -1+\epsilon$. c,d in $Z \Rightarrow a-4b \equiv 6 \bmod 11$.

(3) $\frac{(a+b\sqrt{5})}{2} \cdot \epsilon^2 \equiv 1$; c,d in $Z \Rightarrow a-4b \equiv 7 \bmod 11$.

(4) $\frac{(a+b\sqrt{5})}{2} \cdot \epsilon^3 \equiv 1$; c,d in $Z \Rightarrow a-4b \equiv 10 \bmod 11$.

(5) $\frac{(a+b\sqrt{5})}{2} \cdot \epsilon^4 \equiv 1$; c,d in $Z \Rightarrow a-4b \equiv 8 \bmod 11$.

Since $4p = a^2-5b^2$ all that is required for the ∞_1 condition to hold is that a be positive ; b may be positive or negative. Thus we have that $\mathfrak{p} = \left(\frac{(a+b\sqrt{5})}{2}\right) \equiv 1 \bmod (2+3\epsilon)\infty_1 \Leftrightarrow a \pm 4b \equiv 2,6,7,8,10 \bmod 11$. But from another point of view, in order for a prime (of degree 1) in

$Q(\sqrt{5})$ to split in K we must have $(\xi/p) = 1$, i.e., $\frac{-1-3\sqrt{5}}{2} \equiv x^2 \bmod p$ for some x in Z. This is equivalent to $(2x^2+1)^2 \equiv 45 \bmod p$ being solvable. Thus we have:

Theorem 1: Let p be a prime $\ni$ $(p/5) = 1$ (i.e., $p \equiv 1,9 \bmod 10$) $p \neq 11$. Let a and b be positive integers $\ni$ $4p = a^2-5b^2$. Then $(2x^2+1)^2 \equiv 45 \bmod p$ is solvable $\Leftrightarrow$ $a \pm 4b \equiv 2,6,7,8,10 \bmod 11$ (i.e., if and only if one of these ten conditions is satisfied).

Examples:

(1) $p = 19$, $4p = 76$, $a = 9$, $b = 1$, $a+4b \equiv 2 \bmod 11$.
$(2x^2+1)^2 \equiv 45 \equiv 7 \bmod 19$ is solvable; solution $x = 9$.

Note: Solvability is determined using the Legendre symbol.

(2) $4p = 124$, $a = 12$, $b = 2$, $a+4b \equiv 9 \bmod 11$, $a-4b \equiv 4 \bmod 11$.
$(2x^2+1)^2 \equiv 45 \bmod 31$ is unsolvable.

Example B: For $(19) = (5-\epsilon)(4+\epsilon) = pp'$, $|\mathcal{J}_p^*/\mathcal{J}_p^1| = 1$ and $|\mathcal{J}_p^*/\mathcal{J}_{p\infty_1}^1| = 2$; thus the procedure for finding ξ is the same as above. It is easily seen that $\xi = -1-2\sqrt{5}$ satisfies the three requirements, $(\xi) = (5-\epsilon)$, $\xi \equiv \alpha^2 \bmod 4$, and $\xi > 0$, $\xi' < 0$. Thus $K = Q(\sqrt{5}, \sqrt{-1-2\sqrt{5}})$. Since $\epsilon^9 \equiv 1 \bmod (5-\epsilon)\infty_1$ we have 18 possible conditions for a and b.

Theorem 2: Let p be a prime $\ni$ $(p/5) = 1$ (i.e., $p \equiv 1,9 \bmod 10$), $p \neq 19$. Let a and b be positive integers such that $4p = a^2-5b^2$. Then $(x^2+1)^2 \equiv 20 \bmod p$ is solvable $\Leftrightarrow$ $a \pm 9b \equiv 2,3,8,10,12,13,14,15,18 \bmod 19$ (i.e., if and only if any of these 18 conditions is satisfied).

Examples:

(1) $p = 11$, $a = 7$, $b = 1$, $a+9b \equiv 16 \bmod 19$, $a-9b \equiv 17 \bmod 19$.
$(x^2+1)^2 \equiv 20 \bmod 11$ is unsolvable.

(2) $p = 29$, $a = 11$, $b = 1$, $a+9b \equiv 1 \bmod 19$, $a-9b \equiv 2 \bmod 19$, $(x^2+1)^2 \equiv 20 \bmod 29$ is solvable.

Example C: $p = (29) = (5+\epsilon)(6-\epsilon)$, $|\mathcal{J}_p^*/\mathcal{J}_p^1| = 2$, $|\mathcal{J}_{4p}^*/\mathcal{J}_{4p}^1| = 4$. Thus we can construct a "tower"of quadratic extensions. Since $5+\epsilon \equiv \alpha^2 \bmod 4$, we can choose $\xi = 5+\epsilon$. There is no sign restriction on ξ since there is no ∞_1 in the first conductor. $K_p = Q(\sqrt{5},\sqrt{5+\epsilon})$ and we are led to a theorem as before.

Theorem 3: Let p be a prime such that $(p/5) = 1$ (i.e., $p \equiv 1,9 \bmod 10$), $p \neq 29$. Let a and b be positive integers such that $4p = a^2 - 5b^2$. Then $(2x^2-11)^2 \equiv 5 \bmod p$ is solvable $\Leftrightarrow \pm a \pm 18b \equiv 2,3,11,14,17,19,21 \bmod 29$ (i.e., if and only if one of these 28 conditions is satisfied).

Examples:

(1) $p = 11$, $a = 7$, $b = 1$, $-a+18b \equiv 11 \bmod 29$, congruence solvable.

(2) $p = 59$, $a = 16$, $b = 2$, $a+18b \equiv 23$, $a-18b \equiv 9$, $-a+18b \equiv 20$, $-a-18b \equiv 6$, congruence unsolvable.

Let us now consider the class field corresponding $\mathcal{J}_{4p}^1$. Since $\mathcal{J}_{4p}^1 \subseteq \mathcal{J}_p^1$ we have $K_p \subseteq K_{4p}$. Assume the generator for this quadratic extension is of the form $\zeta = \sqrt{\lambda+\mu\sqrt{5+\epsilon}}$. Then if $K_{4p}/Q(\sqrt{5})$ is to be relatively abelian K_{4p} must contain all conjugates of ζ. Thus $\eta' = \sqrt{\lambda-\mu\sqrt{5+\epsilon}}$ is in K_{4p} or equivalently $\zeta\zeta' = \sqrt{\lambda^2-\mu^2\sqrt{5+\epsilon}}$ is in K_{4p}. Now $(\zeta\zeta') = (\sqrt{5+\epsilon})$ since $\zeta\zeta' \in K_p$. Thus $\sqrt{\lambda^2-\mu^2(5+\epsilon)} = \sqrt{5+\epsilon}\cdot(\text{unit})$. We see that unit $= \epsilon$, $\lambda = 5+\epsilon$, $\mu = 2$ is a solution. Thus $K_{4p} = Q(\sqrt{5},\sqrt{5+\epsilon},\sqrt{5+\epsilon+2\sqrt{5+\epsilon}})$. It can be shown $\zeta \neq A^2 \bmod 4$ by using the fact that the ring of integers in $Q(\sqrt{5+\epsilon}) = [1,\frac{\epsilon+\sqrt{5+\epsilon}}{2}]_R$ where $R = \mathfrak{G}$. Thus there is a factor of (4) in the discriminant of K_{4p}/K_p.

