Densities of 4-Ranks of K(2) of Rings of Integers.

Robert Burke Osburn
Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation
https://digitalcommons.lsu.edu/gradschool_disstheses/304

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
DENSITIES OF 4-RANKS OF $K_2$ OF RINGS OF INTEGERS

A Dissertation
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in
The Department of Mathematics

by
Robert B. Osburn
B.S., Louisiana State University, 1996
M.S., Louisiana State University, 1998
May 2001

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Acknowledgments

I would like to thank my advisor, Dr. Jurgen Hurrelbrink, for his constant patience and support during this work and Dr. P.E. Conner for his help and advice. I also wish to thank my committee members, Professors Hui-Hsiung Kuo, Bogdan Oporowski, Robert Perlis, Lawrence Smolinsky, and Suresh Rai.

I am especially grateful for the computational help of Brian Murray and the graduate students who listened to me. I would like to thank both of my families for their encouragement and love.

This work is dedicated to my wife, Amy Masner. This simply would not have happened without her.
# Table of Contents

Acknowledgments ................................................................................................ ii

Abstract ................................................................................................................ iv

Introduction ........................................................................................................... 1

1. Background ........................................................................................................ 7  
   1.1 Tools ........................................................................................................... 7  
   1.2 Densities ..................................................................................................... 19

2. $K_2(\mathcal{O})$ ................................................................................................... 23

3. Main Results ....................................................................................................... 39  
   3.1 Overview ..................................................................................................... 39  
   3.2 First Extension ........................................................................................ 39  
   3.3 Second Extension ..................................................................................... 44  
   3.4 Third Extension ........................................................................................ 52  
   3.5 The Composite ........................................................................................ 53  
   3.6 The Cases $\mathbb{Q}(\sqrt{p_{l}})$ and $\mathbb{Q}(\sqrt{2pl})$ ......................................................... 61  
   3.7 The Cases $\mathbb{Q}(\sqrt{-p_{l}})$ and $\mathbb{Q}(\sqrt{-2pl})$ ......................................................... 65

References ................................................................................................................. 70

Appendix 1: Possible Densities ............................................................................. 74

Appendix 2: The Program .................................................................................... 82

Vita ............................................................................................................................. 99
Abstract

In [7], the authors established a method of determining the structure of the 2-Sylow subgroup of the tame kernel $K_2(\mathcal{O})$ for certain quadratic number fields. Specifically, the 4-rank for these fields was characterized in terms of positive definite binary quadratic forms. Numerical calculations led to questions concerning possible density results of the 4-rank of tame kernels. In this thesis, we succeed in giving affirmative answers to these questions.
Introduction

In 1637, Pierre de Fermat claimed the equation

\[ x^n + y^n = z^n \]

had no nonzero integral solutions for \( n > 2 \). The search for a proof of this claim has inspired mathematicians and greatly contributed to the development of number theory. To understand this development, let us briefly retrace part of this search.

For \( n = 3 \), Euler gave an incomplete proof in 1770 which was later completed without difficulty. Gauss gave another proof using properties of the number field \( \mathbb{Q}(\sqrt{-3}) \). Fermat himself proved the \( n = 4 \) case using the method of infinite descent. In 1825 Dirichlet attempted to prove the \( n = 5 \) case, but as Legendre noted the proof was incomplete. Dirichlet completed his proof in 1828. The next case of interest was \( n = 7 \). Lame handled it in 1839. He then presented in 1847 what he thought was a solution for all \( n \). The difficulty with Lamé's approach, as Liouville noted, was that he assumed the property that the "integers" of the cyclotomic field \( \mathbb{Q}(\zeta_p) \), \( p \) an odd prime, have unique factorization into irreducible elements. Kummer actually knew in 1844 that unique factorization need not hold for \( \mathbb{Q}(\zeta_p) \) (e.g. \( p = 23 \)). Once he realized this, he pursued concepts which would "save" unique factorization. We note that Lamé's difficulty is more generally due to the fact that one may not have unique prime element decomposition in the ring...
of integers for a given number field. In a letter from Kummer to Liouville in 1847, he states [48] "it is possible to rescue it [Fermat's Last Theorem], by introducing a new kind of complex numbers, which I have called ideal complex number."

This idea of "ideal complex numbers" matches the modern term "ideal", a notion introduced by Dedekind, see discussion in [58]. Dedekind [12] and Hilbert [24] separately "restored" unique factorization by proving that an ideal in the ring of integers of an algebraic number field can be factored uniquely as a product of prime ideals. So we have unique prime ideal decomposition. How close are we from unique prime element decomposition? How can we "measure" such a difference? In order to do this, we introduce for any number field $\mathbb{F}$ and its ring of integers $\mathcal{O}_F$, the ideal class group of $\mathbb{F}$, denoted $\text{C}(\mathbb{F})$.

Let $J$ be the group of nonzero fractional $\mathcal{O}_F$-ideals and $H$ the subgroup of nonzero principal fractional $\mathcal{O}_F$-ideals. Then $\text{C}(\mathbb{F})$ is the quotient group $J/H$. $\text{C}(\mathbb{F})$ is trivial if and only if $\mathcal{O}_F$ is a principal ideal domain (PID) and thus we have unique prime element decomposition. For any number field $\mathbb{F}$, $\text{C}(\mathbb{F})$ is a finite abelian group. The number of elements in $\text{C}(\mathbb{F})$ is the class number of $\mathbb{F}$, denoted $h(\mathbb{F})$. It is a classical problem to investigate the structure and order of the ideal class group.

Gauss knew for $d < 0$ and squarefree that there are at least nine fields $\mathbb{Q} (\sqrt{d})$ with class number 1. Heilbronn and Linfoot [23] in 1934 showed that the class number is 1 for at most one more such $d$. It was finally proved that there are only nine such fields with class number 1, first by Heegner [22] in 1952, then independently by Baker [1] and Stark [51] in 1966. All number fields with class number 2 were characterized by Carlitz [6].

To understand the structure of the ideal class group for a quadratic number field, it is important to determine the structure of its 2-Sylow subgroup. As the ideal class group $\text{C}(\mathbb{F})$ of $\mathbb{F}$ is a finite abelian group, it is a product of cyclic groups
of prime power order. The **2-rank** of $C(F)$ is the number of cyclic factors of order divisible by 2. Similarly, the **4-rank** of $C(F)$ is the number of cyclic factors of order divisible by 4. We note that these notions of 2-rank and 4-rank hold for any finite abelian group. Using quadratic forms, Gauss proved that the 2-rank of the (narrow) ideal class group of $F$ is $t - 1$ where $t$ is the number of distinct prime divisors of the discriminant of $F$. As a consequence, the 2-rank of $C(F)$ equals $t - 2$ if $F$ is real quadratic and $-1$ is not a norm from $F$, and $t - 1$ otherwise.

Much work has been done concerning 4-ranks of (narrow) ideal class groups. In the 1930's, Redei and Reichardt proved several important results in terms of ranks of matrices over $F_2$, see [42], [43], [44], [45], [46], and [47]. Recent work has also been done by Lagarias [32] and Gerth [17], [18], and [19]. At LSU, results have been obtained by Conner and Hurrelbrink. Now we could ask "how often" do specific 2-ranks occur for certain quadratic number fields? Similarly, "how often" do specific 4-ranks occur for certain quadratic number fields? In order to discuss these questions further, we introduce the concept of units in rings of integers.

For a number field $F$ and its ring of integers $O_F$, the **units** of $O_F$ are the elements $u \in O_F$ such that there exists $x \in O_F$ with $ux = 1$. The units form a multiplicative group, denoted $O_F^*$. Consider the quadratic number field $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, squarefree, and its ring of integers $O_F$. For an imaginary quadratic number field $F$, we have

**Proposition 0.1.** *If $d < 0$ and squarefree, then*

(i) For $d = -1$, $O_F^* = \{\pm 1, \pm i\}$

(ii) For $d = -3$, $O_F^* = \{\pm 1, \pm \omega, \pm \omega^2\}$ where $\omega = \frac{-1 + \sqrt{-3}}{2}$.

(iii) For $d < -3$ or $d = -2$, $O_F^* = \{\pm 1\}$

Determining $O_F^*$ in the case of a real quadratic field $F$ relies on the fact that
the Pell equation

\[ x^2 - dy^2 = \pm 1 \]

has a solution in nonzero integers \( x, y \). Using this result, one obtains

**Proposition 0.2.** If \( \mathcal{O}_F \) is the ring of integers in \( F = \mathbb{Q}(\sqrt{d}) \), \( d > 0 \) and square-free, then there exists a unit \( \epsilon > 1 \) such that every unit of \( \mathcal{O}_F \) is of the form \( \pm \epsilon^m \), \( m \in \mathbb{Z} \).

The unique unit \( \epsilon \) is called the **fundamental unit** of \( \mathbb{Q}(\sqrt{d}) \). For a real quadratic field \( F \), Dirichlet related the class number \( h(F) \) and the fundamental unit of \( F \). Propositions 0.1 and 0.2 are very special cases of Dirichlet’s Unit Theorem which gives the structure of the group of units in a number field.

Let us now return to the previously asked questions: What about “densities” and 2-ranks of ideal class groups? Morton [38] has proven density results relating 2-ranks and the fundamental unit of certain quadratic number fields. Now what about “densities” and 4-ranks of ideal class groups? For motivation let us consider the following example.

**Example 0.3.** Let \( p \) be a prime. The structure of the 2-Sylow subgroup of the ideal class group of the real quadratic fields \( \mathbb{Q}(\sqrt{2p}) \) is given by:

\[
\begin{align*}
\text{For } p = 2 & : \{1\} \\
\text{For } p \equiv 3, 7 \mod 8 & : \{1\} \\
\text{For } p \equiv 1 \mod 8 & : C_2 \text{ if } p \neq x^2 + 32y^2 \text{ for all } x, y \in \mathbb{Z} \\
& : C_{2^j} \text{ with } j \geq 2 \text{ if } p = x^2 + 32y^2 \text{ for some } x, y \in \mathbb{Z} \\
\text{For } p \equiv 5 \mod 8 & : C_2.
\end{align*}
\]

By Theorem 21.6 in [9], the sets \( \{p \equiv 1 \mod 8 : p \neq x^2 + 32y^2 \ \forall x, y \in \mathbb{Z}\} \) and \( \{p \equiv 1 \mod 8 : p = x^2 + 32y^2 \text{ for some } x, y \in \mathbb{Z}\} \) each have a density \( \frac{1}{2} \) in
the set of primes \( p \equiv 1 \mod 8 \). By Dirichlet's Theorem on primes in arithmetic progressions, the subsets

\[
\{ p : \text{the ideal class group of } \mathbb{Q}(\sqrt{2p}) \text{ has 4-rank 0} \}
\]

\[
\{ p : \text{the ideal class group of } \mathbb{Q}(\sqrt{2p}) \text{ has 4-rank 1} \}
\]

have densities \( \frac{1}{4} + \frac{1}{8} + \frac{1}{4} = \frac{7}{8} \) and \( \frac{1}{8} \) respectively in the set of all primes \( p \).

To motivate further let us consider real quadratic number fields \( F = \mathbb{Q}(\sqrt{D}) \) whose discriminants \( D \) have no prime divisors congruent to 3 modulo 4. We can associate to the fields \( \mathbb{Q}(\sqrt{D}) \) a certain graph. The density of the set of graphs corresponding to these fields with 4-rank \( C(F) = 0 \) is approximately 41.9\%. This result is related to work dating back to Redei and more recently by Conner and Hurrelbrink [27]. Conjectures involving these fields \( F \) and densities can also be found in [52]. Let us now consider a natural analog of the density questions concerning ideal class groups and groups of units of rings of integers.

In the 1960's and 1970's, relationships between algebraic K-theory and number theory were intensely studied. For number fields \( F \) and their rings of integers \( \mathcal{O}_F \), the K-groups \( K_0(\mathcal{O}_F), K_1(\mathcal{O}_F), K_2(\mathcal{O}_F), \ldots \) were a main focus of attention. From [37] we have

\[
K_0(\mathcal{O}_F) \cong \mathbb{Z} \times C(F)
\]

where \( C(F) \) is the ideal class group of \( F \), and

\[
K_1(\mathcal{O}_F) \cong \mathcal{O}_F^*,
\]

the group of units of \( \mathcal{O}_F \).

For the group \( K_2(\mathcal{O}_F) \), no general structure theorem yet exists. What can we
say in general about $K_2(\mathcal{O}_F)$? Garland and Quillen in [15] and [41] showed that $K_2(\mathcal{O}_F)$ is finite. A conjecture of Birch and Tate connects the order of $K_2(\mathcal{O}_F)$ and the value of the zeta function of $F$ at $-1$ when $F$ is a totally real number field. Now, what about the structure of $K_2(\mathcal{O}_F)$? So far we must rely on specific families of fields to give us insight. A starting point for investigating this problem is the following.

We are interested in the 4-rank of $K_2(\mathcal{O})$ for the quadratic number fields $\mathbb{Q}(\sqrt{pl}), \mathbb{Q}(\sqrt{2pl}), \mathbb{Q}(\sqrt{-pl}), \mathbb{Q}(\sqrt{-2pl})$ for primes $p \equiv 7 \mod 8, l \equiv 1 \mod 8$ with $(\frac{l}{p}) = 1$. In [7], the authors established a method of determining the 4-rank of $K_2(\mathcal{O})$ for these fields by checking at most two positive definite binary quadratic forms. In order to study densities of 4-ranks, we fix a prime $p \equiv 7 \mod 8$ and consider the set $\Omega = \{l \text{ prime} : l \equiv 1 \mod 8, (\frac{l}{p}) = 1\}$. In this thesis, we prove for the fields $\mathbb{Q}(\sqrt{pl}), \mathbb{Q}(\sqrt{2pl}), 4$-rank 1 and 2 each appear with natural density $\frac{1}{2}$ in $\Omega$. For the fields $\mathbb{Q}(\sqrt{-pl}), \mathbb{Q}(\sqrt{-2pl})$, we prove 4-rank 0 and 1 each appear with natural density $\frac{1}{2}$ in $\Omega$. We then form tuples of 4-ranks and prove that each of the eight possible tuples of 4-ranks appear with natural density $\frac{1}{8}$ in $\Omega$.

In chapter 1, we collect the main tools which are necessary to prove our results. These tools involve Legendre symbols, Artin symbols, primes which split completely, unramified primes, natural densities, and the Chebotarëv Density Theorem.

In chapter 2, we provide information about the object $K_2(\mathcal{O})$ and its structure, in particular the 4-rank.

In chapter 3, we construct certain finite extensions of $\mathbb{Q}$ which, via the ideas in chapters 1 and 2, lead us to our density results. In Appendices 1 and 2, we include our tables which suggested density results and present the program that we used for the computation of the these tables.
1. Background

1.1 Tools

A number field $K$ is a subfield of the complex numbers $\mathbb{C}$ which has finite degree over $\mathbb{Q}$. Denote the degree of $K$ over $\mathbb{Q}$ by $[K : \mathbb{Q}]$. Given a number field $K$, we let $\mathcal{O}_K$ denote the ring of algebraic integers of $K$, that is the collection of all $\alpha \in K$ which are roots of a monic polynomials with integer coefficients. For a nonzero ideal $a$ of $\mathcal{O}_K$, we form the quotient ring or residue field $\mathcal{O}_K/a$ and note that this ring is finite. Given a nonzero ideal $a$ of $\mathcal{O}_K$, we define the norm of $a$ to be $N(a) = |\mathcal{O}_K/a|$, that is the number of elements of $\mathcal{O}_K/a$. Note that $N(a)$ is finite. In general, rings of integers are not unique factorization domains, but are Dedekind domains. This means that nonzero elements of $\mathcal{O}_K$ do not necessarily have unique prime element decompositions, but nonzero ideals of $\mathcal{O}_K$ have a unique decomposition into a product of prime ideals. To clarify,

Theorem 1.4. If $K$ is a number field, then any nonzero ideal $a$ in $\mathcal{O}_K$ can be written as a product

$$a = p_1 \ldots p_r$$

of prime ideals and the decomposition is unique up to order.

Note the $p_i$'s are exactly the prime ideals of $\mathcal{O}_K$ containing $a$. We can phrase this statement as “to divide is to contain” [28].

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
We sometimes say prime for nonzero prime ideal and rational prime for a prime in \( \mathbb{Z} \). Also, the phrases “prime of \( K \)” and “nonzero prime ideal of \( \mathcal{O}_K \)” are interchanged. Now we want to investigate how primes behave in finite extensions of number fields. Suppose \( K \) is a number field, and \( L \) is a finite extension of \( K \). For \( p \), a prime ideal of \( \mathcal{O}_K \), we consider \( p\mathcal{O}_L \), an ideal of \( L \). From Theorem 1.4, we have

\[
p\mathcal{O}_L = \beta_1^{e_1} \cdots \beta_g^{e_g}
\]

where the \( \beta_i \)'s are distinct primes of \( L \) containing \( p \). The integer \( e_i \) is called the \textbf{ramification index} of \( p \) in \( \beta_i \). It is sometimes denoted \( e_{\beta_i | p} \) to emphasize the dependence on the ideal \( p \) and prime \( \beta_i \).

Note that we have a residue field extension \( \mathcal{O}_L / \beta_i \) over \( \mathcal{O}_K / p \) for each prime \( \beta_i \) containing \( p \). The degree of this extension, \( [\mathcal{O}_L / \beta_i : \mathcal{O}_K / p] \), written \( f_i \) or \( f_{\beta_i | p} \), is the \textbf{inertial degree} of \( p \) in \( \beta_i \). A nice relationship between the \( e_i \)'s, \( f_i \)'s, \( g \), and the degree of \( L \) over \( K \) is the following, see [3], section 3.5 or [28], chapter 12, section 3.

**Theorem 1.5.** Let \( K \subset L \) be number fields, and let \( p \) be a prime of \( K \). If \( e_i \) and \( f_i \) are the ramification and inertial degrees respectively for \( i = 1, \ldots, g \), then

\[
\sum_{i=1}^{g} e_i f_i = [L : K].
\]

We say that a prime \( p \) of \( K \) is \textbf{ramified} in \( L \) if there exists a positive integer \( i \) such that \( e_i > 1 \). Also, a prime \( p \) of \( K \) is \textbf{inert} in \( L \) if \( p\mathcal{O}_L \) is prime in \( L \). We will mainly be concerned with Galois extensions \( K \subset L \).