Using the multiplicativity of differents to compare discriminants of the 4^{th} degree extension with the tower of 2 quadratic extensions we see that the discriminant of $K_{4p}/Q(\sqrt{5})$ also contains a factor of (4). We now make a conjecture similar to that made in the last section. We conjecture that $|\mathcal{J}^*_{2K_p}/\mathcal{J}^1_{2K_p}| = 2^K$ and that $\mathcal{J}^*_{2K_p}/\mathcal{J}^1_{2K_p}$ is cyclic for all K. This is a powerful assumption which implies there is exactly one class group, viz. $\mathcal{J}^1_{2K_p}$ with conductor $2^K p$ for all $K \geq 2$. With this conjecture we again use the fact that the primes which split completely in a class field extension are those which are $\equiv 1 \bmod \mathfrak{f}$, in this case $\mathfrak{f} = 4p$. Such primes (of degree 1) must split in K_p, i.e., $((5+\epsilon)/p) = 1$ and must split in the extension from K_p to K_{4p}, i.e., $(\zeta/p) = 1$. Thus we have

Proposition: (Assuming conjecture) Let p be a prime such that $(p/5) = 1$ (i.e., $p \equiv 1,9 \bmod 10$), $p \neq 29$. Let a and b be positive integers such that $4p = a^2 - 5b^2$. Then the cascading sequence $x_1^2 \equiv 5 \bmod p$, $2x_2^2 - 11 \equiv x_1 \bmod p$, $x_2^2 + 2x_2 \equiv x_3^2 \bmod p$ is solvable $\Leftrightarrow$ $\pm 3a \pm 4b \equiv 4,5,6,9,13,22,28,33,34,35,38,42,51,57,62,63,64,67,71,80,86,91,92,93,96,100,109,115 \bmod 116$ and, letting

a' = (sign in front of $3a$)$\cdot a$

b' = (sign in front of $4b$)$\cdot b$

$a' - 11b' \equiv$	214 mod 232	if $\pm 3a \pm 4b \equiv$	4 mod 116
$\equiv$	108,166,224	$\equiv$	5
$\equiv$	2	$\equiv$	6
$\equiv$	32,148,206	$\equiv$	9
$\equiv$	14,72,188	$\equiv$	13
$\equiv$	162	$\equiv$	22
$\equiv$	222	$\equiv$	28
$\equiv$	40,156,214	$\equiv$	33
$\equiv$	50	$\equiv$	34
$\equiv$	118	$\equiv$	35
$\equiv$	90	$\equiv$	38
$\equiv$	130	$\equiv$	42
$\equiv$	46	$\equiv$	51
$\equiv$	48,164,222	$\equiv$	57
$\equiv$	98	$\equiv$	62
$\equiv$	166	$\equiv$	63

$a' - 11b' \equiv$	118 mod 232	if $\pm 3a \pm 4b \equiv$	64 mod 116
$\equiv$	206	$\equiv$	67
$\equiv$	14	$\equiv$	71
$\equiv$	46	$\equiv$	80
$\equiv$	106	$\equiv$	86
$\equiv$	214	$\equiv$	91
$\equiv$	166	$\equiv$	92
$\equiv$	60,118,176	$\equiv$	93
$\equiv$	206	$\equiv$	96
$\equiv$	14	$\equiv$	100
$\equiv$	46,104,220	$\equiv$	109
$\equiv$	222	$\equiv$	115

Examples:

(1) $p = 11$, $a = 7$, $b = 1$, $-3a-4b \equiv 91 \bmod 116$. Thus $a' = -7$, $b' = 1$ $a'-11b' \equiv 214 \bmod 232$ and sequence is solvable. (Using Legendre symbol to test solvability).

(2) $p = 19$, $a = 9$, $b = 1$, $-3a+4b \equiv 93 \bmod 116$. Thus $a' = -9$, $b' = -1$ $a' - 11b' \equiv 2 \bmod 232$ and sequence is not solvable.

If our conjecture is correct then there is an infinite tower of class fields*, of $Q(\sqrt{5})$ each a quadratic extension over its predecessor, viz. $K_p \subseteq K_{4p} \subseteq K_{8p} \subseteq K_{16p} \subseteq \ldots$. It should be possible to construct generators for each extension although we leave the problem here because of computational difficulties.

*This class field tower should not be confused with those discussed by Golod and Shafarevich where each field is a class field of its predecessor.

CHAPTER V. CLASS GROUPS MOD m OF REAL QUADRATIC FIELDS FOR $m = (p)^t$

§1. General Definitions and Proofs; Normality, Skipping

Definition: An A-field is a real quadratic field in which $N(\epsilon) = -1$; a B-field is a real quadratic field in which $N(\epsilon) = +1$.

Examples: $Q(\sqrt{2}), Q(\sqrt{5}), Q(\sqrt{10})$ are A-fields; $Q(\sqrt{3}), Q(\sqrt{6}), Q(\sqrt{7}), Q(\sqrt{11})$ are B-fields.

Note: In the following results when we say mod p we really mean mod (p) where (p) is an ideal in $Q(\sqrt{d})$ and p is an odd prime of Z.

Definition: $x_{k,p}$ is the smallest power x of the fundamental unit ϵ such that $\epsilon^x \equiv 1 \bmod p^k$.

Lemma 1: Let $r \in \mathbb{Z}$ and $\epsilon^x \equiv r \bmod p$. If $N(\epsilon) = -1$ then $r \equiv \pm 1 \bmod p$ if x is even and $r^2 \equiv -1 \bmod p$ if x is odd. If $N(\epsilon) = 1$ then $r \equiv \pm 1 \bmod p$ regardless of the parity of x .

Proof: Case Ia. $N(\epsilon) = -1$, x even. $\epsilon^x \equiv r \bmod p \Rightarrow$ (taking norms) $(\epsilon')^x \equiv r \bmod p \Rightarrow (\epsilon \cdot \epsilon')^x \equiv r^2 \bmod p \Rightarrow r \equiv \pm 1 \bmod p$.

Case Ib. $N(\epsilon) = -1$, x odd. We have as in Ia. $(\epsilon \cdot \epsilon')^x \equiv r^2 \bmod p$; $-1 \equiv r^2 \bmod p$ (this case can occur only if $p \equiv 1 \bmod 4$).

Case II: $N(\epsilon) = 1$. $\epsilon^x \equiv r \bmod p \Rightarrow (\epsilon \cdot \epsilon')^x \equiv r^2 \bmod p \Rightarrow 1 \equiv r^2 \bmod p \Rightarrow r \equiv \pm 1 \bmod p$. //

Thus if $N(\epsilon) = -1$ powers of ϵ can be congruent to at most 4 rational integers mod p ; if $N(\epsilon) = +1$ at most two.

Now we prove a converse of Lemma 1, which requires that we distinguish between inert and splitting primes p in $Q(\sqrt{d})$. For an inert prime p , the residue class degree $f = |\mathcal{O}/(p)/\mathbb{Z}/(p)| = 2 \Rightarrow$ $\mathcal{O}/(p)$ is a field with p^2 elements. Like any finite field its multiplicative group is cyclic and hence has exactly one element of order 2,

namely -1 . For a splitting prime p , i.e., $(p) = \mathfrak{p}\mathfrak{p}'$, $\mathcal{O}/(p) = \mathcal{O}/\mathfrak{p} \times \mathcal{O}/\mathfrak{p}'$ (cf. Goldstein [7], p. 29) and since $f = |\mathcal{O}/\mathfrak{p} \,/\, \mathbb{Z}/(p)| = 1$, $\mathcal{O}/(p) \cong Z_p \oplus Z_p$ and $\mathcal{O}/(p)$ thus has three elements of order 2.

Lemma 2: If $N(\epsilon) = -1$ then $x_{1,p}$ is even. Furthermore if p is inert then $\frac{1}{2} x_{1,p}$ is even and $\epsilon^{\frac{1}{2}x_{1,p}} \equiv -1 \bmod p$. If $p \equiv 1 \bmod 4$, $\exists\, r \in \mathbb{Z} \ni \epsilon^{\frac{1}{2} x_{1,p}} \equiv r \bmod p$.

Proof: $\epsilon^{x_{1,p}} \equiv 1 \bmod p \Rightarrow (\epsilon')^{x_{1,p}} \equiv 1 \bmod p \Rightarrow (N(\epsilon))^{x_{1,p}} \equiv 1 \bmod p \Rightarrow$ $x_{1,p}$ is even $\Rightarrow$ $\epsilon^{\frac{1}{2}x_{1,p}} \equiv -1 \bmod p$ (since -1 is the only element of order 2) $\Rightarrow (\epsilon')^{\frac{1}{2}x_{1,p}} \equiv -1 \bmod p \Rightarrow (N(\epsilon))^{\frac{1}{2}x_{1,p}} \equiv 1 \bmod p \Rightarrow \frac{1}{2}x_{1,p}$ is even $\Rightarrow \exists\, r \in \mathbb{Z} \ni \epsilon^{\frac{1}{2}x_{1,p}} \equiv r \bmod p$ if $p \equiv 1 \bmod 4$, since $\mathcal{O}/(p)$ is cyclic. //

Definition: Let $(\underset{\sim}{+})$ denote an element of $\mathcal{O} \equiv 1 \bmod p$ with signature $+\ -$. It is clear there always exists such an element.

Lemma 3: "The Equivalence Lemma" . Case Ia of Lemma 1 $\Leftrightarrow (r) \in (1)\, \mathcal{J}^1_{p^\infty}$. Case Ib $\Leftrightarrow (r) \in (\underset{\sim}{+})\, \mathcal{J}^1_{p^\infty}$. Case II $\Leftrightarrow (r) \in \mathcal{J}^1_{p^\infty}$.

Proof: $\epsilon^x \equiv r \bmod p \Leftrightarrow 1 \equiv r(\epsilon^{-x}) \bmod p$. If x is even or $N(\epsilon) = +1$, ϵ^{-x} is totally positive (abbreviated: $+\ +$) so $1 = r(\epsilon^{-x}) \bmod p^\infty \Leftrightarrow$ $(r) \in (1)\, \mathcal{J}^1_{p^\infty}$. If $N(\epsilon) = -1$ and x is odd then ϵ^{-x} is $+\ -$ so if we multiply by $(\underset{\sim}{+})$ we get $1(\underset{\sim}{+}) \equiv r \cdot \epsilon^{-x} \bmod p^\infty$, i.e., $(r) \in (\underset{\sim}{+})\, \mathcal{J}^1_{p^\infty}$. //

Inert Primes

If p is inert $\quad |\mathcal{J}^*_p / \mathcal{J}^1_{p^\infty}| = \dfrac{2^r \cdot N(p) \prod_{\mathfrak{p}|p} (1-(1/N(\mathfrak{p}))}{[\mathcal{O}^* : \mathcal{O}^1_{p^\infty}]} = \dfrac{4 \cdot p^2 (1 - (1/p^2))}{[\mathcal{O}^* : \mathcal{O}^1_{p^\infty}]}$

$= \frac{4(p^2-1)}{[\mathfrak{O}^* : \mathfrak{O}^1_{p\infty}]}$ (where $\mathfrak{O}^*$ is the group of units; $\mathfrak{O}^1_{p\infty}$ the group of units $\equiv 1 \bmod p\infty$.)

Proposition 1: For inert primes p in A-fields, $|\mathcal{J}^*_p/\mathcal{J}^1_{p\infty}| = E(p-1)$ where E is in Z^+ , E odd. For inert primes p in B-fields, $|\mathcal{J}^*_p/\mathcal{J}^1_{p\infty}| = 2E(p-1)$ where E is in Z^+ .

Proof: From Chapter II we know that the decomposition group of the ideal (p) in $Q(\sqrt{d})$ (which equals the Galois group $G = \{1,\sigma\}$ of $Q(\sqrt{d})$ over Q for inert primes) is isomorphic to the Galois group of $\mathfrak{O}/(p)$ over $Z/(p)$. The latter Galois group is generated by $\bar{x} \to \bar{x}^p$; thus the isomorphism implies there is a unique automorphism τ in the decomposition group which satisfies $\tau(x) \equiv x^p \bmod (p)$; $x \in \mathfrak{O}$, τ being the Frobenius automorphism of (p) . Clearly $\tau = \sigma$ for inert primes. Let us denote $\sigma(x)$ by x' as usual. Let η be a primitive root which generates the cyclic multiplicative group (of order p^2-1) of the residue class field $\mathfrak{O}/(p)$. Let $\epsilon \equiv \eta^x \bmod (p)$. Then $\epsilon' \equiv (\eta')^x \bmod p$ and $N(\epsilon) \equiv (\eta\cdot\eta')^x \bmod (p)$. The Frobenius automorphism states $\eta' \equiv \eta^p \bmod (p)$; thus $N(\epsilon) \equiv (\eta^{p+1})^x \bmod (p)$. If $N(\epsilon) = -1$, then $(\eta^{p+1})^x \equiv -1 \bmod (p)$ implies $x = ((p-1)/2)\cdot K$, K in Z , K odd. If $N(\epsilon) = +1$, $(\eta^{p+1})^x \equiv 1 \bmod (p)$ implies $x = (p-1)\cdot K$, K in Z . If $N(\epsilon) = -1$, then $x_{1,p} = 2(p+1)/K$. If $N(\epsilon) = +1$, $x_{1,p} = (p+1)/K$. Thus if $N(\epsilon) = -1$, $[\mathfrak{O}^* : \mathfrak{O}^1_{p\infty}] = 4(p+1)/K$ and $|\mathcal{J}^*_p/\mathcal{J}^1_{p\infty}| = \frac{4(p^2-1)}{4(p+1)/K} = K\cdot(p-1)$ where K is in Z , K odd. If $N(\epsilon) = +1$, $[\mathfrak{O}^* : \mathfrak{O}^1_{p\infty}] = 2(p+1)/K$ and $|\mathcal{J}^*_p/\mathcal{J}^1_{p\infty}| = 2\cdot K(p-1)$, K in Z . //

Numerical evidence is that $E = 1$ for many inert primes in both A and B-fields.

Definition: An inert prime p is normal if $E = 1$. If $E > 1$ it is called special.

Examples:

FIELD	NORMAL INERT PRIMES	SPECIAL INERT PRIMES
$Q(\sqrt{2})$	3,5,11,13,19,37	29,59,197,5741,33461
$Q(\sqrt{3})$	7,17	5,19,29,41,43,53
$Q(\sqrt{5})$	2,3,7,13,17,23,37,43,53, 73	47,107,113,233,1597,28657
$Q(\sqrt{6})$	7,17	11,13,83,89,109
$Q(\sqrt{7})$	5,11,13	17,23,127
$Q(\sqrt{10})$	7,11,17	19,103,131
$Q(\sqrt{11})$		3,13,199

We now wish to examine $|\mathcal{I}^*_{p^K}/\mathcal{I}^1_{p^{K_\infty}}| = \dfrac{4 \cdot p^{2K}(1-(1/p^2))}{[\mathcal{O}^* : \mathcal{O}^1_{p^{K_\infty}}]}$.

In order to calculate $[\mathcal{O}^* : \mathcal{O}^1_{p^{K_\infty}}]$ we need the following proposition.

Proposition 2: Let p be a prime that does not divide $2(\epsilon-\epsilon')^2$. If $p^\lambda \| (\epsilon^{x_{1,p}}-1)$ then $x_{K,p} = p^{K-\lambda} \cdot x_{1,p}$.

Proof: This follows from a result of Lucas called the law of repetition of primes (stated in Dickson [5], p. 396). This law states that if $u_n = (\epsilon^n-(\epsilon')^n)/(\epsilon-\epsilon')$ and u_i is the first term containing the prime factor p to the power λ then u_{pi} is the first term divisible

by $p^{\lambda+1}$ and not by $p^{\lambda+2}$. //

Using Proposition 2 and Lemma 2 we see that $[\mathcal{O}^*:\mathcal{O}^1_{p^{K_\infty}}] = p^{K-\lambda} \cdot [\mathcal{O}^*:\mathcal{O}^1_{p^\infty}]$. Numerical evidence is that $\lambda = 1$ for most p . If for a given p , $\lambda = 1$, then $x_{K,p} = p^{K-1} \cdot x_{1,p}$ and $|\mathcal{I}^*_{p^K}/\mathcal{I}^1_{p^{K_\infty}}| = p^{K-1}|\mathcal{I}^*_p/\mathcal{I}^1_{p^\infty}|$ for all K in Z^+ .

Definition: If $\lambda = 1$ we say p does not skip or p is a non-skipping prime.

For some primes we do notice a "skipping" phenomena; i.e., $\lambda > 1$ which implies $x_{K,p} = x_{1,p}$ for $K = 2,\ldots \lambda$. This implies $|\mathcal{I}^*_{p^K}/\mathcal{I}^1_{p^{K_\infty}}| = p^{2(K-1)}|\mathcal{I}^*_p/\mathcal{I}^1_{p^\infty}|$ for those values of K , and $|\mathcal{I}^*_{p^K}/\mathcal{I}^1_{p^{K_\infty}}| = p^{\lambda-2+K}|\mathcal{I}^*_p/\mathcal{I}^1_{p^\infty}|$ for $K > \lambda$.