**Theorem 1.6.** Let \( K \subset L \) be a Galois extension, and let \( p \) be a prime in \( K \). The Galois group \( \text{Gal}(L/K) \) acts transitively on the primes of \( L \) containing \( p \), i.e, if \( \beta \) and \( \beta' \) are primes of \( L \) containing \( p \), then there is a \( \sigma \in \text{Gal}(L/K) \) such that...
If $L$ is a Galois extension of $K$, Theorem 1.5 simplifies.

**Theorem 1.7.** Let $K \subset L$ be a Galois extension and let $p$ be a prime in $K$. Then the primes $\beta_1, \ldots, \beta_g$ of $L$ containing $p$ all have the same ramification index $e$, the same inertial degree $f$, and

$$efg = [L : K].$$

**Example 1.8.** Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Consider the rational prime 2. We have

$$2\mathcal{O}_L = < 1 + i >^2$$

and so $e = 2$, $f = 1$, $g = 1$.

For the rational prime 3, we have

$$3\mathcal{O}_L = < 3 >$$

and so $e = 1$, $f = 2$, $g = 1$.

For the rational prime 5, we have

$$5\mathcal{O}_L = < 1 - 2i > < 1 + 2i >$$

and so $e = 1$, $f = 1$, and $g = 2$.

More generally, let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{N})$ for some $N \neq 0,1$ squarefree integer. As $L$ is Galois over $\mathbb{Q}$, from Theorem 1.7

$$efg = 2.$$

So we have the following possibilities for a rational prime $p$. 

\[9\]
(i) If \( e = 2, f = 1, g = 1 \), then \( p\mathcal{O}_L = \beta^2 \) for some prime \( \beta \) in \( L \) containing \( p \).

(ii) If \( e = 1, f = 2, g = 1 \), then \( p\mathcal{O}_L = \beta \) for some prime \( \beta \) in \( L \) containing \( p \).

(iii) If \( e = 1, f = 1, g = 2 \), then \( p\mathcal{O}_L = \beta_1\beta_2 \) for some primes \( \beta_1, \beta_2 \) in \( L \) containing \( p \).

For a Galois extension \( K \subset L \), an ideal \( p \) of \( K \) is \textbf{ramified} in \( L \) if \( e > 1 \), and is \textbf{unramified} in \( L \) if \( e = 1 \). If \( e = f = 1 \), we say that \( p \) splits completely in \( L \). Such a \( p \) would also be unramified in \( L \) and the number of primes in the decomposition of \( p\mathcal{O}_L \) is \([L : K]\). For a prime \( p \) of \( K \) which is inert in \( L \), \( g = e = 1 \) and \( f = [L : K] \).

Now we consider the following question which will prove useful in Chapter 3. Is there a criterion for when primes are unramified or split completely in a composite field? Recall for two number fields \( L \) and \( M \), the \textbf{composite} \( LM \) is defined as the smallest subfield of \( \mathbb{C} \) containing \( L \) and \( M \). From [35], Theorem 31, we have

\textbf{Theorem 1.9.} Let \( K \) be a number field, and let \( L \) and \( M \) be two extensions of \( K \). Fix a prime \( p \) of \( K \). If \( p \) is unramified in both \( L \) and \( M \), then \( p \) is unramified in the composite field \( LM \). If \( p \) splits completely in both \( L \) and \( M \), then \( p \) splits completely in \( LM \).

We say \( L \) is a \textbf{normal} extension of \( K \) if the embeddings of \( L \) in \( \mathbb{C} \) fixing \( K \) are actually automorphisms of \( L \). Given \( K, L \) number fields such that \( K \subset L \), we say \( M \) is the \textbf{normal closure} of \( L \) over \( K \) if \( M \) is the smallest normal extension of \( K \) containing \( L \). As a consequence of Theorem 1.9, we have

\textbf{Corollary 1.10.} Let \( K \) and \( L \) be number fields, \( K \subset L \) and let \( p \) be a prime in \( K \). If \( p \) is unramified or split completely in \( L \), then the same is true in the normal closure \( M \) of \( L \) over \( K \).

Now, how can we classify primes which are ramified or split completely in a number field \( K \)? Let us consider quadratic number fields, that is fields of degree 2
over \( \mathbb{Q} \). Let \( K = \mathbb{Q}(\sqrt{N}) \), where \( N \neq 0,1 \) is a squarefree integer. The discriminant \( d_K \) is given by

\[
    d_K = \begin{cases} 
        N & \text{if } N \equiv 1 \mod 4 \\
        4N & \text{otherwise}
    \end{cases}
\]

For quadratic number fields, we can nicely determine their rings of integers in the following way:

\[
    \mathcal{O}_K = \begin{cases} 
        \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \mod 4 \\
        \mathbb{Z}[\frac{1+\sqrt{N}}{2}] & \text{if } N \equiv 1 \mod 4
    \end{cases}
\]

We also define the Legendre symbol \( \left( \frac{a}{p} \right) \). If \( a \) is an integer and \( p \) an odd prime, then

\[
    \left( \frac{a}{p} \right) = \begin{cases} 
        0 & \text{if } p \mid a \\
        1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \mod p \text{ is solvable for some } x \in \mathbb{Z} \\
        -1 & \text{if } p \nmid a \text{ and } x^2 \not\equiv a \mod p \forall x \in \mathbb{Z}
    \end{cases}
\]

We shall list some properties of this symbol.

**Proposition 1.11.** Let \( a \) and \( b \) be integers and \( p \) an odd prime. Then

(i) \( a^{\frac{p-1}{2}} \equiv \left( \frac{a}{p} \right) \mod p \)

(ii) \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \)

(iii) If \( a \equiv b \mod p \), then \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \).

Now we may state a classical law formulated by Euler and Legendre. As Gauss was the first to give a complete proof, he called it the Theorem Aureum or golden theorem.
Theorem 1.12. (Law of Quadratic Reciprocity) Let $p$ and $q$ be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

We can now describe the primes of $K$.

Proposition 1.13. Let $p$ be an odd prime in $\mathbb{Z}$ and $K$ a quadratic field of discriminant $d_K$. Then

(i) If $\left(\frac{d_K}{p}\right) = 0$, then $p\mathcal{O}_K = p^2$ for some prime ideal $p$ of $\mathcal{O}_K$ (i.e. $p$ ramifies in $K$).

(ii) If $\left(\frac{d_K}{p}\right) = 1$, then $p\mathcal{O}_K = pp'$ for some prime ideals $p \neq p'$ of $\mathcal{O}_K$ (i.e. $p$ splits completely in $K$).

(iii) If $\left(\frac{d_K}{p}\right) = -1$, then $p\mathcal{O}_K$ is prime in $\mathcal{O}_K$ (i.e. $p$ is inert in $K$).

Example 1.14. Let $N = -163$ and consider $K = \mathbb{Q}(\sqrt{-163})$. Since $N \equiv 1 \mod 4$, $d_K = -163$. Every odd rational prime $p \neq 163$ is unramified in $K$ as $p \nmid -163$.

Thus part (i) in Proposition 1.13 does not occur. Let us realize parts (ii) and (iii).

For the rational prime $p = 167$, we have

$$\left(\frac{-163}{167}\right) = \left(\frac{-1}{167}\right)\left(\frac{163}{167}\right) = -\left(\frac{163}{167}\right) = \left(\frac{167}{163}\right) = \left(\frac{4}{163}\right) = 1.$$ 

Thus

$$167\mathcal{O}_K = pp'$$

for some primes $p \neq p'$ in $K$.

For the rational prime $3$, we have

$$\left(\frac{-163}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{163}{3}\right) = -\left(\frac{163}{3}\right) = -\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$ 

Thus $3\mathcal{O}_K$ is prime in $\mathcal{O}_K$.

As a historical note, $N = -163$ was chosen as it relates to Gauss’ class number.
M problem, which aims to classify all imaginary quadratic fields with class number M. For \( K = \mathbb{Q}(\sqrt{N}) \), \( N < 0 \), squarefree, Stark proved in 1966 that \( h(K) = 1 \) happens for exactly nine fields, i.e,

\[
h(K) = 1 \text{ if and only if } N = -1, -2, -3, -7, -11, -19, -43, -67, -163.
\]

Recent work by Mark Watkins [57] allows one to handle all \( M \leq 16 \).

So we have related the decomposition of an ideal in a quadratic number field and the Legendre symbol. Let us note that there exists a general procedure for determining how a given rational prime decomposes in a given number field. We now discuss the relationship between primes and another symbol, the Artin symbol. To do this we introduce two important groups. Let \( K \subset L \) be Galois and let \( \beta \) be a prime of \( L \).

**Definition 1.15.** The decomposition group is the group

\[
D_\beta = \{ \sigma \in \text{Gal}(L/K) : \sigma(\beta) = \beta \}.
\]

**Definition 1.16.** The inertia group is the group

\[
I_\beta = \{ \sigma \in \text{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \mod \beta, \quad \forall \alpha \in \mathcal{O}_L \}.
\]

**Illustration 1.17.** Let \( K = \mathbb{Q} \) and \( L = \mathbb{Q}(\sqrt{N}) \) where \( N \neq 0, 1 \) is a squarefree integer. Let \( p \) be a rational prime which ramifies in \( L \). Then

\[
p\mathcal{O}_L = \beta^2
\]

where \( \beta = \langle 2, \sqrt{N} \rangle \) is a prime of \( L \). We have \( \text{Gal}(L/K) = \{ \sigma_1, \sigma_2 \} \) where

\[
\sigma_1 = \text{id} : \sqrt{N} \rightarrow \sqrt{N} \text{ and } \sigma_2 : \sqrt{N} \rightarrow -\sqrt{N}.
\]

Clearly \( \sigma_1 \in D_\beta \). Also \( \sigma_2 \in D_\beta \) as
for $\alpha = 2x + y\sqrt{N} \in <2,\sqrt{N}>$ with $x, y \in \mathbb{Z}$, we have

$$\sigma_2(\alpha) = 2x - y\sqrt{N}$$
$$= 2x + (-y)\sqrt{N} \in <2,\sqrt{N}>.$$  

Thus $|D_\beta| = 2$. Now of course $\sigma_1 \in I_\beta$. To see that $\sigma_2 \in I_\beta$, let $\alpha \in \mathcal{O}_L = \mathbb{Z}[\sqrt{N}]$ (for $N \equiv 2,3 \text{ mod } 4$) and so $\alpha = a + b\sqrt{N}$ where $a, b \in \mathbb{Z}$. Then

$$\sigma_2(\alpha) = a - b\sqrt{N}$$
$$\equiv a + b\sqrt{N} \mod <2,\sqrt{N}>$$

as $a - b\sqrt{N} - (a + b\sqrt{N}) = -2b\sqrt{N} \in <2,\sqrt{N}>$. Similarly if $\alpha \in \mathcal{O}_L = \mathbb{Z}[\frac{1 + \sqrt{N}}{2}]$ (for $N \equiv 1 \text{ mod } 4$). Hence $|I_\beta| = 2$.

**Remark 1.18.** If $\sigma \in I_\beta$, then $\sigma(\alpha) \equiv \alpha \mod \beta$, $\forall \alpha \in \mathcal{O}_L$. In particular, $\sigma(\alpha) \equiv 0 \mod \beta$ for $\alpha \equiv 0 \mod \beta$. Thus $\sigma(\beta) = \beta$, that is $\sigma \in D_\beta$ and so $I_\beta \subset D_\beta$.

Also an element $\sigma \in D_\beta$ induces an automorphism $\tilde{\sigma}$ of $\mathcal{O}_L/\beta$. To see this, we first note that every element $\sigma \in \text{Gal}(L/K)$ restricts to an automorphism of $\mathcal{O}_L$. Now, if $\sigma \in D_\beta$, then the induced map $\mathcal{O}_L \to \mathcal{O}_L/\beta$ has kernel $\beta$. By the 1st Isomorphism Theorem, we have an automorphism $\tilde{\sigma}$ of $\mathcal{O}_L/\beta$. Since $\sigma \in D_\beta$ fixes $K$ and thus $\mathcal{O}_K$, $\tilde{\sigma}$ fixes $\mathcal{O}_K/p$. If $\tilde{G}$ denotes the Galois group of $\mathcal{O}_L/\beta$ over $\mathcal{O}_K/p$, then $\tilde{\sigma} \in \tilde{G}$. Note we have a homomorphism $\Psi: D_\beta \to \tilde{G}$ defined by $\sigma \mapsto \tilde{\sigma}$. We see ker $\Psi = I_\beta$ as $\gamma \in \ker \Psi$ if and only if $\Psi(\gamma) = \text{Id}_{\tilde{G}}$ if and only if $\gamma(\alpha) \equiv \alpha \mod \beta$ for all $\alpha \in \mathcal{O}_L$ if and only if $\gamma \in I_\beta$.

We further describe $I_\beta$, $D_\beta$, and $\Psi$ in the following, compare Prop 5.10 [10] or Theorem 28 [35].

**Proposition 1.19.** Let $D_\beta$, $I_\beta$, and $\tilde{G}$ be as above. Then

(i) The homomorphism $\Psi: D_\beta \to \tilde{G}$ is surjective. Thus $D_\beta/I_\beta \cong \tilde{G}$.

(ii) $|I_\beta| = e_{\beta|p}$ and $|D_\beta| = e_{\beta|p}f_{\beta|p}$.
It is well known that $\tilde{G}$ is a cyclic group as it is a Galois group of a finite extension of a finite field. Hence from Proposition 1.19, $D_\beta/I_\beta$ is a cyclic group. Now that we have discussed the decomposition and inertia groups, we use the following lemma to introduce the Artin symbol. Since this lemma is of great interest, we will state the proof.

**Lemma 1.20.** Let $K \subset L$ be a Galois extension, and let $p$ be a prime of $\mathcal{O}_K$ which is unramified in $L$. If $\beta$ is a prime of $\mathcal{O}_L$ containing $p$, then there is a unique element $\sigma \in \text{Gal}(L/K)$ such that

$$\sigma(a) \equiv a^{N(p)} \mod \beta, \quad \forall a \in \mathcal{O}_L$$

where $N(p) = |\mathcal{O}_K/p|$ is the norm of $p$.

**Proof.** We follow [10]. Let $D_\beta$ and $I_\beta$ be the decomposition group and inertia group of $\beta$. We have seen that $\sigma \in D_\beta$ induces an element $\tilde{\sigma} \in \tilde{G}$. Since $p$ is unramified in $L$, $|I_\beta| = 1$ by Proposition 1.19 part (ii). Thus by part (i) of this Proposition, $\sigma \mapsto \tilde{\sigma}$ defines an isomorphism

$$D_\beta \rightarrow \tilde{G}.$$  

If $\mathcal{O}_K/p$ has $q$ elements, then $\tilde{G}$ is a cyclic group with generator $x \mapsto x^q$. Since $N(p) = q$, $\sigma$ satisfies the condition

$$\sigma(a) \equiv a^{N(p)} \mod \beta, \quad \forall a \in \mathcal{O}_L.$$  

Note that any $\sigma$ satisfying this condition must be in $D_\beta$ and so we have uniqueness. 

The generator $x \mapsto x^q$ in the proof of Lemma 1.20 is called the Frobenius
automorphism. The unique element \( \sigma \) is called the Artin symbol. This symbol will be denoted \( \left( \frac{L/K}{\beta} \right) \) as it depends on \( \beta \). Now what are some important properties of the Artin symbol?

**Corollary 1.21.** Let \( K \subset L \) be a Galois extension, and let \( p \) be a prime of \( K \) which is unramified in \( L \). Given a prime \( \beta \) of \( L \) containing \( p \), we have

(i) If \( \sigma \in \text{Gal}(L/K) \), then \( \left( \frac{L/K}{\sigma(\beta)} \right) = \sigma \left( \frac{L/K}{\beta} \right) \sigma^{-1} \)

(ii) The order of \( \left( \frac{L/K}{\beta} \right) \) is the inertial degree \( f = f_{\beta|\mathfrak{p}} \)

(iii) \( p \) splits completely in \( L \) if and only if \( \left( \frac{L/K}{\beta} \right) = 1 \text{Id}_{\text{Gal}(L/K)} \).

**Proof.** (i) Any element in \( \mathcal{O}_L \) can be written as \( \tau^{-1}(x) \) where \( x \in \mathcal{O}_L \) and \( \tau \in \text{Gal}(L/K) \). Thus we have

\[
\left( \frac{L/K}{\beta} \right) \tau^{-1}(x) \equiv \tau^{-1}(x)^{\sigma} \mod \beta.
\]

Applying \( \tau \), we obtain

\[
\tau \left( \frac{L/K}{\beta} \right) \tau^{-1}(x) \equiv x^{\sigma} \mod \tau(\beta).
\]

But we also have

\[
\left( \frac{L/K}{\tau(\beta)} \right)(x) \equiv x^{\sigma} \mod \tau(\beta) \quad, \quad \forall x \in \mathcal{O}_L.
\]

So by uniqueness, \( \left( \frac{L/K}{\tau(\beta)} \right) = \tau \left( \frac{L/K}{\beta} \right) \tau^{-1} \).

(ii) Since \( p \) is unramified, the decomposition group \( D_\beta \) is isomorphic to \( \tilde{G} \). The Artin symbol maps to the generator of \( \tilde{G} \) which has order \( f \). Thus the Artin symbol has order \( f \).

(iii) Recall \( p \) splits completely in \( L \) if and only if \( e = f = 1 \). We are assuming \( e = 1 \) and so the conclusion follows from (ii). \( \square \)
Corollary 1.22. Let $K \subset E \subset L$ be number fields with $L$ a Galois extension of $K$ and $E$ normal over $K$. Let $\beta$ be a prime of $L$ containing a prime $p$ of $E$ which in turn contains a prime $p_0$ in $K$ which is unramified in $L$. Then

$$\left(\frac{L/K}{\beta}\right)_E = \left(\frac{E/K}{p}\right).$$

Proof. If $p_0$ is unramified in $L$, then $p$ is unramified in $L$. Note that $p$ is unramified in $E$. As $E$ is normal over $K$, $\text{Gal}(E/K)$ is defined. Now for $x \in \mathcal{O}_E$ and $\sigma \in \text{Gal}(L/K)$, we have the following equivalence:

$$\sigma(x) \equiv x^q \mod \beta \text{ if and only if } \sigma(x) \equiv x^q \mod p.$$

To see this, suppose $\sigma(x) \equiv x^q \mod p$. Then $\sigma(x) - x^q \equiv 0 \mod p$ and so $\sigma(x) - x^q \in p$. Since $p \subset \beta$, $\sigma(x) - x^q \in \beta$ which implies $\sigma(x) \equiv x^q \mod \beta$. Conversely, suppose $x \in \mathcal{O}_E$ and $\sigma(x) \equiv x^q \mod \beta$, i.e. $\sigma(x) - x^q \in \beta$. Now as $E$ is normal over $K$, $\forall \sigma \in \text{Gal}(L/K)$ we have $\sigma|_E \in \text{Gal}(E/K)$ and so $\sigma(x) \in E$. Clearly $x^q \in E$ and thus $\sigma(x) - x^q \in E$. So $\sigma(x) - x^q \in E \cup \beta = p$, i.e. $\sigma(x) \equiv x^q \mod p$. □

Remark 1.23. Suppose $E_1$ and $E_2$ are normal over $K$ and $L$ is the compositum of $E_1$ and $E_2$. Let $\beta$ be a prime of $L$ containing primes $p_1$ and $p_2$ of $E_1$ and $E_2$ respectively which in turn both contain a prime $p_0$ of $K$ which is unramified in $L$. The Artin symbols $\left(\frac{L/K}{\beta}\right)$, $\left(\frac{E_1/K}{p_1}\right)$, and $\left(\frac{E_2/K}{p_2}\right)$ are defined, but they lie in different Galois groups. Consider the mapping

$$\text{Gal}(L/K) \to \text{Gal}(E_1/K) \times \text{Gal}(E_2/K)$$

defined by

$$\sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2}).$$
This is a one to one mapping as an automorphism fixing $E_1$ and $E_2$ would fix $L$. After identifying $\text{Gal}(L/K)$ with its image in the direct product and using Corollary 1.22, we have

**Proposition 1.24.**

\[
\left( \frac{L/K}{\beta} \right) = \left( \frac{E_1/K}{p_1} \right) \times \left( \frac{E_2/K}{p_2} \right).
\]

**Remark 1.25.** Notice that the set \( \{(L/K)_{\beta} : \beta \text{ is a prime of } L \text{ containing } p\} \) is a conjugacy class of $\text{Gal}(L/K)$. To see this, let $\beta_1, \ldots, \beta_q$ be the primes of $L$ containing $p$. Then

\[
\{\sigma \left( \frac{L/K}{\beta} \right) \sigma^{-1} : \sigma \in \text{Gal}(L/K)\} = \left\{ \left( \frac{L/K}{\sigma(\beta)} \right) : \sigma \in \text{Gal}(L/K) \right\} \quad \text{by Corollary 1.21}
\]

\[
= \left\{ \left( \frac{L/K}{\beta_1} \right), \ldots, \left( \frac{L/K}{\beta_q} \right) \right\}
\]

since $\text{Gal}(L/K)$ acts transitively on the primes of $L$ containing $p$. We will denote this conjugacy class by $\left( \frac{L/K}{p} \right)$ and say this is the Artin symbol of $p$.

Let $K = \mathbb{Q}$, $L$ be a Galois extension of $\mathbb{Q}$, and $G = \text{Gal}(L/\mathbb{Q})$. Recall the group $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$ is the center of $G$. Let $Z(G)'$ denote the fixed field of $Z(G)$, that is $\{x \in L : \sigma(x) = x, \forall \sigma \in Z(G)\}$. By the Fundamental Theorem of Galois Theory, we have the following one to one correspondence of subfields of $L$ and subgroups of $\text{Gal}(L/\mathbb{Q})$:

\[
\begin{array}{ccc}
L & \{1\} \\
| & | \\
Z(G)' & \leftrightarrow & Z(G) \\
| & | \\
\mathbb{Q} & \text{Gal}(L/\mathbb{Q}).
\end{array}
\]
Let $p$ be a prime of $\mathbb{Q}$ which is unramified in $L$ and $\beta$ be a prime of $L$ containing $p$. From Corollary 1.21, part (iii),

$$\left(\frac{L/\mathbb{Q}}{\beta}\right) = \text{Id}_{\text{Gal}(L/\mathbb{Q})}$$

if and only if $p$ splits completely in $L$.

From the diagram and Remark 1.25, this statement reduces to the following. Here $\{g\}$ denotes the conjugacy class containing one element $g$.

**Lemma 1.26.** $\left(\frac{L/\mathbb{Q}}{p}\right) = \{g\} \subseteq Z(G)$ for some $g \in Z(G)$ if and only if $p$ splits completely in $Z(G)'$.

**Proof.** Let $p$ be unramified in $L/\mathbb{Q}$ and $\beta$ a prime in $L$ containing $p$. Then $\left(\frac{L/\mathbb{Q}}{p}\right) = \{g\}$ for some $g \in Z(G)$ if and only if $\left(\frac{L/\mathbb{Q}}{\beta}\right) = g$ if and only if $\left(\frac{Z(G)'/\mathbb{Q}}{\beta}\right) = \left(\frac{L/\mathbb{Q}}{Z(G)'}\right) = g\mid_{Z(G)'} = \text{Id}_{\text{Gal}(Z(G)'/\mathbb{Q})}$ if and only if $p$ splits completely in $Z(G)'$ by Corollary 1.21, part (iii).

Thus if we can show that rational primes are split completely in a fixed field of the center of a certain Galois group $G$, then we know the associated Artin symbol is a conjugacy class containing one element. Hence we may identify the Artin symbol with this one element and consider the symbol to be an automorphism which lies in $Z(G)$. Thus determining the order of $Z(G)$ gives us the number of possible choices for the Artin symbol. This lemma will play an important role in Chapter 3.

### 1.2 Densities

We will now discuss the notion of a set of rational primes having a natural density. The idea is that the natural density of a set of certain primes can be related to Artin symbols. To begin, let us consider two types of density. Throughout this section, $|G|$ denotes the order of a finite set $G$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
**Definition 1.27.** A set $S$ of prime numbers has **Dirichlet Density**, $\delta(S)$, if

$$\lim_{s \to 1^+} \frac{\sum_{p \in S} \frac{1}{p^s}}{\sum_{p \text{ prime}} \frac{1}{p^s}}$$

exists and equals $\delta(S)$.

A more intuitive notion is the following.

**Definition 1.28.** A set $S$ of prime numbers has **Natural Density** $\Delta(S)$ if

$$\lim_{n \to \infty} \frac{|\{p \leq n : p \in S\}|}{|\{p \leq n : p \text{ prime}\}|}$$

exists and equals $\Delta(S)$.

If a set of primes has a natural density, then it has a Dirichlet density, and the two densities are equal, see [20], page 252. Note that the converse is not true in general. For example from [49], let $S$ be the set of prime numbers whose leading digit (in the decimal system) is 1. Then $S$ does not have a natural density, but its Dirichlet density is $\log_{10}(2)$. Thus it is stronger to say that a set of prime numbers has a natural density, as opposed to a Dirichlet density.

For an example of a set of primes having a natural density, let us recall a famous theorem of Dirichlet. Denote by $\phi(m)$, the number of integers $x$ with $1 \leq x < m$ and $\gcd(x, m) = 1$. For example, $\phi(1837) = 1660$. Dirichlet proved the following theorem in 1837.

**Theorem 1.29.** Let $m$ be a positive integer. Then for each integer $a$ with $\gcd(a, m) = 1$ the set of prime numbers $p$ with $p \equiv a \pmod{m}$ has natural density $\frac{1}{\phi(m)}$.

The proof of this theorem in terms of natural density was given by De la Vallée-Poussin in 1896 [11].
Now we relate natural densities of certain sets of prime numbers to Artin symbols. This beautiful relationship is given by the Chebotarev Density Theorem proved in 1922.

**Theorem 1.30.** Let $N$ be a normal extension of $\mathbb{Q}$, $G = Gal(N/\mathbb{Q})$, $q$ a rational prime unramified in $N/\mathbb{Q}$, and $C_g$ the conjugacy class of $g \in G$. Then the set of rational primes $q$ for which
\[
\left(\frac{N/\mathbb{Q}}{q}\right) = C_g
\]
has a natural density which is equal to $\frac{|C_g|}{|G|}$.

For the convenience of the reader, we give suitable references of proofs. One proof uses Ikehara's Tauberian theorem which yields a density for primes in given ideal classes. Refer to section 5 in [33] which uses techniques, in part due to Hecke [21].

Alternatively, Lagarias and Odlyzko in [31] prove two versions of the Chebotarev Density Theorem, each of which involve an explicitly computable error term. One version assumes the truth of the Generalized Riemann Hypothesis and the other holds unconditionally.

It is noted in [34] that modern treatments of this theorem involve class field theory. The original proof did not as Chebotarev's argument relied on "crossing" arbitrary abelian extensions of number fields with cyclotomic extensions.

**Remark 1.31.** The set of rational primes $p$ that split completely in $N$ has natural density $\frac{1}{|G|}$. To see this, let $p$ be a rational prime unramified in $N$. From Corollary 1.21, part(iii),
\[
p \text{ splits completely in } N \text{ if and only if } \left(\frac{N/\mathbb{Q}}{p}\right) = \{Id_{Gal(N/\mathbb{Q})}\}.
\]

Thus we are considering the conjugacy class of the identity element and so $|C_g| = 1$. 

21

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
In the next chapter, we discuss $K_2(\mathcal{O})$ and relate its structure in some cases to natural densities.
2. $K_2(O)$

Let $R$ be a ring with unity and $R^*$ its group of units. For $n \in \mathbb{N}$, denote by $GL(n, R)$ the group of invertible $n \times n$ matrices over $R$. Let $E(n, R)$ be the group generated by elementary matrices $e_{ij}(\lambda), \lambda \in R, 1 \leq i, j \leq n, i \neq j$ where $\lambda$ is in the $i^{th}$ row, $j^{th}$ column, there are 1's along the main diagonal and zeros elsewhere. We are concerned with $GL(R)$ and $E(R)$ which are direct limits as $n \to \infty$ of the groups $GL(n, R)$ and $E(n, R)$. For example, a matrix in $GL(R)$ looks like

\[
\begin{pmatrix}
A & & \\
& 1 & \\
& & 1 \\
& & & \ddots
\end{pmatrix}
\]

where $A \in GL(n, R)$ for some $n \in \mathbb{N}$, there are infinitely many 1's along the main diagonal and zeros elsewhere. In 1962, Steinberg introduced the following group which mimics the properties of the group generated by elementary matrices.

**Definition 2.32.** The **Steinberg group** $St(R)$ is the group given by generators $x_{ij}(\lambda), \lambda \in R, i, j \in \mathbb{N}, i \neq j$, and relations

\[
(i) \ x_{ij}(\lambda)x_{ij}(\gamma) = x_{ij}(\lambda + \gamma)
\]
Here \([a, b] = aba^{-1}b^{-1}\) denotes the commutator of \(a\) and \(b\). Note that an equivalent definition could be given for \(St(n, R)\) for \(n \geq 3\). Since the elementary matrices \(e_{ij}(\lambda)\) also satisfy these relations, we have a canonical homomorphism \(\phi : St(R) \rightarrow GL(R)\) given by \(\phi(x_{ij}(\lambda)) = e_{ij}(\lambda)\). For example,

\[
\phi(x_{12}(\lambda)) = e_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ & 1 \\ & & \ddots \end{pmatrix}.
\]

Of course, \(\phi(St(R)) = E(R) \subset GL(R)\). Now we define \(K_2(R)\).

**Definition 2.33.** \(K_2(R) = \ker(\phi)\)

This tells us that \(K_2(R)\) can be viewed as the normal subgroup of \(St(R)\) generated by all non-trivial relations between elementary matrices over \(R\) where (i) and (ii) are considered trivial relations.

Theorem 5.1 in [37] gives us that \(K_2(R)\) is the center of \(St(R)\), whereby \(K_2(R)\) is an abelian group. If \(R\) is commutative, then we can describe other elements of \(K_2(R)\).

**Definition 2.34.** Let \(R\) be a commutative ring with unity, \(a, b \in R^*\). Let \(w_{12}(a) = x_{12}(a)x_{21}(-a^{-1})x_{12}(a), h_{12}(a) = w_{12}(a)w_{12}(-1)\). The element \(\{a, b\}\) of \(St(R)\), defined by \(\{a, b\} = h_{12}(a)h_{12}(b)h_{12}(ab)^{-1}\), is called a Steinberg symbol with entries in \(R\).

Actually a more general setting to discuss these symbols can be found in [37],
Corollary 11.3 or [50]. Note that

\[
\phi([a, b]) = \phi(h_{12}(a)h_{12}(b)h_{12}(ab)^{-1}) = \phi(h_{12}(a))\phi(h_{12}(b))\phi(h_{12}(ab)^{-1})
\]

\[
= \begin{pmatrix}
    a & a^{-1} \\
    b & b^{-1} \\
\end{pmatrix}
\begin{pmatrix}
    (ab)^{-1} \\
    ab \\
\end{pmatrix}
\begin{pmatrix}
    1 & 1 \\
    1 & \ldots \\
\end{pmatrix}
\]

Thus \{a, b\} \in K_2(R) for all \(a, b \in R^*\).

Now what can we say about \(K_2(F)\) for \(F\) a field? How does this object relate to the above definition? Nicely enough from [36], we have

**Theorem 2.35.** \(K_2(F)\) has a presentation as an abelian group given by generators \(\{a, b\}\) with \(a, b \in F^*\) and relations:

(i) \(\{a_1a_2, b\} = \{a_1, b\}\{a_2, b\}, \forall a_1, a_2, b \in F^*\)

(ii) \(\{a, b_1b_2\} = \{a, b_1\}\{a, b_2\}, \forall a, b_1, b_2 \in F^*\)

(iii) \(\{a, 1 - a\} = 1, \forall a \in F^* \setminus \{1\}\).

Now let \(F\) be a number field and \(\mathcal{O}_F\) its ring of integers. To obtain an alternative yet equivalent definition of \(K_2(R)\) when \(R = \mathcal{O}_F\), we first need the following.

**Definition 2.36.** Let \(p\) be a prime ideal of \(\mathcal{O}_F\), \(v\) the valuation corresponding to
p with residue class field \( \mathcal{O}_F/p \). The map

\[
\tau_p : F^* \times F^* \rightarrow (\mathcal{O}_F/p)^*
\]

\[
(x, y) \mapsto (-1)^{u(x)u(y)} \frac{x^{u(y)}}{y^{u(x)}} \mod p
\]

is called the \( p \)-adic tame symbol on \( F \).

This tame symbol gives rise to a homomorphism from \( K_2(F) \) onto \( (\mathcal{O}_F/p)^* \) via Corollary 11.3 in [37]. We denote this homomorphism by \( T_p : K_2 F \rightarrow (\mathcal{O}_F/p)^* \). For a number field \( F \), we have such a map \( T_p \) for each prime \( p \) of \( \mathcal{O}_F \). Call \( \bigoplus_p T_p \) the tame symbol map \( T : K_2(F) \rightarrow \bigoplus_p (\mathcal{O}_F/p)^* \). This map is surjective by Lemma 13.8 in [37]. It was shown in [41] that \( \ker T \cong K_2(\mathcal{O}_F) \).

**Definition 2.37.** \( K_2(\mathcal{O}_F) \) is called the tame kernel of \( F \).

For any number field \( F \), Garland [15] gives us further information about the tame kernel of \( F \).

**Theorem 2.38.** \( K_2(\mathcal{O}_F) \) is a finite group.

What can we say about the order of the tame kernel? Recall that \( F \) is a totally real number field if all of its embeddings into \( \mathbb{C} \) are actually just embeddings into \( \mathbb{R} \). In 1970, J. Birch [2] and J. Tate [54] conjectured that

\[
\#K_2(\mathcal{O}_F) = |w_2(F) \cdot \zeta_F(-1)|
\]

for all totally real number fields \( F \). Here \( \zeta_F \) is the Dedekind zeta-function of \( F \) and \( w_2(F) \) is the largest integer \( N \) such that the Galois group of \( F(\mu_N) \) over \( F \) is elementary abelian 2-group. This means a product (possibly empty) of non-trivial cyclic factors, all of order 2. Here \( \mu_N \) denotes the group of \( N \)-th roots of unity. The
Birch-Tate conjecture was confirmed up to the 2-part in [59]. Thus the 2-Sylow subgroup of $K_2(O_F)$ is of great interest.

**Illustration 2.39.** For $F = \mathbb{Q}$, $w_2(F) = 24$ and $\zeta_4(-1) = -\frac{1}{12}$. Thus $\#K_2(O_{\mathbb{Q}}) = 2$. From chapter 10 in [37], $K_2(O_{\mathbb{Q}}) \cong C_2$.

To discuss the structure of the tame kernel, we introduce the following definition. Let $B$ be a finite abelian group. Hence $B$ is a product of cyclic groups of prime power order.

**Definition 2.40.** The $2^j$-rank, $j \geq 1$, of $B$ is the number of factors of $B$ of order divisible by $2^j$.

**Illustration 2.41.** Let $A$ be a finite abelian group of order 40. Then

$$A \cong C_2 \times C_4 \times C_5 \quad \text{or} \quad C_2 \times C_2 \times C_2 \times C_5 \quad \text{or} \quad C_8 \times C_5$$

Hence 2-rank $A = 2, 3,$ or 1 respectively and 4-rank $A = 1, 0,$ or 1 respectively.

For any number field $F$, the 2-rank of $K_2(O_F)$ is given by Tate's 2-rank formula in [53]. Before stating it, we need some notation. The primes ideals of a ring of integers are called the finite primes of the number field. Infinite primes are embeddings of the number field into the complex numbers. Embeddings of $F$ into $\mathbb{R}$ are called real embeddings of $F$. Dyadic primes are the prime ideals of $O_F$ that contain the rational prime number 2. Note that a general number field $F$ may have more than one dyadic prime ideal. Let $S$ be the set consisting of all dyadic and all infinite primes of $F$. If we take $C(F)$, the ideal class group of $F$, and factor out the subgroup generated by the dyadic primes of $F$, we form the $S$-class group, $C^S(F)$. 