Examples:

In $Q(\sqrt{2})$ $\quad |\mathcal{I}^*_{13}/\mathcal{I}^1_{13^\infty}| = 12 = p-1$; $\quad |\mathcal{I}^*_{13^2}/\mathcal{I}^1_{13^{2_\infty}}| = 12\cdot 13^2 = (p-1)p^2$

In $Q(\sqrt{6})$ $\quad |\mathcal{I}^*_7/\mathcal{I}^1_{7^\infty}| = 2\cdot 6 = 2(p-1)$; $\quad |\mathcal{I}^*_{7^2}/\mathcal{I}^1_{7^{2_\infty}}| = 2\cdot 6\cdot 49 = 2(p-1)p^2$

Proposition 3: If $N(\epsilon) = -1$, $E(p-1)p^{K-1}$ divides $|\mathcal{I}^*_{p^K}/\mathcal{I}^1_{p^{K_\infty}}|$.

If $N(\epsilon) = 1$, $2E(p-1)p^{K-1}$ divides $|\mathcal{I}^*_{p^K}/\mathcal{I}^1_{p^{K_\infty}}|$.

Proof: Follows easily from Propositions 1 and 2 . //

Note: We have considered the "ray mod p^∞" rather than the "ray mod p" because of its somewhat more interesting ray class group and the connection of $|\mathcal{I}^*_p/\mathcal{I}^1_{p^\infty}|$ with the class number of quadratic forms of discriminant dp^2 to be discussed later. However, for the sake of

completeness we include the connection with $|\mathcal{I}_p^*/\mathcal{I}_p^1|$.

A-fields: $|\mathcal{I}_p^*/\mathcal{I}_{p\infty}^1| = 2 \cdot |\mathcal{I}_p^*/\mathcal{I}_p^1|$ (since there always exists a $z \ni \epsilon^z \equiv -1 \bmod p$)

B-fields: $|\mathcal{I}_p^*/\mathcal{I}_{p\infty}^1| = |\mathcal{I}_p^*/\mathcal{I}_p^1| \cdot \begin{cases} 4 & \text{if } \nexists\, z \ni \epsilon^z \equiv -1 \bmod p \\ 2 & \text{if } \exists\, z \ni \epsilon^z \equiv -1 \bmod p \end{cases}$.

Splitting primes p $(p = pp')$

$$|\mathcal{I}_p^*/\mathcal{I}_{p\infty}^1| = \frac{4 \cdot p^2(1-(1/p))^2}{[\mathcal{O}^* : \mathcal{O}_p^1]} = \frac{4(p-1)^2}{[\mathcal{O}^* : \mathcal{O}_p^1]}$$

$$|\mathcal{I}_p^*/\mathcal{I}_p^1| = \frac{p(1-(1/p))}{[\mathcal{O}^* : \mathcal{O}_p^1]} = \frac{p-1}{[\mathcal{O}^* : \mathcal{O}_p^1]} \quad .$$

Definition: Let $p = pp'$. p is normal if $|\mathcal{I}_p^*/\mathcal{I}_p^1| = 1$; p is special if $|\mathcal{I}_p^*/\mathcal{I}_p^1| > 1$.

Examples:

FIELD	NORMAL SPLITTING PRIMES	SPECIAL SPLITTING PRIMES
$Q(\sqrt{2})$	7,17,23	41,137,199
$Q(\sqrt{3})$	11,13,23	71,97,181,193
$Q(\sqrt{5})$	11,19,31,41,61	29,89
$Q(\sqrt{6})$	5,19	97
$Q(\sqrt{7})$	3	
$Q(\sqrt{10})$	3	13,37
$Q(\sqrt{11})$	5,7	19

In the definition above we considered the "ray mod p" rather than the "ray mod p" since p is a prime ideal in $Q(\sqrt{d})$ and (p) is not.

However, in the next two sections we will work exclusively with $|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^*|$. Thus in this section we must establish the relationship between $|\mathcal{J}_p^*/\mathcal{J}_p^1|$ and $|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1|$. Also included is the relationship to $|\mathcal{J}_p^*/\mathcal{J}_{p\infty_1}^1|$. First however we need some facts about units.

Proposition 4: If x is even or $N(\epsilon) = +1$ then $(\epsilon^x \equiv 1 \bmod \mathfrak{p} \Leftrightarrow \epsilon^x \equiv 1 \bmod \mathfrak{p}')$ and $(\epsilon^x \equiv -1 \bmod \mathfrak{p} \Leftrightarrow \epsilon^x \equiv -1 \bmod \mathfrak{p}')$. If x is odd and $N(\epsilon) = -1$ then $(\epsilon^x \equiv 1 \bmod \mathfrak{p} \Leftrightarrow \epsilon^x \equiv -1 \bmod \mathfrak{p}')$.

Proof: $\epsilon^x \equiv 1 \bmod \mathfrak{p} \Leftrightarrow (\epsilon')^x \equiv 1 \bmod \mathfrak{p}' \Leftrightarrow (\epsilon'.\epsilon)^x \equiv \epsilon^x \bmod \mathfrak{p}' \Leftrightarrow \epsilon^x \equiv (N(\epsilon))^x \bmod \mathfrak{p}'$. //

Remark: If $\epsilon^x \equiv 1 \bmod \mathfrak{p}$ and if x is even or $N(\epsilon) = +1$, then x cannot be smaller than $x_{1,p}$ ($x_{1,p}$ is the lowest power of ϵ congruent to 1 mod p) since $\epsilon^x \equiv 1 \bmod \mathfrak{p}$ and $\epsilon^x \equiv 1 \bmod \mathfrak{p}' \Rightarrow \epsilon^x \equiv 1 \bmod p$. Similarly if $\epsilon^x \equiv -1 \bmod \mathfrak{p}$, x cannot be smaller than the lowest power of ϵ congruent to $-1 \bmod p$.

Proposition 5: If $y = 2w$ is the lowest even power of ϵ such that $\epsilon^y \equiv -1 \bmod p$ then $\epsilon^y \equiv -1 \bmod \mathfrak{p}$ and y is the lowest such power.

Proof: Suppose $\epsilon^z \equiv -1 \bmod \mathfrak{p}$ with $z < y$ and z is the lowest such power with these properties. Then z must be odd by Proposition 4. (Since if z is even then $\epsilon^z \equiv -1 \bmod \mathfrak{p}'$ and $\epsilon^z \equiv -1 \bmod p$) . y is a multiple of z , i.e., $y = 2 \cdot z \cdot k$. Thus $\epsilon^z \equiv -1 \bmod \mathfrak{p} \Rightarrow (\epsilon^z)^{2k} \equiv (-1)^{2k} \bmod \mathfrak{p} \Rightarrow \epsilon^y \equiv 1 \bmod \mathfrak{p}$. Contradiction. //

Relationship between $|\mathcal{J}_p^*/\mathcal{J}_p^1|$ and $|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1|$ in A-fields

Proposition 6: If $N\epsilon = -1$, $[\mathcal{O}^*:\mathcal{O}_p^1] = \frac{1}{2}[\mathcal{O}^*:\mathcal{O}_{p\infty}^1]$.

Proof: Notice that if $\epsilon^z \equiv \pm 1 \bmod p$ then z must be even since $\epsilon^z \equiv \pm 1 \bmod p \Rightarrow (N(\epsilon))^z \equiv 1 \bmod p$. So there are two cases

i) The first power of ϵ congruent to a rational mod p is congruent to 1 mod p and the power is even; and $\epsilon^{\frac{1}{2}x_{1,p}} \equiv 1 \bmod p$ and no lower power has this property. (Here $\frac{1}{2}x_{1,p}$ must be odd, otherwise $\epsilon^{\frac{1}{2}x_{1,p}} \equiv 1 \bmod p$ by Proposition 4, but this contradicts definition of $x_{1,p}$).

ii) An even power of ϵ, say z is congruent to -1 mod p so obviously $\epsilon^z \equiv -1 \bmod p \Rightarrow -\epsilon^z \equiv +1 \bmod p$; however no lower power has this property by Proposition 5. //

Proposition 7: $|\mathcal{J}_p^*/\mathcal{J}_p^1| = |\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1| \,/\, 2(p-1)$.