27
Theorem 2.42. Let $F$ be an arbitrary number field, $r_1(F)$ the number of real embeddings of $F$, $g_2(F)$ the number of dyadic prime ideals of $F$, and $C^S(F)$ the $S$-class group of $F$. Then

$$2\text{-rank } K_2(O_F) = r_1(F) + g_2(F) - 1 + 2\text{-rank } (C^S(F)).$$

Example 2.43. Take $F = \mathbb{Q}$. Then $r_1(F) = 1$ and $g_2(F) = 1$. Also $C(\mathbb{Q}) = \{1\}$ as $\mathbb{Z}$ is a principal ideal domain. Thus $2\text{-rank } C^S(F) = 0$. So $2\text{-rank } K_2(O_{\mathbb{Q}}) = 2\text{-rank } K_2(\mathbb{Z}) = 1$. We have seen that $K_2(\mathbb{Z}) \cong C_2$.

We consider the case where $F$ is a quadratic number field. For quadratic number fields, the 2-rank formula simplifies. From [5],

Theorem 2.44. Let $F$ be a quadratic number field. Then

$$2\text{-rank } K_2(O_F) = \begin{cases} s + t & \text{if } F \text{ is a real quadratic number field} \\ s + t - 1 & \text{if } F \text{ is an imaginary quadratic number field} \end{cases}$$

where $2^s$ is the number of elements in $\{\pm 1, \pm 2\}$ which are norms from the given quadratic field, and $t$ is the number of odd primes which are ramified in the given quadratic field.

Example 2.45. Consider $F = \mathbb{Q}(\sqrt{2})$. Here the discriminant of $F$, denoted $d_F$, is 8. Since an odd prime $p$ is ramified in a quadratic number field if and only if $p$ divides $d_F$, we see in our case $t = 0$. Now we count the number of elements in $\{\pm 1, \pm 2\}$ which are norms from $F$. Let $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ where $a, b \in \mathbb{Q}$. Then

$$N_{F/\mathbb{Q}}(x) = a^2 - 2b^2.$$ 

We have $-1$ is a norm from $F$ as $-1 = (1)^2 - 2(1)^2$. Similarly $1 = (1)^2 - 2(0)^2$, $2 = (2)^2 - 2(1)^2$, and $-2 = (0)^2 - 2(1)^2$. So 1, 2, and -2 are also norms from.
F. Thus $s = 2$. It follows $2$-rank $K_2(O_F) = 2$. Also from Theorem 2.42, we see $2$-rank $K_2(O_F) = 2 + 1 - 1 + 0 = 2$.

Now what about 4-ranks? In [8], Conner and Hurrelbrink investigate the 4-ranks of quadratic number fields $\mathbb{Q}(\sqrt{d})$ where $d = p_1 p_2$ is a product of two prime numbers congruent to 1 modulo 8. Also in this paper, they pose a conjecture for the case when $d$ is a product of an arbitrary number of primes congruent to 1 modulo 8. They give a similar conjecture for the field $\mathbb{Q}(\sqrt{2d})$ where $d$ again is a product of an arbitrary number of primes congruent to 1 modulo 8. These two conjectures were subsequently settled by Vazzana [55], [56]. In addition, Vazzana obtains upper and lower bounds for 4-ranks of the tame kernel for any quadratic number field.

In [39] and [40], Qin determines the 4-ranks of the tame kernel for quadratic number fields whose discriminant has 3 or less odd prime divisors in terms of indefinite quadratic forms.

Hurrelbrink and Kolster in [26] have recently obtained, for any quadratic number field, 4-rank results in terms of matrices with Hilbert symbols as entries. This leads to the method in [7] of computing matrix ranks over the field $\mathbb{F}_2$ of $3 \times 3$ matrices to determine 4-ranks. This approach is then used to characterize the 4-ranks of $K_2(O_F)$ for certain quadratic number fields $F$ in terms of positive definite binary quadratic forms.

More precisely, Conner and Hurrelbrink determine the 4-rank of the tame kernel of the fields $E = \mathbb{Q}(\sqrt{pl}), \mathbb{Q}(\sqrt{2pl})$ and $F = \mathbb{Q}(\sqrt{-pl}), \mathbb{Q}(\sqrt{-2pl})$ where $p$ and $l$ are primes such that $p \equiv 7 \mod 8$, $l \equiv 1 \mod 8$ with $\left( \frac{l}{p} \right) = \left( \frac{p}{l} \right) = 1$. Let us use Theorem 2.44 to obtain $s$ and $t$ for our fields $E$ and $F$.

Let us first determine $s$. Let $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ where $a, b \in \mathbb{Q}$ and
\[ d = pl, 2pl, -pl, \text{ or } -2pl \] Then

\[ N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = a^2 - db^2. \]

We have 1 is a norm from \( \mathbb{Q}(\sqrt{d}) \) as 1 = \((1)^2 - d(0)^2\). Also, 2 is a norm from \( \mathbb{Q}(\sqrt{d}) \) as the equation 2 = \( a^2 - db^2 \) is solvable, e.g.

\[
\begin{align*}
2 &= (11)^2 - 7 \cdot 17(1)^2 \\
2 &= (108)^2 - 2 \cdot 7 \cdot 17(7)^2 \\
2 &= \left(\frac{3}{8}\right)^2 + 7 \cdot 17 \left(\frac{1}{8}\right)^2 \\
2 &= \left(\frac{10}{13}\right)^2 + 2 \cdot 7 \cdot 17 \left(\frac{1}{13}\right)^2.
\end{align*}
\]

In general where \( d \) is a squarefree positive integer, we can see that \(-1\) is not a norm from \( \mathbb{Q}(\sqrt{-d}) \) as the equation

\[-1 = a^2 + db^2\]

is not solvable for \( a, b \in \mathbb{Q} \). So in particular, \(-1\) is not a norm from \( \mathbb{Q}(\sqrt{-pl}) \) or \( \mathbb{Q}(\sqrt{-2pl}) \). Assume \(-1\) is a norm from \( \mathbb{Q}(\sqrt{pl}) \), i.e

\[-1 = a^2 - plb^2\]

is solvable for \( a, b \in \mathbb{Q} \). Let \( c \) be the gcd of the denominators of \( a \) and \( b \). Multiplying by \( c \) we have

\[-c^2 = r^2 - pls^2 \quad \text{or} \quad c^2 + r^2 = pls^2\]

where \( r, s \in \mathbb{Z} \). Now we recall the following.
Proposition 2.46. Let $n$ be a positive integer. Then $n$ is a sum of two squares of integers if and only if no prime $p \equiv 3 \mod 4$ appears in the unique prime factorization of $n$ with an odd exponent.

Since $p \equiv 7 \mod 8$ which implies $p \equiv 3 \mod 4$, Proposition 2.46 yields $plr^2$ is not the sum of two squares, a contradiction. By the same argument, $-1$ is not a norm from $\mathbb{Q}(\sqrt{2pl})$.

We can see that $-2$ is not a norm from $\mathbb{Q}(\sqrt{-pl})$ or $\mathbb{Q}(\sqrt{-2pl})$ as the equations

$$-2 = a^2 + plb^2, \quad -2 = a^2 + 2plb^2$$

are not solvable for $a, b \in \mathbb{Q}$. Assume $-2$ is a norm from $\mathbb{Q}(\sqrt{pl})$, i.e

$$-2 = a^2 - plb^2$$

is solvable for $a, b \in \mathbb{Q}$. Let $c$ be the gcd of the denominators of $a$ and $b$. Multiplying by $c$ we have

$$-2c^2 = x^2 - ply^2 \quad \text{or} \quad 2c^2 + x^2 = ply^2$$

where $x, y \in \mathbb{Z}$. Then $x^2 \equiv -2c^2 \mod p$. But $x^2 \equiv -2c^2 \mod p$ if and only if $(\frac{-2c^2}{p}) = (\frac{-2}{p}) = 1$ if and only if

(i) $(\frac{2}{p}) = 1$ and $(\frac{-1}{p}) = 1$ if and only if $p \equiv \pm 1 \mod 8$ and $p \equiv 1 \mod 4$ or

(ii) $(\frac{2}{p}) = -1$ and $(\frac{-1}{p}) = -1$ if and only if $p \equiv \pm 3 \mod 8$ and $p \equiv 3 \mod 4$

Since $p \equiv 7 \mod 8$, both (i) and (ii) lead to a contradiction. By the same argument, $-2$ is not a norm from $\mathbb{Q}(\sqrt{2pl})$. Thus $s = 1$.

Now, let us determine $t$. For $\mathbb{Q}(\sqrt{pl})$, we have $pl \equiv 7 \mod 8$ which implies $pl \equiv 3 \mod 4$ and so $d_{\mathbb{Q}(\sqrt{pl})} = 4pl$. Thus $t = 2$. 

31

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
For $\mathbb{Q}(\sqrt{-pl})$, $-pl \equiv 1 \mod 8$ which implies $-pl \equiv 1 \mod 4$ and so $d_{\mathbb{Q}(\sqrt{-pl})} = -pl$. Thus $t = 2$.

For $\mathbb{Q}(\sqrt{2pl})$, $2pl \equiv 6 \mod 8$ which implies $2pl \equiv 2 \mod 4$ and so $d_{\mathbb{Q}(\sqrt{2pl})} = 8pl$. Thus $t = 2$.

For $\mathbb{Q}(\sqrt{-2pl})$, $-2pl \equiv 2 \mod 8$ which implies $-2pl \equiv 2 \mod 4$ and so $d_{\mathbb{Q}(\sqrt{-2pl})} = -8pl$. Thus $t = 2$.

So for our fields $E$ and $F$, we have obtained

$$s = 1 \quad \text{and} \quad t = 2$$

and so

$$2\text{-rank } K_2(\mathcal{O}_E) = 3 \quad \text{and} \quad 2\text{-rank } K_2(\mathcal{O}_F) = 2.$$ 

Via [4] and the discussion in [7], we have $0 < 4\text{-rank } K_2(\mathcal{O}_E) < 2\text{-rank } K_2(\mathcal{O}_E)$ and so

$$4\text{-rank } K_2(\mathcal{O}_E) = 1 \quad \text{or} \quad 2.$$ 

For our fields $F$, compare Proposition 5.10 in [26] and Corollary 3.8 in [39] to see $4\text{-rank } K_2(\mathcal{O}_F) < 2\text{-rank } K_2(\mathcal{O}_F)$ and so

$$4\text{-rank } K_2(\mathcal{O}_F) = 0 \quad \text{or} \quad 1.$$ 

Before stating the characterizations of 4-ranks in positive definite terms, we need the following

**Definition 2.47.** For primes $p \equiv 7 \mod 8$, $l \equiv 1 \mod 8$ with $\left(\frac{l}{p}\right) = (\frac{p}{l}) = 1$, $\mathcal{K} = \mathbb{Q}(\sqrt{-2p})$, and $h(\mathcal{K})$ the class number of $\mathcal{K}$, we say:

1. satisfies $A^+$ if and only if $l = x^2 + 32y^2$ for some $x, y \in \mathbb{Z}$
2. satisfies $A^-$ if and only if $l \neq x^2 + 32y^2$ for all $x, y \in \mathbb{Z}$
l satisfies \( < 2, p > \) if and only if \( l^{\frac{A(K)}{4}} = 2n^2 + pm^2 \) for some \( n, m \in \mathbb{Z} \) with \( m \not\equiv 0 \mod l \)

l satisfies \( < 1, 2p > \) if and only if \( l^{\frac{A(K)}{4}} = n^2 + 2pm^2 \) for some \( n, m \in \mathbb{Z} \) with \( m \not\equiv 0 \mod l \).

We will see why the condition \( m \not\equiv 0 \mod l \) is necessary in Chapter 3. We can now state the main results from [7]. It should be pointed out that these characterizations are quite useful to us as they give information about the structure of the tame kernel by checking at most two positive definite binary quadratic forms. Let us repeat; results about the structure of a Milnor K-group, are obtained in terms of positive definite binary quadratic forms!

**Theorem 2.48.** Let \( p \equiv 7 \mod 8 \), \( l \equiv 1 \mod 8 \) with \( \left( \frac{l}{p} \right) = \left( \frac{p}{l} \right) = 1 \). If \( E = \mathbb{Q}(\sqrt{l}) \) then:

4-rank \( K_2(\mathcal{O}_E) = 1 \) if and only if \( l \) satisfies \( < 2, p > \);
4-rank \( K_2(\mathcal{O}_E) = 2 \) if and only if \( l \) satisfies \( < 1, 2p > \).

**Theorem 2.49.** Let \( p \equiv 7 \mod 8 \), \( l \equiv 1 \mod 8 \) with \( \left( \frac{l}{p} \right) = \left( \frac{p}{l} \right) = 1 \). If \( E = \mathbb{Q}(\sqrt{2pl}) \) with \( l \equiv 1 \mod 16 \), then:

4-rank \( K_2(\mathcal{O}_E) = 1 \) if and only if \( l \) satisfies \( < 2, p > \);
4-rank \( K_2(\mathcal{O}_E) = 2 \) if and only if \( l \) satisfies \( < 1, 2p > \).

If \( E = \mathbb{Q}(\sqrt{2pl}) \) with \( l \equiv 9 \mod 16 \), then:

4-rank \( K_2(\mathcal{O}_E) = 1 \) if and only if \( l \) satisfies \( < 1, 2p > \);
4-rank \( K_2(\mathcal{O}_E) = 2 \) if and only if \( l \) satisfies \( < 2, p > \).

**Theorem 2.50.** Let \( p \equiv 7 \mod 8 \), \( l \equiv 1 \mod 8 \) with \( \left( \frac{l}{p} \right) = \left( \frac{p}{l} \right) = 1 \). If \( F = \mathbb{Q}(\sqrt{-pl}) \) then:

4-rank \( K_2(\mathcal{O}_F) = 0 \) if and only if \( l \) satisfies \( (A^+ \text{ and } < 2, p >) \) or \( (A^- \text{ and } < 1, 2p >) \);
4-rank $K_2(\mathcal{O}_F) = 1$ if and only if $l$ satisfies $(A^+ \text{ and } < 1, 2p>)$ or $(A^- \text{ and } < 2, p>)$.

**Theorem 2.51.** Let $p \equiv 7 \text{ mod } 8$, $l \equiv 1 \text{ mod } 8$ with \((\frac{l}{p}) = (\frac{p}{l}) = 1\). If $F = \mathbb{Q}(\sqrt{-2pl})$ with $l \equiv 1 \text{ mod } 16$, then:

4-rank $K_2(\mathcal{O}_F) = 0$ if and only if $l$ satisfies $(A^+ \text{ and } < 2, p>)$ or $(A^- \text{ and } < 1, 2p>)$;

4-rank $K_2(\mathcal{O}_F) = 1$ if and only if $l$ satisfies $(A^+ \text{ and } < 1, 2p>)$ or $(A^- \text{ and } < 2, p>)$.

If $F = \mathbb{Q}(\sqrt{-2pl})$ with $l \equiv 9 \text{ mod } 16$, then:

4-rank $K_2(\mathcal{O}_F) = 0$ if and only if $l$ satisfies $(A^+ \text{ and } < 1, 2p>)$ or $(A^- \text{ and } < 2, p>)$;

4-rank $K_2(\mathcal{O}_F) = 1$ if and only if $l$ satisfies $(A^+ \text{ and } < 2, p>)$ or $(A^- \text{ and } < 1, 2p>)$.

The following corollary follows nicely from the four theorems above. Note that $|\cdot|$ denotes the classical (archimedean) absolute value.

**Corollary 2.52.** Let $E_1 = \mathbb{Q}(\sqrt{pl})$, $E_2 = \mathbb{Q}(\sqrt{2pl})$, $F_1 = \mathbb{Q}(\sqrt{-pl})$, $F_2 = \mathbb{Q}(\sqrt{-2pl})$.

If $l \equiv 1 \text{ mod } 16$, then

4-rank $K_2(\mathcal{O}_{E_1}) = 4$-rank $K_2(\mathcal{O}_{E_2})$;

4-rank $K_2(\mathcal{O}_{F_1}) = 4$-rank $K_2(\mathcal{O}_{F_2})$.

If $l \equiv 9 \text{ mod } 16$, then

$|4$-rank $K_2(\mathcal{O}_{E_1}) - 4$-rank $K_2(\mathcal{O}_{E_2})| = 1$;

$|4$-rank $K_2(\mathcal{O}_{F_1}) - 4$-rank $K_2(\mathcal{O}_{F_2})| = 1$.

**Example 2.53.** Let us illustrate Theorem 2.48. Fix $p = 7$ and $l = 5881$. We certainly have $p \equiv 7 \text{ mod } 8$ and $l \equiv 1 \text{ mod } 8$. Also \((\frac{5881}{7}) = 1\) as $5881 \equiv 1 \text{ mod } 7$. Let $E = \mathbb{Q}(\sqrt{7 \cdot 5881})$. We have $5881 = 2(33)^2 + 7(23)^2$ and so $5881$ satisfies $< 2, 7 >$. Thus 4-rank $K_2(\mathcal{O}_E) = 1$. 

34

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Take \( p = 7 \) and \( l = 2377 \). Once again \( p \equiv 7 \mod 8 \) and \( l \equiv 1 \mod 8 \). Also \( \left( \frac{2377}{7} \right) = 1 \) as \( 2377 \equiv 4 \mod 7 \). Let \( E = \mathbb{Q}(\sqrt{7 \cdot 2377}) \). Note that \( 2377 = (19)^2 + 2 \cdot 7(12)^2 \) and so \( 2377 \) satisfies \( < 1, 2 \cdot 7 > \). Thus \( 4\text{-rank } K_2(\mathcal{O}_E) = 2 \).