Proof: $|\mathcal{J}_p^*/\mathcal{J}_p^1| = \dfrac{p(1-(1/p))}{\frac{1}{2}[\mathcal{O}^*:\mathcal{O}_{p\infty}^1]}$ by Proposition 6, but

$$|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1| = \frac{4\cdot p^2(1-(1/p))^2}{[\mathcal{O}^*:\mathcal{O}_{p\infty}^1]} \Rightarrow \frac{|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1|}{4(p-1)^2} = \frac{1}{[\mathcal{O}^*:\mathcal{O}_{p\infty}^1]} \Rightarrow$$

$$|\mathcal{J}_p^*/\mathcal{J}_p^1| = 2(p-1)\cdot\frac{|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1|}{4(p-1)^2} = \frac{|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1|}{2(p-1)} \quad . \qquad //$$

Relationship between $|\mathcal{J}_p^*/\mathcal{J}_p^1|$ and $|\mathcal{J}_p^*/\mathcal{J}_{p\infty_1}^1|$ in A-fields

$$|\mathcal{J}_p^*/\mathcal{J}_{p\infty_1}^1| = |\mathcal{J}_p^*/\mathcal{J}_p^1| \cdot \begin{cases} 2 & \text{for case i in Proposition 6} \\ 1 & \text{for case ii in Proposition 6} \end{cases}.$$

Relationship between $|\mathcal{J}_p^*/\mathcal{J}_p^1|$ and $|\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1|$ in B-fields

Proposition 8: If $N\epsilon = +1$, then

i) $[\mathcal{O}^*:\mathcal{O}^1_{\mathfrak{p}}] = [\mathcal{O}^*:\mathcal{O}^1_{\mathfrak{p}\infty}]$ if $\nexists\, z \ni \epsilon^z \equiv -1 \bmod \mathfrak{p}$

ii) $[\mathcal{O}^*:\mathcal{O}^1_{\mathfrak{p}}] = \frac{1}{2}[\mathcal{O}^*:\mathcal{O}^1_{\mathfrak{p}\infty}]$ if $\exists\, z \ni \epsilon^z \equiv -1 \bmod \mathfrak{p}$.

Proof: i) Suppose $\exists\, x \ni \pm \epsilon^x \equiv 1 \bmod \mathfrak{p}$ and $x < x_{1,\mathfrak{p}}$. Then $N\epsilon = +1 \Rightarrow \pm \epsilon^x \equiv 1 \bmod \mathfrak{p}'$ thus $\pm \epsilon^x \equiv 1 \bmod \mathfrak{p}$. Contradiction.

ii) Obviously $-\epsilon^z \equiv 1 \bmod \mathfrak{p}$. If $\pm \epsilon^w \equiv 1 \bmod \mathfrak{p}$ for $w \le z$ then $\pm \epsilon^w \equiv 1 \bmod \mathfrak{p}' \Rightarrow \pm \epsilon^w \equiv 1 \bmod \mathfrak{p} \Rightarrow w = z$. //

Proposition 9: Case i) $|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}}| = \dfrac{\mathfrak{p}(1-(1/\mathfrak{p}))}{[\mathcal{O}^*:\mathcal{O}^1_{\mathfrak{p}\infty}]} = \dfrac{|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}\infty}|}{4(\mathfrak{p}-1)}$.

Case ii) $|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}}| = \dfrac{|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}\infty}|}{2(\mathfrak{p}-1)}$

Proof: Follows immediately from Proposition 8. //

Relationship between $|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}}|$ and $|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}\infty_1}|$ in B-fields

$$|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}\infty_1}| = |\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}}| \cdot \begin{cases} 2 & \text{for case i) in Proposition 8} \\ 1 & \text{for case ii) in Proposition 8} . \end{cases}$$

§2. Structure of the Class Group; Number of Class Groups of Given Conductor

For the time being we restrict ourselves to normal inert primes, i.e., inert $\mathfrak{p}$ such that $|\mathcal{J}^*_{\mathfrak{p}}/\mathcal{J}^1_{\mathfrak{p}\infty}| = M \cdot (\mathfrak{p}-1)$ where $M = 1$ for A-fields and $M = 2$ for B-fields. We know from Chapter 4 that (1) $\mathcal{J}^1_{\mathfrak{p}\infty} = (\mathfrak{p}-1)\mathcal{J}^1_{\mathfrak{p}\infty}$ for such $\mathfrak{p}$. We also know that $(r)\mathcal{J}^1_{\mathfrak{p}\infty} = (1)\mathcal{J}^1_{\mathfrak{p}\infty}$ is impossible for $1 < r < \mathfrak{p}-1$. Thus if s is a primitive root mod $\mathfrak{p}$ ($\mathfrak{p}$ rational) then $(1)\mathcal{J}^1_{\mathfrak{p}\infty}$, $(s)\mathcal{J}^1_{\mathfrak{p}\infty}, \ldots (s^{(\mathfrak{p}-3)/2})\mathcal{J}^1_{\mathfrak{p}\infty}$ are distinct rays forming a cyclic subgroup of the ray class group. This subgroup has order $(\mathfrak{p}-1)/2$; thus we have a factor of 2 to account for in the case of A-fields and a

factor of 4 in the case of B-fields. We know that (d) ramifies in $Q(\sqrt{d})$; $(d) = (\sqrt{d})^2$.

Proposition 10: $(\sqrt{d})\mathcal{J}^1_{p^\infty} \neq (r)\mathcal{J}^1_{p^\infty}$ for any rational r .

Proof: Suppose we have equality. Then $\sqrt{d} \equiv r \cdot \epsilon^z \bmod p^\infty \Rightarrow -\sqrt{d} \equiv r \cdot (\epsilon')^z \bmod p^\infty \Rightarrow -d \equiv r^2 \cdot (N(\epsilon))^z \bmod p^\infty$. ∞ condition $\Rightarrow N(\epsilon) = -1$ and z odd $\Rightarrow d \equiv r^2 \bmod p$ which contradicts fact that p is inert. //

Since $(p,d) = 1$ $\exists$ k such that $d \equiv s^k \bmod p$. If k is even, say $k = 2x$ we have $d = (s^x)^2 \bmod p$ which contradicts the fact that p is inert. Thus k is odd, say $k = 2x+1$. Thus $(d)\mathcal{J}^1_{p^\infty} = (\sqrt{d})^2 \mathcal{J}^1_{p^\infty} = (s)^{2x+1} \mathcal{J}^1_{p^\infty}$. This implies there is a ray of order p-1 , viz. $(\sqrt{d}/s^x)\mathcal{J}^1_{p^\infty}$. Thus we have accounted for the factor 2 for A-fields and we conclude:

Proposition 11: In A-fields a ray class group mod a normal inert prime has structure Z_{p-1} .

We still have a factor of 2 to account for in the case of B-fields. We claim that there is a subgroup of order 2 generated by $(\pm)\mathcal{J}^1_{p^\infty}$ where $(\pm)$ denotes an element of $Q(\sqrt{d})$ which is $\equiv 1 \bmod p$ and has signature + - . We need to show that $(\pm)\mathcal{J}^1_{p^\infty}$ is not already contained in the main cyclic subgroup. Note that every element in the main cyclic subgroup can be expressed in the form $(\sqrt{d})^L \cdot (r)\mathcal{J}^1_{p^\infty}$ where L is 0 or 1 and r is a rational integer.

Proposition 12: In B-fields $(\pm)\mathcal{J}^1_{p^\infty}$ is not in the main cyclic subgroup.

Proof: Suppose $(\pm)\mathcal{J}^1_{p^\infty} = (\sqrt{d})^L (r)\mathcal{J}^1_{p^\infty}$. Then $\exists\, z \ni (\pm) \equiv \sqrt{d}^L \cdot r \cdot \epsilon^z \bmod p^\infty \Rightarrow (\mp) \equiv (-\sqrt{d})^L \cdot r \cdot (\epsilon')^z \bmod p^\infty \Rightarrow (\mp) \equiv (-d)^L \cdot r^2 \cdot (N(\epsilon))^z \bmod p^\infty$. If $L = 0$, ∞ condition $\Rightarrow N(\epsilon) = -1$, z odd. If $L = 1$, ∞ condition $\Rightarrow N(\epsilon) = +1$

or z even and congruence reduces to $-1 \equiv d \cdot r^2 \bmod p$. But we also have $1 \equiv d \cdot r^2 \cdot \epsilon^{2z} \bmod p \Rightarrow d \equiv (r^{-1} \cdot \epsilon')^2 \bmod p$ which contradicts the fact that p is inert. //

This accounts for the extra factor of 2 in B-fields. We conclude with:

Proposition 13: In B-fields a ray class group mod a normal inert prime has structure $Z_{p-1} \oplus Z_2$.