From Theorems 2.48, 2.49, 2.50, and 2.51, we can determine the 4-rank of the tame kernel for our fields \( E = \mathbb{Q}(\sqrt{pl}), \mathbb{Q}(\sqrt{2pl}), \) and \( F = \mathbb{Q}(\sqrt{-pl}), \mathbb{Q}(\sqrt{-2pl}) \). Let

\[
\begin{align*}
\nu &= 4\text{-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{pl})}) \quad , \quad \sigma = 4\text{-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-pl})}) \\
\mu &= 4\text{-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{2pl})}) \quad , \quad \tau = 4\text{-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-2pl})}).
\end{align*}
\]

Note that we have \( \nu, \mu = 1 \) or \( 2 \) while \( \sigma, \tau = 0 \) or \( 1 \). From Corollary 2.52, there are at most eight distinct tuples \((\nu, \mu, \sigma, \tau)\).

**Example 2.54.** Let \( p = 7 \). The primes \( l \equiv 1 \mod 8 \) with \( \left( \frac{l}{7} \right) = 1 \) are the primes \( l \equiv 1, 9, 25 \mod 56 \) via the Chinese Remainder Theorem. Here \( h(K) = 4 \) for \( K = \mathbb{Q}(\sqrt{-14}) \). All eight possible tuples \((\nu, \mu, \sigma, \tau)\) occur. To see this, here are the primes \( l \) that realize the indicted tuples \((\nu, \mu, \sigma, \tau)\).

<table>
<thead>
<tr>
<th>( l )</th>
<th>( \nu )</th>
<th>( \mu )</th>
<th>( \sigma )</th>
<th>( \tau )</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>193</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>137</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>233</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>617</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>457</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>449</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2129</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Let us explain for example the tuple \((2, 2, 1, 1)\) for the prime \( l = 2129 \). We have \( l \equiv 1 \mod 16 \) and \( 2129 = 27^2 + 2 \cdot 7 \cdot 10^2 \). So \( l \) satisfies \( < 1, 2 \cdot 7 > \). Thus by Theorem 2.48 with Theorem 2.49 or Corollary 2.52, it follows \( \nu = \mu = 2 \). Also, \( 2129 = 9^2 + 32 \cdot 8^2 \), so \( l \) satisfies \( A^+ \). Thus by Theorem 2.50 with Theorem 2.51 or Corollary 2.52, we have \( \sigma = \tau = 1 \).

To clarify further, let us also explain the tuple \((1, 2, 1, 0)\) for the prime \( l = 617 \).
We have $l \equiv 9 \mod 16$ and $617 = 2 \cdot 5^2 + 7 \cdot 9^2$. So $l$ satisfies $< 2, 7 >$. Thus by Theorem 2.48 with Theorem 2.49, we obtain $\nu = 1$ and $\mu = 2$. In addition, $l$ satisfies $A^-$ and so by Theorem 2.50 with Theorem 2.51, we have $\sigma = 1$ and $\tau = 0$.

We have defined what it means for a set of prime numbers to have a natural density in the last chapter. In this chapter, we relate certain prime numbers to 4-ranks, see Theorems 2.48, 2.49, 2.50, 2.51, and Corollary 2.52. Now, what is the connection between 4-ranks and densities? For motivation, let us consider the following example from [9].

**Example 2.55.** Let $q$ be a prime. The structure of the 2-Sylow subgroup of the tame kernel of the real quadratic fields $\mathbb{Q}(\sqrt{q})$ is given by:

\[
q = 2 : C_2 \times C_2 \\
q \equiv 3, 5 \mod 8 : C_2 \times C_2 \\
q \equiv 7 \mod 8 : C_2 \times C_{2^a} \quad \text{with} \quad a \geq 2 \\
q \equiv 1 \mod 8 : C_2 \times C_2 \times C_2 \quad \text{if} \quad q \quad \text{satisfies} \quad A^- \\
q \equiv 1 \mod 8 : C_2 \times C_2 \times C_2 \quad \text{with} \quad a \geq 2 \quad \text{if} \quad q \quad \text{satisfies} \quad A^+.
\]

In [9] it is proved that the sets $\{q \equiv 1 \mod 8 : q \text{ satisfies } A^+\}$ and $\{q \equiv 1 \mod 8 : q \text{ satisfies } A^-\}$ each have a density of $\frac{1}{2}$ in the set of all primes $q \equiv 1 \mod 8$. By Theorem 1.29, the subsets

\[
\{q : \text{the tame kernel of } \mathbb{Q}(\sqrt{q}) \text{ has 4-rank 0}\}
\]

\[
\{q : \text{the tame kernel of } \mathbb{Q}(\sqrt{q}) \text{ has 4-rank 1}\}
\]

have densities $\frac{1}{4} + \frac{1}{4} + \frac{1}{8} = \frac{5}{8}$ and $\frac{1}{4} + \frac{1}{8} = \frac{3}{8}$ respectively in the set of all primes $q$.

In the case of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-q})$, the structure of the
2-Sylow subgroup of the tame kernel is given by:

\[
q = 2 : \{1\}
\]
\[
q \equiv 3, 5 \mod 8 : \{1\}
\]
\[
q \equiv 7 \mod 8 : C_2
\]
\[
q \equiv 1 \mod 8 : C_{2^a} \quad \text{with} \quad a \geq 2.
\]

Here the subsets

\[
\{q : \text{the tame kernel of } \mathbb{Q}(\sqrt{-q}) \text{ has 4-rank 0}\}
\]

\[
\{q : \text{the tame kernel of } \mathbb{Q}(\sqrt{-q}) \text{ has 4-rank 1}\}
\]

have densities \(\frac{3}{4}\) and \(\frac{1}{4}\) respectively in the set of all primes \(q\).

Do similar density results appear for the quadratic fields considered in Theorems 2.48, 2.49, 2.50, and 2.51? Let us consider Theorem 2.48. Fix a prime \(p \equiv 7 \mod 8\) and let

\[
\Omega = \{l \text{ rational prime : } l \equiv 1 \mod 8 \text{ and } \left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) = 1\},
\]

\[
\Omega_1 = \{l \in \Omega : l \text{ satisfies } <2, p>\},
\]

\[
\Omega_2 = \{l \in \Omega : l \text{ satisfies } <1, 2p>\}.
\]

From Theorem 2.48 where \(E = \mathbb{Q}(\sqrt{p})\),

4-rank \(K_2(\mathcal{O}_E) = 1\) if and only if \(l \in \Omega_1\),

4-rank \(K_2(\mathcal{O}_E) = 2\) if and only if \(l \in \Omega_2\).
Result 2.56. We have computed the following: For \( p = 7 \), there are 9730 primes \( l \) in \( \Omega \) with \( l \leq 10^6 \). Among them, there are 4,866 primes (50.01\%) in \( \Omega_1 \) and 4,864 primes (49.99\%) in \( \Omega_2 \). This leads us to

**Question 2.57.** For the fields \( E = \mathbb{Q}(\sqrt{pl}) \) as in Theorem 2.48, do 4-rank 1 and 4-rank 2 each appear with natural density \( \frac{1}{2} \) in \( \Omega \)?

Based on Tables 1, 2, and 3 in Appendix 1, we can also ask

**Question 2.58.** For the fields \( \mathbb{Q}(\sqrt{2pl}) \), do 4-rank 1 and 2 each appear with natural density \( \frac{1}{2} \) in \( \Omega \)?

**Question 2.59.** For the fields \( \mathbb{Q}(\sqrt{-pl}) \), \( \mathbb{Q}(\sqrt{-2pl}) \), do 4-rank 0 and 1 each appear with natural density \( \frac{1}{2} \) in \( \Omega \)?

**Result 2.60.** For a fixed prime \( p \equiv 7 \mod 8 \) and \( l \in \Omega \) we considered in Example 2.54 the fields \( \mathbb{Q}(\sqrt{\pm pl}) \) and \( \mathbb{Q}(\sqrt{\pm 2pl}) \). The 4-ranks of their tame kernels are given by tuples \( (v, \mu, \sigma, \tau) \). For these fields we computed the following (see Table 4 in Appendix 1): For \( p = 7 \), among the 9730 primes \( l \in \Omega \) with \( l \leq 10^6 \), the eight possible cases are realized by 1215, 1213, 1228, 1210, 1210, 1228, 1225, 1201 primes \( l \) respectively. This result leads us to

**Question 2.61.** Do each of the eight possible tuples \( (v, \mu, \sigma, \tau) \) listed in Example 2.54 appear with natural density \( \frac{1}{8} \) in \( \Omega \)?

These questions will be the focus of the next chapter.
3. Main Results

3.1 Overview

We consider three degree eight field extensions of $\mathbb{Q}$. The idea will be to study composites of these fields and relate Artin symbols to 4-ranks. Rational primes which split completely in a degree 64 extension of $\mathbb{Q}$ will relate to Artin symbols and thus 4-ranks. Therefore calculating the density of these primes will answer density questions involving 4-ranks.

3.2 First Extension

To begin, consider $\mathbb{Q} (\sqrt{2})$ over $\mathbb{Q}$. Let $\epsilon = 1 + \sqrt{2} \in (\mathbb{Z}[\sqrt{2}])^*$. Then $\epsilon$ is a fundamental unit of $\mathbb{Q} (\sqrt{2})$ which has norm $-1$. Let $\mathcal{F} = \mathbb{Q} (\sqrt{2}, \sqrt{\epsilon})$. Then $\mathcal{F}$ has degree 4 over $\mathbb{Q}$. We claim that $\mathcal{F} = \mathbb{Q} (\sqrt{2} + \sqrt{\epsilon})$.

Lemma 3.62. $\mathcal{F} = \mathbb{Q} (\sqrt{2} + \sqrt{\epsilon})$.

Proof. Certainly, $\mathbb{Q} (\sqrt{2} + \sqrt{\epsilon}) \subset \mathbb{Q} (\sqrt{2}, \sqrt{\epsilon})$. For the field $\mathbb{Q} (\sqrt{2} + \sqrt{\epsilon})$, we have a $\mathbb{Q}$-basis: $1, \sqrt{2} + \sqrt{\epsilon}, (\sqrt{2} + \sqrt{\epsilon})^2, (\sqrt{2} + \sqrt{\epsilon})^3$. As

$$5\sqrt{\epsilon} = 2(\sqrt{2} + \sqrt{\epsilon})^3 - (\sqrt{2} + \sqrt{\epsilon})^2 - 9(\sqrt{2} + \sqrt{\epsilon}) - 9$$
we have $\sqrt{\varepsilon} \in \mathbb{Q}(\sqrt{2} + \sqrt{\varepsilon})$ and so $\sqrt{2} = (\sqrt{2} + \sqrt{\varepsilon}) - \sqrt{\varepsilon} \in \mathbb{Q}(\sqrt{2} + \sqrt{\varepsilon})$. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{\varepsilon})$. □

The minimal polynomial of $\sqrt{2} + \sqrt{\varepsilon}$ over $\mathbb{Q}$ is $f(x) = x^4 - 6x^2 - 8x - 1$. We have $f(x) = g(x)h(x)$ where

$$g(x) = x^2 - 2\sqrt{2}x + 1 - \sqrt{2}$$

and

$$h(x) = x^2 + 2\sqrt{2}x + 1 + \sqrt{2}.$$

Checking the discriminant of $h(x)$ yields that $h(x)$ has two nonreal roots. Thus $\mathcal{F}$ is not a splitting field for $f(x)$ over $\mathbb{Q}$ and so $\mathcal{F}$ is not normal over $\mathbb{Q}$. Since $\varepsilon \in \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon})$ has norm -1 and $\mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon}, \sqrt{-1})$ is a quadratic extension of $\mathcal{F}$, the normal closure of $\mathcal{F}$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon}, \sqrt{-1})$. Set

$$N_1 = \mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon}, \sqrt{-1}).$$

Then $N_1$ is Galois over $\mathbb{Q}$ and $[N_1 : \mathbb{Q}] = 8$. So $|\text{Gal}(N_1/\mathbb{Q})| = 8$. We claim that $\text{Gal}(N_1/\mathbb{Q})$ is the dihedral group of order 8.

**Proposition 3.63.** $\text{Gal}(N_1/\mathbb{Q}) \cong D_4$.

**Proof.** Let $\text{Gal}(N_1/\mathbb{Q}) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8\}$. Here are the automorphisms of $\text{Gal}(N_1/\mathbb{Q})$:
\[
\begin{array}{c|cccc|c}
\alpha_1 & \sqrt{-1} & \sqrt{2} & \sqrt{\epsilon} & \text{order} \\
\hline
\alpha_1 & + & + & + & 1 \\
\alpha_2 & + & + & - & 2 \\
\alpha_3 & + & - & \sqrt{\epsilon} & 2 \\
\alpha_4 & + & - & -\sqrt{\epsilon} & 2 \\
\alpha_5 & - & + & - & 2 \\
\alpha_6 & - & + & + & 2 \\
\alpha_7 & - & - & \sqrt{\epsilon} & 4 \\
\alpha_8 & - & - & -\sqrt{\epsilon} & 4 \\
\end{array}
\]

Here + and − denote for example \(\alpha_2(\sqrt{-1}) = \sqrt{-1}\) and \(\alpha_2(\sqrt{\epsilon}) = -\sqrt{\epsilon}\) respectively. Note that \(\alpha_1\) is the identity element of \(\text{Gal}(N_1/Q)\). Now consider the multiplication table for \(\text{Gal}(N_1/Q)\):

<table>
<thead>
<tr>
<th>\alpha_1</th>
<th>\alpha_2</th>
<th>\alpha_3</th>
<th>\alpha_4</th>
<th>\alpha_5</th>
<th>\alpha_6</th>
<th>\alpha_7</th>
<th>\alpha_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>\alpha_1</td>
<td>\alpha_1</td>
<td>\alpha_2</td>
<td>\alpha_3</td>
<td>\alpha_4</td>
<td>\alpha_5</td>
<td>\alpha_6</td>
<td>\alpha_7</td>
</tr>
<tr>
<td>\alpha_2</td>
<td>\alpha_2</td>
<td>\alpha_1</td>
<td>\alpha_4</td>
<td>\alpha_3</td>
<td>\alpha_6</td>
<td>\alpha_5</td>
<td>\alpha_8</td>
</tr>
<tr>
<td>\alpha_3</td>
<td>\alpha_3</td>
<td>\alpha_4</td>
<td>\alpha_1</td>
<td>\alpha_2</td>
<td>\alpha_8</td>
<td>\alpha_7</td>
<td>\alpha_6</td>
</tr>
<tr>
<td>\alpha_4</td>
<td>\alpha_4</td>
<td>\alpha_3</td>
<td>\alpha_2</td>
<td>\alpha_1</td>
<td>\alpha_7</td>
<td>\alpha_8</td>
<td>\alpha_6</td>
</tr>
<tr>
<td>\alpha_5</td>
<td>\alpha_5</td>
<td>\alpha_6</td>
<td>\alpha_7</td>
<td>\alpha_8</td>
<td>\alpha_1</td>
<td>\alpha_2</td>
<td>\alpha_3</td>
</tr>
<tr>
<td>\alpha_6</td>
<td>\alpha_6</td>
<td>\alpha_5</td>
<td>\alpha_8</td>
<td>\alpha_7</td>
<td>\alpha_2</td>
<td>\alpha_1</td>
<td>\alpha_4</td>
</tr>
<tr>
<td>\alpha_7</td>
<td>\alpha_7</td>
<td>\alpha_8</td>
<td>\alpha_5</td>
<td>\alpha_6</td>
<td>\alpha_4</td>
<td>\alpha_3</td>
<td>\alpha_1</td>
</tr>
<tr>
<td>\alpha_8</td>
<td>\alpha_8</td>
<td>\alpha_7</td>
<td>\alpha_6</td>
<td>\alpha_5</td>
<td>\alpha_4</td>
<td>\alpha_3</td>
<td>\alpha_2</td>
</tr>
</tbody>
</table>

Here for example \(\alpha_5\alpha_3 = \alpha_7\). We note that \(\text{Gal}(N_1/Q)\) is generated by \(\alpha_3\) and \(\alpha_7\) as \(\alpha_1 = \alpha_3^2, \alpha_2 = \alpha_7^2, \alpha_4 = \alpha_3\alpha_7, \alpha_5 = \alpha_7\alpha_3, \alpha_6 = \alpha_3\alpha_7, \) and \(\alpha_8 = \alpha_7^3\). Also, \(\alpha_3\) has order 2 and \(\alpha_7\) has order 4. From [25], we need only show \(\alpha_3\alpha_7 = \alpha_7^{-1}\alpha_3\) and \(\alpha_7^k \neq \alpha_1\) for \(k = 1, 2,\) or \(3\). From the multiplication table, \(\alpha_3\alpha_7 = \alpha_6 = \alpha_6\alpha_3 = \alpha_7^{-1}\alpha_3\) and \(\alpha_7^2 = \alpha_2, \alpha_7^3 = \alpha_8\). Thus \(\text{Gal}(N_1/Q) \cong D_4\).

Note that \(\alpha_1\) and \(\alpha_2\) from the proof of Proposition 3.63 commute with every element of \(\text{Gal}(N_1/Q)\) and \(\text{Gal}(N_1/Q(\sqrt{2}, \sqrt{-1})) = \{\alpha_1, \alpha_2\}\). Combining this statement with example 11 from [14], it follows

**Corollary 3.64.** \(Z(\text{Gal}(N_1/Q)) \cong C_2 = \{\alpha_1, \alpha_2\} = \text{Gal}(N_1/Q(\sqrt{2}, \sqrt{-1}))\).

41
Recall from Chapter 2, $\Omega = \{l$ rational prime : $l \equiv 1 \mod 8$ and $(\frac{l}{p}) = 1\}$ for a fixed prime $p \equiv 7 \mod 8$. In order to discuss the Artin symbol $\left( \frac{N_1/Q}{l} \right)$, we must first know that the primes $l \in \Omega$ are unramified in $N_1$ over $\mathbb{Q}$.

**Proposition 3.65.** If $l \in \Omega$, then $l$ is unramified in $N_1$.

**Proof.** For an odd prime $l$ and $K$ a quadratic field of discriminant $d_K$, we have from Proposition 1.13 (ii) if $(\frac{d_K}{l}) = 1$, then $l$ splits completely in $K$. For $l \in \Omega$, $l$ splits completely in $\mathbb{Q}(\sqrt{2})$ as

$$\left( \frac{d_{\mathbb{Q}(\sqrt{2})}}{l} \right) = \left( \frac{8}{l} \right) = \left( \frac{2}{l} \right) = 1.$$  

In particular for $l \in \Omega$, $l$ is unramified in $\mathbb{Q}(\sqrt{2})$. For $l \in \Omega$, $l$ splits completely in $\mathbb{Q}(\sqrt{-1})$ as

$$\left( \frac{d_{\mathbb{Q}(\sqrt{-1})}}{l} \right) = \left( \frac{-4}{l} \right) = \left( \frac{-1}{l} \right) = 1.$$  

In particular for $l \in \Omega$, $l$ is unramified in $\mathbb{Q}(\sqrt{-1})$. By Theorem 1.9, for $l \in \Omega$, $l$ is unramified in the composite field $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$.

To see that $l$ is unramified in $\mathbb{Q}(\sqrt{\bar{\varepsilon}})$, we compute the discriminant for the minimal polynomial of $\sqrt{\bar{\varepsilon}}$ over $\mathbb{Q}$. The minimal polynomial of $\sqrt{\bar{\varepsilon}}$ over $\mathbb{Q}$ is $x^4 - 2x^2 - 1$ which has roots $\alpha_1 = \sqrt{\bar{\varepsilon}}, \alpha_2 = -\sqrt{\bar{\varepsilon}}, \alpha_3 = \sqrt{\bar{\varepsilon}},$ and $\alpha_4 = -\sqrt{\bar{\varepsilon}}$ where $\bar{\varepsilon} = 1 - \sqrt{2}$. Now,

$$D_{\mathbb{Q}(\sqrt{\bar{\varepsilon}})/\mathbb{Q}(\sqrt{\varepsilon})} = \prod_{i>j} (\alpha_i - \alpha_j)^2$$  

$$= (\alpha_4 - \alpha_3)^2(\alpha_4 - \alpha_2)^2(\alpha_4 - \alpha_1)^2(\alpha_3 - \alpha_2)^2(\alpha_3 - \alpha_1)^2(\alpha_2 - \alpha_1)^2$$  

$$= (4\bar{\varepsilon})(4\varepsilon)(2 - 2i)^2(2 + 2i)^2$$  

$$= -1024$$  

$$= -2^{10}.$$  

42

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Thus no odd prime divides $D_{Q(\sqrt{\varepsilon})/Q(\sqrt{\varepsilon})}$. This implies that no odd prime divides the field discriminant of $Q(\sqrt{\varepsilon})$ over $Q$, denoted by $\Delta(Q(\sqrt{\varepsilon}))$. Recall that an odd prime $p$ is unramified in a number field $F$ if and only if $p \nmid \Delta(F)$. Thus every odd rational prime is unramified in $Q(\sqrt{\varepsilon})$. In particular, $l$ is unramified in $Q(\sqrt{\varepsilon})$. By Theorem 1.9, $l$ is unramified in the composite field $N_1 = Q(\sqrt{2}, \sqrt{\varepsilon}, \sqrt{-1})$. □

Now as $l \in \Omega$ is unramified in $N_1$, the Artin symbol $\left(\frac{N_1/Q}{l}\right)$ is defined for primes $\beta$ of $O_{N_1}$ containing $l$ by Lemma 1.20. Let $\left(\frac{N_1/Q}{l}\right)$ denote the conjugacy class of $\left(\frac{N_1/Q}{l}\right)$ in $Gal(N_1/Q)$. From the arguments in the proof of Proposition 3.65, the primes $l \in \Omega$ split completely in $Q(\sqrt{2}, \sqrt{-1})$. Also,

$$Z(Gal(N_1/Q))' = Gal(N_1/Q(\sqrt{2}, \sqrt{-1}))' = Q(\sqrt{2}, \sqrt{-1})$$

where $G'$ denotes the fixed field of a group $G$. To clarify, we have the following diagram:

$$\begin{array}{ccc}
N_1 & \{1\} & \\
| & | & \\
Q(\sqrt{2}, \sqrt{-1}) & \leftrightarrow & Z(Gal(N_1/Q)) \\
| & | & \\
Q & Gal(N_1/Q). & \\
\end{array}$$

By Lemma 1.26, we have

**Remark 3.66.** For some $g \in Gal(N_1/Q)$, $\left(\frac{N_1/Q}{l}\right) = \{g\} \subset Z(Gal(N_1/Q))$.

Since the conjugacy class consists of a single element, we may identify $\left(\frac{N_1/Q}{l}\right)$ with the automorphism $g$ of $Z(Gal(N_1/Q))$. As $Z(Gal(N_1/Q))$ has order 2, there are two possible choices for $\left(\frac{N_1/Q}{l}\right)$.

From [7], Addendum (3.7), there is a nice way to characterize primes $l \in \Omega$ which are split completely in $N_1$ over $Q$. 

43
Proposition 3.67. \( l \) is split completely in \( N_1 \) over \( \mathbb{Q} \) if and only if \( l \) satisfies \( < 1, 32 > \).

Combining Remark 3.66 with Proposition 3.67, we have

\[
\left( \frac{N_1/Q}{l} \right) = \{id\} \iff l \text{ splits completely in } N_1 \iff l \text{ satisfies } < 1, 32 >.
\]

\[
\left( \frac{N_1/Q}{l} \right) \neq \{id\} \iff l \text{ does not split completely in } N_1 \iff l \text{ does not satisfy } < 1, 32 >.
\]

### 3.3 Second Extension

Consider the fixed prime \( p \equiv 7 \mod 8 \). Note \( p \) splits completely in \( \mathcal{L} = \mathbb{Q}(\sqrt{2}) \) as

\[
\left( \frac{d_{\mathcal{L}}}{p} \right) = \left( \frac{8}{p} \right) = \left( \frac{2}{p} \right) = 1.
\]

So

\[ p\mathcal{O}_\mathcal{L} = \mathfrak{P}\mathfrak{P}' \]

for some primes \( \mathfrak{P} \neq \mathfrak{P}' \) in \( \mathcal{L} \). Note the field \( \mathcal{L} \) has narrow class number \( h^+(\mathcal{L}) = 1 \) as \( h(\mathcal{L}) = 1 \) and \( N_{\mathcal{L}/\mathbb{Q}}(\epsilon) = -1 \) where \( \epsilon = 1 + \sqrt{2} \) is a fundamental unit of \( \mathbb{Q}(\sqrt{2}) \), see [29]. From [7],

**Lemma 3.68.** The prime \( \mathfrak{P} \) which occurs in the decomposition of \( p\mathcal{O}_\mathcal{L} \) has a generator \( \pi = a + b\sqrt{2} \in \mathcal{O}_\mathcal{L} \), unique up to multiplication by the square of a unit in \( \mathcal{O}_\mathcal{L} \) for which \( N_{\mathcal{L}/\mathbb{Q}}(\pi) = a^2 - 2b^2 = -p \).

The degree 4 extension \( \mathbb{Q}(\sqrt{2}, \sqrt{\pi}) \) over \( \mathbb{Q} \) has normal closure \( \mathbb{Q}(\sqrt{2}, \sqrt{\pi}, \sqrt{-p}) \) as \( N_{\mathcal{L}/\mathbb{Q}}(\pi) = -p \). Set

\[ N_2 = \mathbb{Q}(\sqrt{2}, \sqrt{\pi}, \sqrt{-p}). \]
Then $N_2$ is Galois over $\mathbb{Q}$ and $[N_2 : \mathbb{Q}] = 8$. Let us note that such an extension $N_2$ exists since the 2-Sylow subgroup of the ideal class group of $\mathbb{Q}(\sqrt{-2p})$ is cyclic of order divisible by 4 [9]. Thus the Hilbert class field of $\mathbb{Q}(\sqrt{-2p})$ contains a unique unramified cyclic degree 4 extension over $\mathbb{Q}(\sqrt{-2p})$. Also compare [30]. Similar to the proof of Proposition 3.63, $\text{Gal}(N_2/\mathbb{Q})$ is the dihedral group of order 8.

**Proposition 3.69.** $\text{Gal}(N_2/\mathbb{Q}) \cong D_4$

Note that the identity automorphism and the automorphism $\beta$ induced by sending $\sqrt{\pi} \rightarrow -\sqrt{\pi}$ commutes with every element of $\text{Gal}(N_2/\mathbb{Q})$. Also

$$\text{Gal}(N_2/\mathbb{Q}(\sqrt{2}, \sqrt{-p})) = \{id, \beta\}.$$ 

Thus

**Corollary 3.70.** $Z(\text{Gal}(N_2/\mathbb{Q})) \cong C_2 = \{id, \beta\} = \text{Gal}(N_2/\mathbb{Q}(\sqrt{2}, \sqrt{-p}))$.

In order to discuss $(N_2/\mathbb{Q})_l$, we must know that the primes $l \in \Omega$ are unramified in $N_2$ over $\mathbb{Q}$. We will use from [7],

**Lemma 3.71.** $N_2$ is the unique unramified cyclic degree 4 extension over $\mathbb{Q}(\sqrt{-2p})$.

**Proposition 3.72.** If $l \in \Omega$, then $l$ is unramified in $N_2$ over $\mathbb{Q}$.

**Proof.** We first claim that $l$ is unramified in $\mathbb{Q}(\sqrt{-2p})$. Note that $p \equiv 7 \text{ mod } 8$ if and only if $-p \equiv 1 \text{ mod } 8$ if and only if $-2p \equiv 2 \text{ mod } 8$. Thus the discriminant of $\mathbb{Q}(\sqrt{-2p})$ is $-8p$. By Proposition 1.13 (ii) if $(-2p) = 1$, then $l$ splits completely in $\mathbb{Q}(\sqrt{-2p})$. Now $(-2p) = 1$ if and only if

(i) $\left(\frac{2}{l}\right) = 1$, $\left(\frac{-1}{l}\right) = 1$, $\left(\frac{\pi}{l}\right) = 1$ or

(ii) $\left(\frac{2}{l}\right) = 1$, $\left(\frac{-1}{l}\right) = -1$, $\left(\frac{\pi}{l}\right) = -1$ or

(iii) $\left(\frac{2}{l}\right) = -1$, $\left(\frac{-1}{l}\right) = -1$, $\left(\frac{\pi}{l}\right) = 1$ or

(iv) $\left(\frac{2}{l}\right) = -1$, $\left(\frac{-1}{l}\right) = 1$, $\left(\frac{\pi}{l}\right) = -1$
Cases (ii) and (iv) are not applicable since we are considering \( l \in \Omega \) i.e. \( \left( \frac{l}{p} \right) = \left( \frac{p}{l} \right) = 1 \). Case (iii) occurs if and only if \( l \equiv \pm 3 \mod 8 \) and \( \left( \frac{p}{l} \right) = 1 \). Once again for \( l \in \Omega \), this case is not necessary. Since \( l \in \Omega \) satisfies the conditions of case (i), \( l \) splits completely in \( \mathbb{Q}(\sqrt{-2p}) \). In particular \( l \) is unramified in \( \mathbb{Q}(\sqrt{-2p}) \). By Lemma 3.71, \( l \) is unramified in \( N_2 = \mathbb{Q}(\sqrt{2}, \sqrt{-2p}) \).

\( \square \)

As \( l \in \Omega \) is unramified in \( N_2 \) over \( \mathbb{Q} \), the Artin symbol \( \left( \frac{N_2/\mathbb{Q}}{l} \right) \) is defined for primes \( \beta \) of \( \mathcal{O}_{N_2} \) containing \( l \). Let \( \left( \frac{N_2/\mathbb{Q}}{l} \right) \) denote the conjugacy class of \( \left( \frac{N_2/\mathbb{Q}}{l} \right) \) in \( \text{Gal}(N_2/\mathbb{Q}) \). For \( l \in \Omega \), \( l \) splits completely in \( \mathbb{Q}(\sqrt{2}) \) (see proof of Proposition 3.65). Similarly for \( l \in \Omega \), \( l \) splits completely in \( \mathbb{Q}(\sqrt{-p}) \) as

\[
\left( \frac{\sqrt{-p}}{l} \right) = \left( \frac{-p}{l} \right) = \left( \frac{-1}{l} \right) \left( \frac{p}{l} \right) = 1.
\]

By Theorem 1.9, \( l \) splits completely in the composite field \( \mathbb{Q}(\sqrt{2}, \sqrt{-p}) \). But from Corollary 3.70,

\[
Z(\text{Gal}(N_2/\mathbb{Q})) = \text{Gal}(N_2/\mathbb{Q}(\sqrt{2}, \sqrt{-p})) = \mathbb{Q}(\sqrt{2}, \sqrt{-p}).
\]

Once again, to clarify we have the following diagram:

\[
\begin{array}{ccc}
N_2 & \{1\} & \text{Gal}(N_2/\mathbb{Q}), \quad \left( \frac{N_2/\mathbb{Q}}{l} \right) = \{h\} \subset Z(\text{Gal}(N_2/\mathbb{Q})). \\
| & \downarrow & \\
\mathbb{Q}(\sqrt{2}, \sqrt{-p}) & \longleftrightarrow & Z(\text{Gal}(N_2/\mathbb{Q})) \\
| & \downarrow & \\
\mathbb{Q} & \text{Gal}(N_2/\mathbb{Q}). & \\
\end{array}
\]

So by Lemma 1.26,

**Remark 3.73.** For some \( h \in \text{Gal}(N_2/\mathbb{Q}) \), \( \left( \frac{N_2/\mathbb{Q}}{l} \right) = \{h\} \subset Z(\text{Gal}(N_2/\mathbb{Q})) \).

46
Once again we can identify \( (N_2/Q) \) with the automorphism \( h \) of \( Z(\text{Gal}(N_2/Q)) \). As \( Z(\text{Gal}(N_2/Q)) \) has order 2, there are two possible choices for \( (N_2/Q) \).

Let us now characterize primes \( l \in \Omega \) which split completely in \( N_2 \). Set \( K = \mathbb{Q}(\sqrt{-2p}) \) for some prime \( p \equiv 7 \mod 8 \). By Lemma 3.71, \( N_2 \) is the unique unramified cyclic degree 4 extension of \( K \). We have seen that the primes \( l \in \Omega \) split completely in \( \mathbb{Q}(\sqrt{2}, \sqrt{-p}) \). Let us now characterize primes \( l \in \Omega \) that split completely in \( N_2 \).

Let \( D \) be the unique dyadic prime in \( \mathcal{O}_K = \mathbb{Z}[\sqrt{-2p}] \). If \( D \) is a principal ideal of \( \mathcal{O}_K \), i.e. has a generator \( n + m\sqrt{-2p} \in \mathcal{O}_K \), then

\[
    n^2 + 2pm^2 = 2 \quad \text{with } n, m \in \mathbb{Z},
\]

a contradiction. Thus \( D \) is not a principal ideal of \( \mathcal{O}_K \). Denote the class of \( D \) in \( C(K) \) by \([D]\). Thus \([D] \neq 1 \) in \( C(K) \). Because \( D^2 = 2\mathcal{O}_K \), we have

\[
    [D] \neq 1 \quad \text{and} \quad [D]^2 = 1 \quad \text{in } C(K).
\]

So \([D]\) is the unique element of order 2 in \( C(K) \). Now let \( H \) denote the Hilbert class field of \( K \), that is the maximal unramified Abelian extension of \( K \). Thus we have the tower of fields:

\[
\begin{align*}
    &H \\
    &| \\
    &N_2 \\
    &| \\
    &\mathbb{Q}(\sqrt{2}, \sqrt{-p}) \\
    &| \\
    &K.
\end{align*}
\]
By the Artin reciprocity theorem for Hilbert class fields, the ideal class group of $K$ is canonically isomorphic to the Galois group of $H$ over $K$:

$$C(K) \cong \text{Gal}(H/K).$$

Note there is an epimorphism $\text{Gal}(H/K) \to \text{Gal}(N_2/K)$ and by Lemma 3.71 $\text{Gal}(N_2/K)$ is cyclic of order 4. Let $C(K)^4$ be the set of all elements in $C(K)$ which are fourth powers, i.e.

$$C(K)^4 = \{[\alpha] \in C(K) : [\alpha] = [\gamma]^4 \text{ for some } [\gamma] \in C(K)\}.$$

By Corollaries 18.4, 18.6, and 19.6 in [9], 2-Sylow $C(K)$ is cyclic of order divisible by 4 and so $C(K)^4$ is the unique subgroup of $C(K)$ of index 4. Thus

$$C(K)/C(K)^4 \cong \text{Gal}(N_2/K).$$

Similarly,

$$C(K)/C(K)^2 \cong \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{-p})/K).$$

Now the endomorphisms $C(K) \to C(K)$ given by

$$c \mapsto c^{\frac{N(K)}{4}}$$

and

$$c \mapsto c^{\frac{N(K)}{2}}$$

have kernel $C(K)^4$ and $C(K)^2$. Note that the image is given by the unique cyclic subgroups of $C(K)$ of order 4 and 2 respectively.

Now let $p$ be a prime ideal of $\mathcal{O}_K$. By Corollary 1.21 (iii), $p$ splits completely.
in $N_2$ over $K$ if and only if $\left( \frac{N_2}{K} \right) = \text{Id}_{\text{Gal}(N_2/K)}$. Since the Artin map induces an isomorphism $C(K)/C(K)^4 \cong \text{Gal}(N_2/K)$, we see that $p$ determines the trivial class of $C(K)/C(K)^4$. Thus $[p] \in C(K)^4$ if and only if $[p]^{\frac{\Lambda(K)}{4}} = 1$. Similarly, $p$ splits completely in $\mathbb{Q}(\sqrt{2}, \sqrt{-p})$ over $K$ if and only if $\left( \frac{\mathbb{Q}(\sqrt{2}, \sqrt{-p})}{p} \right) = \text{Id}_{\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{-p})/K)}$. Thus $p$ determines the trivial class of $C(K)/C(K)^2$. So $[p] \in C(K)^2$ if and only if $[p]^{\frac{\Lambda(K)}{2}} = [\mathfrak{O}] \neq 1$ or $[p]^{\frac{\Lambda(K)}{4}} = 1$ in $C(K)$. So we have shown

**Lemma 3.74.** Let $p$ be a prime ideal of $\mathcal{O}_K$. Then:

- $p$ is split completely in $N_2$ over $K$ if and only if $[p]^{\frac{\Lambda(K)}{4}} = 1$ in $C(K)$.
- $p$ is split completely in $\mathbb{Q}(\sqrt{2}, \sqrt{-p})$ over $K$ if and only if $[p]^{\frac{\Lambda(K)}{2}} = 1$ in $C(K)$ if and only if $[p]^{\frac{\Lambda(K)}{4}} = [\mathfrak{O}] \neq 1$ or $[p]^{\frac{\Lambda(K)}{4}} = 1$ in $C(K)$.