We now consider the structure of $\mathcal{J}^*_{p^t}/\mathcal{J}^1_{p^{t_\infty}}$ where p is a normal inert prime that does not skip.

Proposition 14: $\mathcal{J}^*_{p^t}/\mathcal{J}^1_{p^{t_\infty}} \cong Z_{(p-1)p^{t-1}}$ for A-fields;

$\cong Z_{(p-1)p^{t-1}} \oplus Z_2$ for B-fields.

Proof: We use the fact that $(Z/(p)^t)^*$ is cyclic for p odd and for all t. Let b be a primitive root mod p^t (p rational). Then we simply repeat the above arguments with b replacing s, the primitive root mod p. In this way we creat p^{t-1} times as many distinct rays since $(r)\mathcal{J}^1_{p^{t_\infty}} = (1)\mathcal{J}^1_{p^{t_\infty}}$ implies $r \equiv \pm 1 \bmod p^t$. Thus by the equivalence lemma the newly created rays are distinct. //

Let us now consider subgroups of $\mathcal{J}^*_{p^t}/\mathcal{J}^1_{p^{t_\infty}}$. Proposition 14 tells us the ray class group has the form $Z_{(p-1)p^{t-1}}$ in A-fields. Since this is a cyclic group there is exactly one subgroup of order x for each x dividing $(p-1)p^{t-1}$. As is conventional let $\tau(y)$ be defined as the number of positive divisors of y. Then $Z_{(p-1)p^{t-1}}$ has $t \cdot \tau(p-1)$ subgroups. All of these subgroups are explained by a

lower modulus except the congruence subgroups of orders 1, $u_2, u_3 \cdots u_{\tau(p-1)} = p-1$ where the u_i are the positive divisors of $p-1$. Thus we have

Proposition 15: There are $\tau(p-1) - \delta_{1t}$ class groups with $\mathfrak{f}^* = (p)^t$, t in Z^+, for (p) a normal inert non-skipping prime in an A-field. The corresponding class fields have degrees $p^{t-1}, p^{t-1}u_2, \ldots, p^{t-1}(p-1)$ over k. Here, $\mathfrak{f}^*$ is defined as the finite part of the conductor $\mathfrak{f}$. //

In B-fields, the ray class group has the form $Z_{(p-1)\cdot p^{t-1}} \oplus Z_2$. By applying Carmichael's method for counting subgroups of various orders, we see that the number of subgroups of index $1, u_2, \ldots, u_i, \ldots p, 2(p-1), \ldots 2(p-1)p^{t-1}$ (where the u_i are the positive divisors of $2(p-1)$) is the same for $Z_{(p-1)p^{t-1}} \oplus Z_2$ and $Z_{(p-1)p^t} \oplus Z_2$. Thus our counting problem is reduced to analyzing the subgroup pattern of $Z_{p-1} \oplus Z_2$. Let M be the number of odd divisors of $p-1$. Then the number of subgroups of $Z_{p-1} \oplus Z_2$ is $2M+3(\tau(2(p-1)) - 2M) = 3\tau(2(p-1)) - 4M$.

Proposition 16: If p is a normal inert non-skipping prime in a B-field there are $3\tau(2(p-1)) - 4M - \delta_{1t}$ class groups with $\mathfrak{f}^* = (p)^t$, t in Z^+. The corresponding class fields have degrees $p^{t-1}, p^{t-1}u_2, \ldots p^{t-1}\cdot 2(p-1)$ over k; there being 3 such class fields for each degree unless u_i or $2(p-1)/u_i$ is odd in which case there is only 1.

Let us now consider the structure of $\mathcal{J}_p^*/\mathcal{J}_{p^\infty}^1$ for normal splitting primes p. For such p in an A-field $x_{1,p} = p-1$, in B-fields $x_{1,p} = \frac{1}{2}(p-1)$ for Case i) of previous section, $x_{1,p} = p-1$ for Case ii)

of previous section. We know that $\mathfrak{O}/(p) = \mathfrak{O}/\mathfrak{p} \times \mathfrak{O}/\mathfrak{p}' \cong Z_p \oplus Z_p$. Also if $x = (a,b)$, $x' = (b,a)$ where $x \in \mathfrak{O}$. Thus (a,b) is a unit mod p only if $ab \equiv \pm 1 \bmod p$. The rationals mod p are imbedded as (r,r) . There are exactly $2(p-1)$ elements of $Z_p \oplus Z_p$ which satisfy $ab \equiv \pm 1$ mod p but the cyclic group generated by the fundamental unit of a particular field will comprise at most $p-1$ of these.

Lemma 4: If A-fields $x_{1,p} = p-1$ implies i) if $p \equiv 1 \bmod 4$ $\exists$ $z \ni$ $\epsilon^z \equiv -1 \bmod p$ and ii) if $p \equiv 3 \bmod 4$ $\nexists$ $z \ni \epsilon^z \equiv -1 \bmod p$.

Proof: If $p \equiv 1 \bmod 4$ let $\epsilon^{x_{1,p}/2} = (a,b)$. We know $ab \equiv 1 \bmod p$ since $x_{1,p}/2 = (p-1)/2$ is even. Also we have $a^2 \equiv b^2 \equiv 1 \bmod p$. Thus $(a,b) = (-1,-1)$ and since $(-1,-1)$ is identified with -1 we have $\epsilon^{x_{1,p}/2} \equiv -1 \bmod p$. If $p \equiv 3 \bmod 4$, $\epsilon^z \equiv -1 \bmod p$ implies z odd which contradicts Lemma 1 of Section 1. //

Proposition 17: $(\sqrt{d})\mathcal{J}^1_{p^\infty} = (r)\mathcal{J}^1_{p^\infty}$ for some rational $r \Leftrightarrow p \equiv 3 \bmod 4$ and $N(\epsilon) = -1$.

Proof: From the proof of Proposition 1 we see $-d \equiv r^2 \cdot (N(\epsilon))^z \bmod p^\infty$. ∞ condition implies $N(\epsilon) = -1$ and z odd. But $\sqrt{d} \equiv r \cdot \epsilon^z \bmod p^\infty$ implies $d \equiv r^2 \cdot \epsilon^{2z} \bmod p^\infty$ which implies $\epsilon^{2z} \equiv 1 \bmod p^\infty$. But z odd and $\epsilon^{2z} \equiv 1 \bmod p^\infty$ implies $p \equiv 3 \bmod 4$. //

Proposition 18: $(\pm)\mathcal{J}^1_{p^\infty} \neq (\sqrt{d})^L (r)\mathcal{J}^1_{p^\infty}$ in A-fields where $p \equiv 3 \bmod 4$ and in Case i B-fields. (Here $L = 0$ or 1 and r is rational).

Proof: Suppose we have equality. From the proof of Proposition 12 we see that if $L = 0$, ∞ condition implies $N(\epsilon) = -1$, z odd and congruence reduces to $r^2 \equiv -1 \bmod p$. But $(\pm) \equiv r \cdot \epsilon^z \bmod p^\infty$ implies $r^2 \cdot \epsilon^{2z} \equiv 1 \bmod p \Rightarrow \epsilon^{2z} \equiv -1 \bmod p \Rightarrow p \equiv 1 \bmod 4$ and $\epsilon^z \equiv \pm r^{-1} \bmod p$.

(Note this type of prime is $\equiv 5 \bmod 8$). If $L = 1$ ∞ condition $\Rightarrow$ $N(\epsilon) = +1$ or z even and congruence reduces to $-1 \equiv d \cdot r^2 \bmod p$ but we also have $1 \equiv d \cdot r^2 \cdot \epsilon^{2z} \bmod p$ which implies $\epsilon^{2z} \equiv -1 \bmod p$. If $N(\epsilon) = +1$, this condition defines a Case ii B-field. If $N(\epsilon) = -1$, then since z is even we obtain $p \equiv 1 \bmod 8$. //

We now have generators for 1 of the 2 types of class groups which occur for normal splitting primes in A-fields, and similarly for B-fields.