For $l \in \Omega$, we have $l\mathcal{O}_K = p_1p_2$ where $p_1$ and $p_2$ are a pair of conjugate prime ideals in $\mathcal{O}_K$. As $l$ splits completely in $\mathbb{Q}(\sqrt{2}, \sqrt{-p})$, $p_1$ splits completely in $\mathbb{Q}(\sqrt{2}, \sqrt{-p})$ over $K$ and so by Lemma 3.74,

$$[p_1]^{\frac{\Lambda(K)}{4}} = 1 \text{ or } [p_1]^{\frac{\Lambda(K)}{4}} = [\mathfrak{O}] \neq 1 \text{ in } C(K).$$

**Lemma 3.75.** For $l \in \Omega$, let $l\mathcal{O}_K = p_1p_2$. Then:

- $l$ splits completely in $N_2$ if and only if $p_1$ splits completely in $N_2$ over $K$ if and only if $[p_1]^{\frac{\Lambda(K)}{4}} = 1$ in $C(K)$.
- $l$ does not split completely in $N_2$ if and only if $[p]^{\frac{\Lambda(K)}{4}} = [\mathfrak{O}] \neq 1$ in $C(K)$.

Using Lemmas 3.74 and 3.75, we now characterize primes $l \in \Omega$ which split completely in $N_2$ in terms of positive definite quadratic forms.

**Lemma 3.76.** Let $l \in \Omega$. Then $l$ splits completely in $N_2$ if and only if $l^{\frac{\Lambda(K)}{4}} = n^2 + 2pm^2$ for $n, m \in \mathbb{Z}$ with $m \not\equiv 0 \text{ mod } l$. 

49

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Proof. We follow [7]. Suppose \( l \) splits completely in \( N_2 \). By Lemma 3.75, \( p_1 \) splits completely in \( N_2 \) over \( K \) and so \( [p_1]^{\frac{h(K)}{4}} = 1 \) in \( \text{C}(K) \). Thus \( p_1^{\frac{h(K)}{4}} \) is a principal ideal of \( \mathcal{O}_K \), i.e, \( p_1^{\frac{h(K)}{4}} \) has a generator \( \sigma = n + m\sqrt{-2p} \), with ramification indices, \( e_{p_1|\sigma} = \frac{h(K)}{4} \) and \( e_{p|\sigma} = 0 \) for all prime ideals \( p \subset \mathcal{O}_K, p \neq p_1 \).

Recall that \( l\mathcal{O}_K = p_1p_2 \) and so taking norms, we have

\[
N_{K/Q}(\sigma) = n^2 + 2pm^2 = l^{\frac{h(K)}{4}}
\]

with \( n, m \in \mathbb{Z} \). Let us now justify the condition \( m \not\equiv 0 \mod l \). Suppose \( m \equiv 0 \mod l \) and so \( n \equiv 0 \mod l \). Then \( \eta = \frac{m}{l} + \frac{n}{l}\sqrt{-2p} \in \mathcal{O}_K \) and \( \sigma = l\eta \). Thus \( e_{p_2|\sigma} = e_{p_2|l} + e_{p_2|\eta} = 1 + e_{p_2|\eta} \geq 1 \), contradicting \( e_{p_2|\sigma} = 0 \).

Conversely, let \( l^{\frac{h(K)}{4}} = n^2 + 2pm^2 \) for some \( n, m \in \mathbb{Z} \) with \( m \not\equiv 0 \mod l \). Thus \( \sigma = n + m\sqrt{-2p} \in \mathcal{O}_K \) and \( N_{K/Q}(\sigma) = l^{\frac{h(K)}{4}} \). As \( l\mathcal{O}_K = p_1p_2 \), we have \( e_{p_1|\sigma} + e_{p_2|\sigma} = \frac{h(K)}{4} \) and \( e_{p|\sigma} = 0 \) for all prime ideals \( p \subset \mathcal{O}_K, p \neq p_1, p_2 \). Assume that \( e_{p_1|\sigma} > 0 \) and \( e_{p_2|\sigma} > 0 \). Thus \( l \) divides \( \sigma \) and so

\[
\sigma = n + \frac{m}{l}\sqrt{-2p} \in \mathcal{O}_K.
\]

Therefore \( \frac{m}{l} \in \mathbb{Z} \), contradicting \( m \not\equiv 0 \mod l \). Without loss of generality, let \( e_{p_1|\sigma} = \frac{h(K)}{4} \) and \( e_{p_2|\sigma} = 0 \). Thus \( \sigma \) generates \( p_1^{\frac{h(K)}{4}} \), i.e, \( [p_1]^{\frac{h(K)}{4}} = 1 \) in \( \text{C}(K) \). By Lemma 3.75, \( l \) splits completely in \( N_2 \).

\[\square\]

Lemma 3.77. Let \( l \in \Omega \). Then \( l \) does not split completely in \( N_2 \) if and only if \( l^{h(K)/4} = 2n^2 + pm^2 \) for \( n, m \in \mathbb{Z} \) with \( m \not\equiv 0 \mod l \).

Proof. We follow [7]. Suppose \( l \) is does split completely in \( N_2 \). By Lemma 3.75,
[\mathfrak{p}_1]^{\frac{h(K)}{4}} = [\mathfrak{D}] \text{ in } C(K). \text{ Since }

[\mathfrak{D}][\mathfrak{p}_1]^{\frac{h(K)}{4}} = [\mathfrak{D}]^2 = 1 \text{ in } C(K),

we have that \mathfrak{D}p^{\frac{h(K)}{4}} \text{ is a principal ideal of } \mathcal{O}_K. \text{ Thus } \mathfrak{D}p^{\frac{h(K)}{4}} \text{ has a generator } 

\sigma = r + m\sqrt{-2p} \in \mathcal{O}_K \text{ with ramification indices } e_{\mathfrak{D}|\sigma} = 1, \ e_{\mathfrak{p}_1|\sigma} = \frac{h(K)}{4}, \text{ and } 

e_{\mathfrak{p}_2|\sigma} = 0 \text{ for all prime ideals } \mathfrak{p} \subset \mathcal{O}_K, \mathfrak{p} \neq \mathfrak{D}, \mathfrak{p}_1. \text{ Taking norms we have }

N_{K/Q}(\sigma) = r^2 + 2pm^2 = 2l^{\frac{h(K)}{4}}

with \( m \neq 0 \mod l \) (as in proof of Lemma 3.76). As \( r \) is even, we set \( r = 2n \) for \( n \in \mathbb{Z} \) and so \( l^{\frac{h(K)}{4}} = 2n^2 + pm^2 \) for \( n, m \in \mathbb{Z} \) with \( m \neq 0 \mod l \).

Conversely, let \( l^{\frac{h(K)}{4}} = 2n^2 + pm^2 \) for \( n, m \in \mathbb{Z} \) with \( m \neq 0 \mod l \). Then

\( 2l^{\frac{h(K)}{4}} = (2n)^2 + 2pm^2 \) and so \( \sigma = 2n + m\sqrt{-2p} \in \mathcal{O}_K \) satisfies \( N_{K/Q}(\sigma) = 2l^{\frac{h(K)}{4}} \) with \( e_{\mathfrak{D}|\sigma} = 1, \ e_{\mathfrak{p}_1|\sigma} + e_{\mathfrak{p}_2|\sigma} = \frac{h(K)}{4}, \) and \( e_{\mathfrak{p}|\sigma} = 0 \) for all prime ideals \( \mathfrak{p} \subset \mathcal{O}_K, \mathfrak{p} \neq \mathfrak{D}, \mathfrak{p}_1, \mathfrak{p}_2. \) As in the proof of Lemma 3.76, we have without loss of generality that \( e_{\mathfrak{p}_1|\sigma} = \frac{h(K)}{4} \) and \( e_{\mathfrak{p}_2|\sigma} = 0. \) Thus \( \sigma \) generates \( \mathfrak{D}p_1^{\frac{h(K)}{4}}, \) i.e., \([p_1]^{\frac{h(K)}{4}} = [\mathfrak{D}] \) in \( C(K). \)

By Lemma 3.75, \( l \) does not split completely in \( N_2. \)

\[ \square \]

By Definition 2.47, we reformulate Lemma 3.76 and 3.77 as follows:

\( l \) splits completely in \( N_2 \Leftrightarrow l \) satisfies \( < 1, 2p > \)

\( l \) does not split completely in \( N_2 \Leftrightarrow l \) satisfies \( < 2, p > . \)

51
Combining Remark 3.73 and the above reformulation,

\[
\left( \frac{N_2/Q}{l} \right) = \{id\} \iff l \text{ splits completely in } N_2
\]

\[\iff l \text{ satisfies } <1, 2p>.
\]

\[
\left( \frac{N_2/Q}{l} \right) \neq \{id\} \iff l \text{ does not split completely in } N_2
\]

\[\iff l \text{ satisfies } <2, p>.
\]

### 3.4 Third Extension

Let us recall a general fact about cyclotomic extensions of \( \mathbb{Q} \), compare [28] or [13]. For \( \mathbb{Q}(\zeta_m) \) with \( m \) a positive integer and \( p \) a rational prime,

\[ p \text{ splits completely in } \mathbb{Q}(\zeta_m) \iff p \equiv 1 \text{ mod } m. \]

For \( l \equiv 1 \text{ mod } 8 \), we have \( l \equiv 1, 9 \text{ mod } 16 \). Thus for \( l \in \Omega \),

\[ l \text{ splits completely in } \mathbb{Q}(\zeta_{16}) \iff l \equiv 1 \text{ mod } 16 \]

\[ l \text{ does not split completely in } \mathbb{Q}(\zeta_{16}) \iff l \equiv 9 \text{ mod } 16. \]

Now as \( \text{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})) \cong (\mathbb{Z}/16\mathbb{Z})^* \), we know for \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})) \)

\[ l \equiv 1 \text{ mod } 16 \iff \sigma(\zeta_{16}) = \zeta_{16} \]

\[ l \equiv 9 \text{ mod } 16 \iff \sigma(\zeta_{16}) = \zeta_{16}^9 = -\zeta_{16}. \]

These statements yield
Remark 3.78.

\[
\left( \frac{\mathbb{Q}(\zeta_{16})/\mathbb{Q}}{l} \right) = \{id\} \iff l \text{ splits completely in } \mathbb{Q}(\zeta_{16}) \iff l \equiv 1 \mod 16
\]

\[
\left( \frac{\mathbb{Q}(\zeta_{16})/\mathbb{Q}}{l} \right) \neq \{id\} \iff l \text{ does not split completely in } \mathbb{Q}(\zeta_{16}) \iff l \equiv 9 \mod 16
\]

3.5 The Composite

In this section we consider the composite field \(N_1 N_2 \mathbb{Q}(\zeta_{16})\). First note that as \(N_1\) and \(N_2\) are normal extensions of \(\mathbb{Q}\), then the composite field \(N_1 N_2\) is a normal extension of \(\mathbb{Q}\). Set \(\mathcal{G} = \mathbb{Q}(\sqrt{2})\). Then \(N_1 = \mathcal{G}(\sqrt{-1}, \sqrt{\zeta})\) is a degree 4 extension of \(\mathcal{G}\). Similarly \(N_2 = \mathcal{G}(\sqrt{-p}, \sqrt{\pi})\) is a degree 4 extension of \(\mathcal{G}\). Thus the composite field \(N_1 N_2 = \mathcal{G}(\sqrt{-1}, \sqrt{\zeta}, \sqrt{-p}, \sqrt{\pi})\) is a degree 16 extension of \(\mathcal{G}\). Since \([\mathcal{G} : \mathbb{Q}] = 2, [N_1 N_2 : \mathbb{Q}] = 32\). We have the following diagram:

![Diagram of composite fields]

For the cyclotomic extension \(\mathbb{Q}(\zeta_{16})\) over \(\mathbb{Q}\) and its subfield \(\mathcal{E} = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})\), we have \([\mathbb{Q}(\zeta_{16}) : \mathcal{E}] = 2\). But also note that \(N_1 N_2 = \mathcal{E}(\sqrt{-p}, \sqrt{\zeta}, \sqrt{\pi})\) and so \([N_1 N_2 : \mathcal{E}] = 8\). Set

\[L = N_1 N_2 \mathbb{Q}(\zeta_{16}).\]
Then \( L = \mathcal{E}(\sqrt{\zeta_6}, \sqrt{-p}, \sqrt{\epsilon}, \sqrt{\pi}) \) is a degree 16 extension of \( \mathcal{E} \). Since \([\mathcal{E} : \mathbb{Q}] = 4\), we obtain \([L : \mathbb{Q}] = 64\). With a diagram, we have

As \( N_1, N_2, \) and \( \mathbb{Q}(\zeta_{16}) \) are normal extensions of \( \mathbb{Q} \), \( L \) is a normal extension of \( \mathbb{Q} \). For the convenience of the reader, we summarize the above discussion with a diagram of normal extensions:

For \( \ell \in \Omega \), \( \ell \) is unramified in \( L \) as it is unramified in \( N_1, N_2, \) and \( \mathbb{Q}(\zeta_{16}) \). The Artin symbol \((\ell/\mathbb{Q})\) is now defined for some prime \( \beta \) of \( \mathcal{O}_L \) containing \( \ell \). Let \((L/\mathbb{Q})\) denote the conjugacy class of \((\ell/\mathbb{Q})\) in \( \text{Gal}(L/\mathbb{Q}) \). Let \( M = \mathbb{Q}(\sqrt{2}, \sqrt{-1}, \sqrt{-p}) \).

Thus we have the diagram:
Let us now calculate $Z(\text{Gal}(L/Q))$.

**Lemma 3.79.** $Z(\text{Gal}(L/Q)) = \text{Gal}(L/M) \cong C_2 \times C_2 \times C_2$.

**Proof.** Note that $\text{Gal}(L/M)$ is determined by where the elements $\sqrt{\epsilon}, \sqrt{\pi}, \sqrt{\zeta_8}$ are sent. We consider the automorphisms induced by $\sigma(\sqrt{\epsilon}) = \pm \sqrt{\epsilon}, \sigma(\sqrt{\pi}) = \pm \sqrt{\pi}, \sigma(\sqrt{\zeta_8}) = \pm \sqrt{\zeta_8}$ for some $\sigma \in \text{Gal}(L/M)$. Using the relations $\sqrt{\epsilon} \cdot \sqrt{\epsilon} = \sqrt{-1}, \sqrt{\pi} \cdot \sqrt{\pi} = \sqrt{-p}$, and $\sqrt{\zeta_8} \cdot \sqrt{\zeta_8} = 1$, we have the following table of automorphisms for $\text{Gal}(L/M)$:

<table>
<thead>
<tr>
<th></th>
<th>$\sqrt{\epsilon}$</th>
<th>$\sqrt{\pi}$</th>
<th>$\sqrt{\zeta_8}$</th>
<th>$\sqrt{\epsilon}$</th>
<th>$\sqrt{\pi}$</th>
<th>$\sqrt{\zeta_8}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>a</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>b</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>c</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
</tbody>
</table>

where $\pm$ denotes $\rightarrow \pm$ in that order. Every $\sigma \in \text{Gal}(L/M)$ can be written in terms of these three elements. We see that $a$, $b$, and $c$ each have order 2 and so $|\text{Gal}(L/M)| = 8$. Thus $\text{Gal}(L/M) \cong < a > \times < b > \times < c > \cong C_2 \times C_2 \times C_2$. Now for the inclusion $\text{Gal}(L/M) \subset Z(\text{Gal}(L/Q))$, we need only show $a, b, c \in Z(\text{Gal}(L/Q))$. Since $a$ fixes $\sqrt{\pi}, \sqrt{\zeta_8}$, we only have to check $\sqrt{\epsilon}$. So for any $\sigma \in \text{Gal}(L/Q)$,
\[ a(\sqrt{\epsilon}) = \left\{ \begin{array}{ll} a(\sqrt{\epsilon}) = -\sqrt{\epsilon} \\ a(-\sqrt{\epsilon}) = -\sqrt{\epsilon} \\ a(\sqrt{\epsilon}) = \sqrt{\epsilon} \\ a(-\sqrt{\epsilon}) = \sqrt{\epsilon} \end{array} \right. \]

Thus \( a \in Z(\text{Gal}(L/Q)) \). Now \( b \) fixes \( \sqrt{\epsilon}, \sqrt{\zeta_8} \) and so we only check \( \sqrt{\pi} \). Thus,

\[ b(\sqrt{\pi}) = -\sqrt{\pi} \quad \text{and} \quad \sigma b(\sqrt{\pi}) = \sigma(-\sqrt{\pi}) = -\sqrt{\pi} \]

So \( b \in Z(\text{Gal}(L/Q)) \). Similarly \( a(\sqrt{\zeta_8}) = \sigma a(\sqrt{\zeta_8}) \) and so \( c \in Z(\text{Gal}(L/Q)) \).

For the inclusion \( Z(\text{Gal}(L/Q)) \subseteq \text{Gal}(L/M) \), the idea is to pick an element \( \sigma \in \text{Gal}(L/Q) \) such that \( \sigma \notin \text{Gal}(L/M) \) and show that \( \sigma \notin Z(\text{Gal}(L/Q)) \). There are seven cases:

(i) Suppose \( \sigma \) does not fix \( \sqrt{2} \) but fixes \( \sqrt{-1}, \sqrt{-p} \). Choose \( \tau \) which sends \( \sqrt{-p} \rightarrow -\sqrt{-p} \) and fixes \( \sqrt{2} \). Then

\[ \sigma \tau(\sqrt{\pi}) = \sigma(\pm \sqrt{\pi}) = \left\{ \begin{array}{ll} \sigma(\sqrt{\pi}) = \pm \sqrt{\pi} \\ \sigma(-\sqrt{\pi}) = \mp \sqrt{\pi} \end{array} \right. \]

Thus \( \sigma \notin Z(\text{Gal}(L/Q)) \).