Proposition 19: For normal splitting primes in A-fields, $\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1$ has structure $Z_{p-1} \oplus Z_2$ if $p \equiv 3 \bmod 4$.

Proof: Using the Equivalence Lemma and Propositions 14 and 15 we obtain $\{(1)(2) \ldots (p-1)\} \times \{(1)(\pm)\}$. //

Proposition 20: For normal splitting primes in B-fields, $\mathcal{J}_p^*/\mathcal{J}_{p\infty}^1$ has structure $Z_{p-1} \oplus Z_2 \oplus Z_2$ if $\nexists\, z \ni \epsilon^z \equiv -1 \bmod p$ (Case i B-field).

Proof: Using Propositions 15 and 16 we have $\{(1) \ldots (p-1)\} \times \{(1)(\sqrt{d}/t)\} \times \{(1)(\pm)\}$ where $t^2 \equiv d \bmod p$. //

We now try to find the missing generator for the one type of A and B-fields not covered by the above propositions. We would like to find an ideal (α) which is not generated by $(\sqrt{d})(r)$, r rational, but whose square is so generated. We consider the easier case of B-fields first. Let s be a primitive root mod p, p rational. Then we claim (s^{p-2}, s) is a unit mod (p) if $N\epsilon = +1$ and $x_{1,p} = p-1$. Certainly $s^{p-2} \cdot s \equiv 1 \bmod p$ and when $N\epsilon = +1$ and $x_{1,p} = p-1$ this characterizes the units since there are exactly $p-1$ elements (a,b) satisfying $ab \equiv 1 \bmod p$. Notice that $(1,s) = (s^{p-2}, s)(s,1)$ and we have

$(s,s) = (1,s)(s,1) = (s,1)^2(s^{p-2},s)$. Since s is identified with the rational s we have for Case ii B-fields $(s)\mathcal{J}^1_{p^\infty} = ((s,1))^2\,\mathcal{J}^1_{p^\infty}$.

Proposition 21: $((s,1))\mathcal{J}^1_{p^\infty} \neq (\sqrt{d})^L(r)\mathcal{J}^1_{p^\infty}$ in B-fields.

Proof: Suppose we have equality. Then squaring we get $(s)\mathcal{J}^1_{p^\infty} = (d)^L(r)^2\,\mathcal{J}^1_{p^\infty}$ which implies $s \equiv d^L \cdot r^2 \cdot \epsilon^z \bmod p$. Taking norms we get $s^2 \equiv d^{2L} \cdot r^4 \bmod p$. Since $d \equiv t^2 \bmod p$ for some rational t we get $s^2 \equiv r^4 \bmod p$ or $s^2 = (tr)^4 \bmod p$ depending on whether $L = 0$ or 1. Either congruence contradicts the fact that s is a primitive root mod p . //

Proposition 22: For normal splitting primes in B-fields where $\exists\ z \ni \epsilon^z \equiv -1 \bmod p$, $\mathcal{J}^*_p/\mathcal{J}^1_{p^\infty}$ has structure $Z_{p-1} \oplus Z_2$.

Proof: Using Propositions 15 and 19 we get $\{(1)((s,1))(s)((s,1))^3 \ldots ((p-1)/2)\} \times \{(1)(\sqrt{d}/t)\}$. //

We now show that $((s,1))$ also serves as the "missing generator" for A-fields where $p \equiv 1 \bmod 4$.

Proposition 23: $((s,1))\mathcal{J}^1_{p^\infty} \neq (\sqrt{d})^L(r)\mathcal{J}^1_{p^\infty}$ in A-fields when $p \equiv 1 \bmod 4$.

Proof: Suppose we have equality. Then $(s,1) \equiv \sqrt{d}^L \cdot r \cdot \epsilon^z \bmod p^\infty$. Taking norms we get $(s,s) \equiv s \equiv (-d)^L \cdot r^2 \cdot (-1)^z \bmod p$. Since -1 and d are squares of rationals, this congruence contradicts the fact that s is a primitive root mod p . //

Proposition 24: $((s,1))^2\,\mathcal{J}^1_{p^\infty} = (s)(\sqrt{d}/t)\,\mathcal{J}^1_{p^\infty}$ where $d \equiv t^2 \bmod p$, t rational.

Proof: We claim that $\sqrt{d}/t = (1,-1)$. Let $\sqrt{d} = (a,b)$. Then squaring we get $d = (a^2,b^2)$. Taking norms we get $-d = (ab,ab)$. Consider

$\sqrt{d}/t = (a/t, b/t)$. Since $(a/t)^2 \equiv (b/t)^2 \equiv 1 \bmod p$ and $ab/t^2 \equiv -1 \bmod p$ we see $(a/t, b/t) = (1,-1)$. One easily checks that $(s,1)^2 = (s,s)(1,-1)(s,-s^{p-2})$ and $(s,-s^{p-2})$ is a unit since it is not a square and its norm is -1 . (In A-fields when $x_{1,p} = p-1$ the units are all elements with norm 1 which are squares and all elements with norm -1 which are not squares). //

Proposition 25: For normal splitting primes in A-fields where $p \equiv 1 \bmod 4$, $\mathcal{J}_p^*/\mathcal{J}_{p^\infty}^1$ has structure $Z_{p-1} \oplus Z_2$.

Proof: $((s,1))$ has order $p-1$ since (s) has order $(p-1)/2$ and $(\sqrt{d}/t)$ has order 2 . Thus we have $\{(1)((s,1))(s)(\sqrt{d}/t) \ldots ((p-1)/2)(\sqrt{d}/t)\} \times \{(1)(\sqrt{d}/t)\}$. //

We now consider the structure of $\mathcal{J}_{p^t}^*/\mathcal{J}_{p^{t_\infty}}^1$ where p is a normal splitting prime that does not skip, i.e., $x_{K,p} = p \cdot x_{K-1,p}$ $\forall$ K .

Proposition 26: $\mathcal{J}_{p^t}^*/\mathcal{J}_{p^{t_\infty}}^1 \cong Z_{(p-1)p^{t-1}} \oplus Z_2$ in A-fields or in Case ii B-fields.

$\cong Z_{(p-1)p^{t-1}} \oplus Z_2 \oplus Z_2$ in Case i B-fields .

Proof: See proof of Proposition 14. //

Let us now consider subgroups of $\mathcal{J}_{p^t}^*/\mathcal{J}_{p^{t_\infty}}^1$. For A-fields or Case ii B-fields we have already described the results in Proposition 16.

Proposition 27: If p is a normal splitting non-skipping prime in an A-field or a Case ii B-field there are $3\tau(2(p-1)) - 4M - \delta_{1t}$ class groups with $\mathfrak{f}^* = (p)^t$, t in Z^+. The corresponding class fields have degrees

p^{t-1} , $p^{t-1}u_2,\ldots,p^{t-1}\cdot 2(p-1)$ over K ; there being 3 such class fields for each degree unless u_i or $2(p-1)/u_i$ is odd in which case there is only 1 . //

For Case i B-fields we again use Carmichael's method and reduce the problem to analyzing the structure of $Z_{p-1} \oplus Z_2 \oplus Z_2$. If u_i or $4(p-1)/u_i$ is an odd divisor of $4(p-1)$ (we call these type 1 divisors) then there is only 1 subgroup of order u_i . Let M be the number of type 1 divisors. If $2\|u_i$ or $2\|4(p-1)/u_i$ (we call these type 2 divisors) then there are exactly 7 subgroups of order u_i . Let N be the number of type 2 divisors. In all other cases (i.e., $4|u_i$ and $4|4(p-1)/u_i$) there are exactly 11 subgroups of order u_i .

Proposition 28: If p is a normal splitting non-skipping prime in a Case i B-field there are $11(\tau(4(p-1)) - (M+N)) + M + 7\cdot N - \delta_{1t} = 11\cdot\tau(4(p-1)) - 10M - 4N - \delta_{1t}$ class groups with $\mathfrak{f}^* = (p)^t$, t in Z^+. The corresponding class fields have degrees p^{t-1}, $p^{t-1}u_2,\ldots,p^{t-1}\cdot 4(p-1)$ over K ; there being 11 such class fields of each degree unless u_i is a type 1 divisor in which case there is only 1 or a type 2 divisor in which case there are 7 . //

We remind the reader that most of our investigations have dealt with a restrictive class of primes; i.e., normal primes that do not skip. There are obviously at least three problems that need further study : finding the structure of the ray class group for special prime, skipping prime and "non-prime" moduli. We enclose "non-prime" in quotes since the ideal (p) where p is a splitting prime of Q is obviously not a prime ideal of $Q(\sqrt{d})$. We chose to study class groups of conductor $(p)^t$ rather than p^t since for normal p , $|\mathcal{I}^*_{p^t}/\mathcal{I}^1_{p^t}| = 1$. However,

it would certainly be worthwhile to study class groups of conductor $\mathfrak{p}^t$ where $\mathfrak{p}$ is not normal and from there to study all possible moduli.

§3. A Connection to Quadratic Forms

We need the following definitions and facts which are taken from Cohn [4], p. 3.23. View the ring of integers of a quadratic field as a $\mathbb{Z}$-module; $\mathcal{O} = [1,\omega]$.

Definition: A quadratic ring R is a ring of the form $R = [1,f\omega]$ where $f \in \mathbb{Z}^+$.

Fact: $R = \{\alpha \mid \alpha \in \mathcal{O}$ and $\alpha \equiv r \bmod f$, $r \in \mathbb{Z}\}$.

Definition: $R^\infty \equiv \{\alpha \mid \alpha \in \mathcal{O}$ and $\alpha \equiv r \bmod f^\infty$, $r \in \mathbb{Z}\}$.

Definition: A ring ideal group mod R , $\mathcal{J}_R^1$ is defined by

$$\mathcal{J}_R^1 = \{(\alpha/\beta) \mid \alpha,\beta \in R\}$$

A ring ideal group mod R^∞ ,

$$\mathcal{J}_{R^\infty}^1 = \{(\alpha/\beta) \mid \alpha,\beta \in R^\infty\} .$$

Fact: $\mathcal{J}_f^1 \subseteq \mathcal{J}_R^1 \subseteq \mathcal{J}_f$; $\mathcal{J}_{f^\infty}^1 \subseteq \mathcal{J}_{R^\infty}^1 \subseteq \mathcal{J}_f^1$.

Definition: $H_R \equiv \mathcal{J}_f/\mathcal{J}_R^1$; $H_{R^\infty} \equiv \mathcal{J}_f/\mathcal{J}_{R^\infty}^1$.

R is uniquely determined by its discriminant

$$\begin{vmatrix} 1 & f\omega \\ 1 & f\omega' \end{vmatrix}^2 = f^2 \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = f^2 d \quad .$$

Hence H_R and H_{R^∞} are usually labelled $H(f^2d)$, $H^+(f^2d)$ with orders $h(f^2d)$, $h^+(f^2d)$ respectively, It can be shown that H_R and H_{R^∞} are nothing but the class groups of quadratic forms under weak and strict equivalence, respectively, and thus $h(f^2d)$, $h^+(f^2d)$ are the corresponding

class numbers.

Using the following formula from Cohn [4], p. 3.27 we will calculate $h^+(p^{2t}d)/h^+(d)$ for various types of primes p .

$$\frac{h^+(f^2d)}{h^+(d)} = \frac{\prod_{p|f} (1 - ((d/p)_2/p))\, u^+(f)}{[\mathcal{O}_\infty^* : \mathcal{O}_{f\infty}^*]}$$

where $u^+(f) = \text{card}\{r \mid 0 \le r < f\ ,\ r \text{ in } Z\ ;\ r \equiv \omega \bmod f^\infty\ ,\ \omega \in \mathcal{O}_\infty^*\}$.

Case I: $f = p^t$ where p is a normal, non-skipping inert prime. Recall that for normal, non-skipping inert primes :

$$[\mathcal{O}^* : \mathcal{O}^*_{p^t\infty}] = p^{t-1}(p+1) \cdot \begin{cases} 4 & \text{in A-fields} \\ 2 & \text{in B-fields} \end{cases} .$$

Since $[\mathcal{O}_\infty^* : \mathcal{O}^*_{p^t\infty}] = [\mathcal{O}^* : \mathcal{O}^*_{p^t\infty}] \cdot \begin{cases} \frac{1}{4} & \text{in A-fields} \\ \frac{1}{2} & \text{in B-fields} \end{cases}$ we have

$$\frac{h^+(p^{2t}d)}{h^+(d)} = u^+(p^t) = u^+(p) = 2 .$$

Case II: $f = p^t$ where p is a normal, non-skipping, splitting prime. Recall that for normal, non-skipping, splitting primes :

$$[\mathcal{O}^* : \mathcal{O}^*_{p^t\infty}] = 2p^{t-1}(p-1) \cdot \begin{cases} 1 & \text{in A-fields, or B-fields where } \exists\ z \ni \epsilon^z \equiv -1 \bmod p \\ \frac{1}{2} & \text{in B-fields, where } \nexists\ z \ni \epsilon^z \equiv -1 \bmod p . \end{cases}$$

Thus we have $\dfrac{h^+(p^{2t}d)}{h^+(d)} = u^+(p^t) \cdot \begin{cases} 2 & \text{in A-fields, or in B-fields where } \nexists\ z \ni \epsilon^z \equiv -1 \bmod p \\ 1 & \text{in B-fields where } \exists\ z \ni \epsilon^z \equiv -1 \bmod p . \end{cases}$

Using Lemma 4, we see

$$\frac{h^+(p^{2t}d)}{h^+(d)} = \begin{cases} 4 & \text{in A-fields if } p \equiv 1 \bmod 4 \\ 2 & \text{in A-fields if } p \equiv 3 \bmod 4 \text{ or, in all B-fields.} \end{cases}$$

BIBLIOGRAPHY

[1] Borevich, Z.I. and Shafarevich, I.R. Number Theory, Academic Press, New York, 1966.

[2] Carmichael, Robert D. Introduction to the Theory of Groups of Finite Order, Dover, New York, 1956.

[3] Cohn, Harvey. A Second Course in Number Theory, Wiley & Sons, New York, 1962.

[4] Cohn, Harvey. Unpublished Lecture Notes on Class Field Theory; 1973-74.

[5] Dickson, L.E. History of the Theory of Numbers, vol. I, Chelsea, New York, 1952.

[6] Gauss, Carl Friedrich. Disquisitiones Arithmeticae, Yale Press, New Haven, Connecticut, 1966.

[7] Goldstein, Larry Joel. Analytic Number Theory, Prentice-Hall, Englewood Cliffs, New Jersey, 1971.

[8] Hardy, G.H. and Wright, E.M. An Introduction to the Theory of Numbers, 4th ed., Oxford University Press, London, England, 1971.

[9] Hasse, Helmut. Uber die Klassenzahl Abelscher Zahlkorper, Akademie-Verlag, Berlin, Germany, 1952.

[10] Hilbert, David. Gesammelte Abhandlungen, vol. I., Chelsea, New York, 1965.

[11] Holzer, Ludwig. Klasskorpertheorie, B.G. Teubner, Leipzig, Germany, 1966.

[12] Janusz, Gerald J. Algebraic Number Fields, Academic Press, New York, 1973.

[13] Lang, Serge. Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.

[14] Niven, Ivan and Zuckerman, Herbert S. An Introduction to the Theory of Numbers, 3rd ed., Wiley & Sons, New York, 1972.

[15] Ribenboim, Paulo. Algebraic Numbers, Wiley-Interscience, New York, 1972.

AUTOBIOGRAPHICAL STATEMENT

Paul Barry Massell was born in Boston, Massachusetts on June 26, 1948. He lived there until he was seven; he then moved to Akron, Ohio and later to Toledo, Ohio. He went to Oak Park and River Forest High School in Oak Park, Illinois for three years and graduated from Hammond High School in Alexandria, Virginia. He received a B.A. in mathematics from the University of Chicago in 1970. From 1971 to 1974 he taught mathematics at Brooklyn College while attending the Graduate Center of The City University of New York.