(ii) Suppose \( \sigma \) does not fix \( \sqrt{-1} \), but fixes \( \sqrt{2}, \sqrt{-p} \). Choose \( \tau \) which sends \( \sqrt{2} \rightarrow -\sqrt{2} \) and fixes \( \sqrt{-1} \). Then

\[ \sigma \tau(\sqrt{\epsilon}) = \sigma(\pm \sqrt{\epsilon}) = \left\{ \begin{array}{ll} \sigma(\sqrt{\epsilon}) = \mp \sqrt{\epsilon} \\ \sigma(-\sqrt{\epsilon}) = \pm \sqrt{\epsilon} \end{array} \right. \]

Thus \( \sigma \notin Z(\text{Gal}(L/Q)) \).
(iii) Suppose \( \sigma \) does not fix \( \sqrt{2}, \sqrt{-1} \) but fixes \( \sqrt{-p} \). Choose \( \tau \) which sends 
\[ \sqrt{-1} \rightarrow -\sqrt{-1} \text{ and fixes } \sqrt{2}. \]
Then
\[ \sigma \tau(\sqrt{\zeta_8}) = \sigma(\pm \sqrt{\zeta_8}) = \begin{cases} 
\sigma(\sqrt{\zeta_8}) = \pm \sqrt{-\zeta_8} \\
\sigma(-\sqrt{\zeta_8}) = \mp \sqrt{-\zeta_8} 
\end{cases} \]
\[ \tau \sigma(\sqrt{\zeta_8}) = \tau(\pm \sqrt{-\zeta_8}) = \begin{cases} 
\tau(\sqrt{-\zeta_8}) = \mp \sqrt{-\zeta_8} \\
\tau(-\sqrt{-\zeta_8}) = \pm \sqrt{-\zeta_8} 
\end{cases} \]
Thus \( \sigma \not\in Z(\text{Gal}(L/Q)). \)

(iv) For \( \sigma \) not fixing \( \sqrt{-p} \) but fixes \( \sqrt{2}, \sqrt{-1} \), take \( \tau = \sigma \) from case (i) and thus 
\( \sigma \tau(\sqrt{\pi}) \neq \tau \sigma(\sqrt{\pi}). \)

(v) For \( \sigma \) not fixing \( \sqrt{2}, \sqrt{-p}, \) but fixes \( \sqrt{-1} \), take \( \tau = \sigma \) from case (ii) and thus 
\( \sigma \tau(\sqrt{\epsilon}) \neq \tau \sigma(\sqrt{\epsilon}). \)

(vi) For \( \sigma \) not fixing \( \sqrt{-p}, \sqrt{-1} \), but fixes \( \sqrt{2} \), take \( \tau = \sigma \) from case (iii) and thus 
\( \sigma \tau(\sqrt{\zeta_8}) \neq \tau \sigma(\sqrt{\zeta_8}). \)

(vii) For \( \sigma \) not fixing \( \sqrt{2}, \sqrt{-p}, \sqrt{-1} \), take \( \tau \) as in case (i) and thus 
\( \sigma \tau(\sqrt{\pi}) \neq \tau \sigma(\sqrt{\pi}). \)

Therefore \( Z(\text{Gal}(L/Q))' = \text{Gal}(L/M). \)

Now for \( l \in \Omega \), we have seen that \( l \) splits completely in \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{2}, \sqrt{-p}). \)
By Theorem 1.9, \( l \) splits completely in the composite field \( M = \mathbb{Q}(\sqrt{2}, \sqrt{-1}, \sqrt{-p}). \)
From Lemma 3.79,
\[ Z(\text{Gal}(L/Q))' = \text{Gal}(L/M)' = M = \mathbb{Q}(\sqrt{2}, \sqrt{-1}, \sqrt{-p}). \]

Thus we have the diagram:
\[ L \quad \{1\} \]
\[ \begin{array}{c|c|c}
M & \leftrightarrow & Z(\text{Gal}(L/\mathbb{Q})) \\
& & \\
\mathbb{Q} & \text{Gal}(L/\mathbb{Q}). & 
\end{array} \]

So by Lemma 1.26,

**Remark 3.80.** For some \( k \in \text{Gal}(L/\mathbb{Q}) \), \( (L/\mathbb{Q}) = \{k\} \subset Z(\text{Gal}(L/\mathbb{Q})) \).

Once again identify \( (L/\mathbb{Q}) \) with the automorphism \( k \) of \( Z(\text{Gal}(L/\mathbb{Q})) \). From Proposition 1.24, we can characterize \( (L/\mathbb{Q}) \) in terms of \( (N_1/\mathbb{Q}) \), \( (N_2/\mathbb{Q}) \), and \( (\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \).

**Lemma 3.81.** \( (L/\mathbb{Q}) = (N_1/\mathbb{Q}) \times (N_2/\mathbb{Q}) \times (\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \).

Using Lemma 3.81, Remark 3.66, the reformulation of Remark 3.73, and Remark 3.78, we now make the following one-to-one correspondences. We observe that there are eight distinct choices for \( (L/\mathbb{Q}) \) as there are two choices for each of \( (N_1/\mathbb{Q}) \), \( (N_2/\mathbb{Q}) \), and \( (\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \). Equivalently, as \( Z(\text{Gal}(L/\mathbb{Q})) \) has order 8, there are eight possible choices for \( (L/\mathbb{Q}) \).

**Remark 3.82.** (i) \( (L/\mathbb{Q}) = \{id\} \iff l \text{ splits completely in } L \iff \begin{cases} l \text{ splits completely in } N_1, \\ N_2, \text{ and } \mathbb{Q}(\zeta_{16}) \end{cases} \iff \begin{cases} l \text{ satisfies } < 1,32 > \\ l \equiv 1 \text{ mod 16} \end{cases} \)

(ii) \( (L/\mathbb{Q}) \neq \{id\} \iff l \text{ does not split completely in } L. \text{ Now there are seven cases.} \)

(1) \( \begin{cases} l \text{ splits completely in } N_1, \\ but \text{ does not in } N_2 \text{ or } \mathbb{Q}(\zeta_{16}) \end{cases} \iff \begin{cases} l \text{ satisfies } < 1,32 > \\ l \text{ satisfies } < 2,p > \\ l \equiv 9 \text{ mod 16} \end{cases} \)

58

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Now using Theorems 2.48, 2.49, 2.50, and 2.51, we relate each Artin symbol $(L/K)_l$ to each of the eight possible tuples of 4-ranks.

**Remark 3.83.** From Remark 3.82, case (i) occurs if and only if we have $(2, 2, 1, 1)$. For case (ii),

(1) occurs if and only if we have $(1, 2, 0, 1)$
(2) occurs if and only if we have $(2, 1, 1, 0)$
(3) occurs if and only if we have (2, 1, 0, 1)
(4) occurs if and only if we have (2, 2, 0, 0)
(5) occurs if and only if we have (1, 1, 0, 0)
(6) occurs if and only if we have (1, 1, 1, 1)
(7) occurs if and only if we have (1, 2, 1, 0).

We can now answer Question 2.61.

**Theorem 3.84.** Each of the eight possible tuples of 4-ranks appear with natural density $\frac{1}{8}$ in $\Omega$.

**Proof.** Consider the set $X = \{l \text{ prime} : l \text{ is unramified in } L \text{ and } (\frac{L/Q}{l}) = C_g\}$ where $C_g$ is the conjugacy class of $g \in \text{Gal}(L/Q)$. From Remark 3.80, we have

$$X = \{l \text{ prime} : l \text{ is unramified in } L \text{ and } (\frac{L/Q}{l}) = C_g\} = \{\text{some } k \in \text{Gal}(L/Q)\}$$

for some $k \in \text{Gal}(L/Q)$. By the Chebotarëv Density Theorem, the set $X$ has natural density $\frac{1}{64}$ in the set of all primes. Recall

$$\Omega = \{l \text{ rational prime} : l \equiv 1 \mod 8 \text{ and } (\frac{l}{p}) = (\frac{p}{l}) = 1\}$$

for some fixed prime $p \equiv 7 \mod 8$. By Theorem 1.29, $\Omega$ has natural density $\frac{1}{8}$ in the set of all primes. Thus $X$ has natural density $\frac{1}{8}$ in $\Omega$. By Remark 3.82 and 3.83, each of the eight choices for $(\frac{L/Q}{l})$ is in one to one correspondence with each of the possible tuples of 4-ranks. Thus each of the eight possible tuples of 4-ranks appear with natural density $\frac{1}{8}$ in $\Omega$. 

$\square$

60

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
3.6 The Cases $\mathbb{Q}(\sqrt{pl})$ and $\mathbb{Q}(\sqrt{2pl})$

Let us turn our attention to Theorems 2.48 and 2.49. In the previous section, we were concerned with the Artin symbol $(\frac{L/Q}{l})$. Let us now use Corollary 1.22 to restrict this symbol to the normal subfield $N_2\mathbb{Q}(\zeta_{16}) \subset L$, i.e.

$$\left(\frac{L/Q}{l}\right)_{N_2\mathbb{Q}(\zeta_{16})} = \left(\frac{N_2\mathbb{Q}(\zeta_{16})/Q}{l}\right).$$

Set $K = N_2\mathbb{Q}(\zeta_{16})$. Let us now calculate $Z(Gal(K/Q))$.

Lemma 3.85. $Z(Gal(K/Q)) = Gal(K/M)$.

Proof. We consider the automorphisms induced by $\sigma(\sqrt{\pi}) = \pm\sqrt{\pi}$, $\pm\sqrt{\pi}$ and $\sigma(\sqrt{\zeta_8}) = \pm\sqrt{\zeta_8}$, $\pm\sqrt{\zeta_8}$ for some $\sigma \in Gal(K/M)$. Using the relations $\sqrt{\pi} \cdot \sqrt{\pi} = \sqrt{-p}$, and $\sqrt{\zeta_8} \cdot \sqrt{\zeta_8} = 1$, we have the following table of automorphisms for $Gal(K/M)$:

<table>
<thead>
<tr>
<th></th>
<th>$\sqrt{\pi}$</th>
<th>$\sqrt{\zeta_8}$</th>
<th>$\sqrt{\pi}$</th>
<th>$\sqrt{\zeta_8}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>$\beta$</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
</tbody>
</table>

where $\pm$ denotes $\cdot \mapsto \pm \cdot$ in that order. Every $\sigma \in Gal(K/M)$ can be written in terms of the automorphisms $\alpha$ and $\beta$. We see that $\alpha$ and $\beta$ each have order 2 and so $|Gal(K/M)| = 4$. Thus $Gal(K/M) \cong < \alpha > \times < \beta > \cong C_2 \times C_2$. For the inclusion $Gal(K/M) \subset Z(Gal(K/Q))$, it is enough to show $\alpha, \beta \in Z(Gal(K/Q))$.

Since $\alpha$ fixes $\sqrt{\zeta_8}$, we only check $\sqrt{\pi}$. So for any $\sigma \in Gal(K/Q)$,

$$\alpha \sigma (\sqrt{\pi}) = \begin{cases} b(\sqrt{\pi}) = -\sqrt{\pi} \\
\sigma(\sqrt{\pi}) = \sqrt{\pi} \\
\sigma(\sqrt{\pi}) = 1 \\
b(\sqrt{\pi}) = -\sqrt{\pi} \\
b(-\sqrt{\pi}) = \sqrt{\pi} \\
b(-\sqrt{\pi}) = \sqrt{\pi} \\
b(-\sqrt{\pi}) = 1 \end{cases}$$

and

$$\sigma \alpha (\sqrt{\pi}) = \begin{cases} -\sqrt{\pi} \\
\sqrt{\pi} \\
\sqrt{\pi} \\
\sqrt{\pi} \\
\sqrt{\pi} \\
\sqrt{\pi} \end{cases}$$

61

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Thus \( \alpha \in Z(\text{Gal}(K/Q)) \). Similarly, \( \beta \sigma(\sqrt{\epsilon}) = \sigma \beta(\sqrt{\epsilon}) \) for every \( \sigma \in \text{Gal}(K/Q) \) and so \( \text{Gal}(K/M) \subset Z(\text{Gal}(K/Q)) \). For the inclusion \( Z(\text{Gal}(K/Q)) \subset \text{Gal}(K/M) \), the arguments are the same as in the proof of Lemma 3.79, i.e., for \( \sigma \in \text{Gal}(K/Q) \) such that \( \sigma \notin \text{Gal}(K/M) \), there are seven cases to check. Since \( K \) is normal over \( Q \), we have \( \forall \tau \in \text{Gal}(L/Q), \tau|_K \in \text{Gal}(K/Q) \). Thus we choose \( \tau \) as in cases (i)-(vii) of the proof of Lemma 3.79 and obtain \( \tau|_K \sigma \neq \sigma \tau|_K \). In case (iii) consider \( \sqrt{\zeta_8} \) to obtain \( \sigma \tau|_K(\sqrt{\zeta_8}) \neq \tau|_K \sigma(\sqrt{\zeta_8}) \). In case (vi) take \( \tau|_K = \sigma \) from case (iii) and thus \( \sigma \tau|_K(\sqrt{\zeta_8}) \neq \tau|_K \sigma(\sqrt{\zeta_8}) \).

Therefore \( Z(\text{Gal}(K/Q)) = \text{Gal}(K/M) \).

\[ \square \]

Once again for \( \ell \in \Omega \), we have seen that \( \ell \) splits completely in \( M = Q(\sqrt{2}, \sqrt{-1}, \sqrt{\ell}) \).

From Lemma 3.85,

\[ Z(\text{Gal}(K/Q))' = \text{Gal}(K/M)' = M. \]

and so we have the diagram:

\[
\begin{array}{ccc}
K & \{1\} & \\
\downarrow & & \downarrow \\
M & \leftrightarrow & Z(\text{Gal}(K/Q)) \\
\downarrow & & \downarrow \\
Q & Gal(K/Q).
\end{array}
\]

So by Lemma 1.26,

**Remark 3.86.** For some \( j \in \text{Gal}(K/Q), (\frac{K/Q}{j}) = \{j\} \subset Z(\text{Gal}(K/Q)) \).

Let us now make the following one to one correspondences. Using Proposition 1.24 and noting that there are two choices for each of \( (\frac{N_{\ell}/Q}{j}) \) and \((\frac{Q(k_{16})/Q}{j}) \), we
have four distinct choices for \( (\frac{K}{l}) \).

**Remark 3.87.** (i) \( (\frac{K}{l}) = \{id\} \iff l \text{ splits completely in } K \iff \)

\[
\left\{ \begin{array}{l}
\text{l splits completely} \\
\text{in } N_2 \text{ and } Q(\zeta_{16})
\end{array} \right\} \iff \left\{ \begin{array}{l}
\text{l satisfies } <1,2p> \\
\text{l } \equiv 1 \text{ mod } 16
\end{array} \right\}.
\]

(ii) \( (\frac{K}{l}) \neq \{id\} \iff l \text{ does not split completely in } K. \text{ There are three cases.} \)

1. \[
\left\{ \begin{array}{l}
l \text{ splits completely in } N_2, \\
\text{but does not in } Q(\zeta_{16})
\end{array} \right\} \iff \left\{ \begin{array}{l}
l \text{ satisfies } <1,2p> \\
\text{l } \equiv 9 \text{ mod } 16
\end{array} \right\}
\]

2. \[
\left\{ \begin{array}{l}
l \text{ splits completely in } Q(\zeta_{16}), \\
\text{but does not in } N_2
\end{array} \right\} \iff \left\{ \begin{array}{l}
l \text{ satisfies } <2,p> \\
\text{l } \equiv 1 \text{ mod } 16
\end{array} \right\}
\]

3. \[
\left\{ \begin{array}{l}
l \text{ does not split completely} \\
in N_2 \text{ or } Q(\zeta_{16})
\end{array} \right\} \iff \left\{ \begin{array}{l}
l \text{ satisfies } <2,p> \\
\text{l } \equiv 9 \text{ mod } 16
\end{array} \right\}
\]

We can now answer Questions 2.57 and 2.58.

**Theorem 3.88.** For the fields \( Q(\sqrt{p_l}) \) and \( Q(\sqrt{2p_l}) \), 4-rank 1 and 2 each appear with natural density \( \frac{1}{2} \) in \( \Omega \).

**Proof.** Let \( X = \{l \text{ prime} : l \text{ is unramified in } K \text{ and } (\frac{K}{l}) = C_g\} \) where \( C_g \) is the conjugacy class of \( g \in \text{Gal}(K/Q) \). From Remark 3.87, we have

\[
X = \{l \text{ prime} : l \text{ is unramified in } K \text{ and } (\frac{K}{l}) = \{k\} \subset Z(\text{Gal}(K/Q))\}
\]

for some \( k \in \text{Gal}(K/Q) \). By the Chebotarëv Density Theorem, the set \( X \) has natural density \( \frac{1}{32} \) in the set of all primes. Recall \( \Omega \) has natural density \( \frac{1}{8} \) in the set of all primes. Let

\[
\Omega_1 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{Q(\sqrt{p_l})}) = 1\}.
\]
By Theorem 2.48,
\[ \Omega_1 = \{ l \in \Omega : l \text{satisfies } <2,p> \}. \]

Clearly,
\[ \Omega_1 = \{ l \in \Omega : l \text{satisfies } <2,p>, l \equiv 1 \text{ mod } 16 \} \cup \{ l \in \Omega : l \text{satisfies } <2,p>, l \equiv 9 \text{ mod } 16 \}. \]

Thus by Remark 3.87, case (ii) parts (2) and (3), \( \Omega_1 \) has natural density \( \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \) in \( \Omega \). Let
\[ \Omega_2 = \{ l \in \Omega : 4\text{-rank } K_2(\mathcal{O}_Q(\sqrt{p})) = 2 \}. \]

Then by Theorem 2.48,
\[ \Omega_2 = \{ l \in \Omega : l \text{satisfies } <1,2p> \}. \]

Once again,
\[ \Omega_2 = \{ l \in \Omega : l \text{satisfies } <1,2p>, l \equiv 1 \text{ mod } 16 \} \cup \{ l \in \Omega : l \text{satisfies } <1,2p>, l \equiv 9 \text{ mod } 16 \}. \]

By Remark 3.87, cases (i) and (ii) part (1), \( \Omega_2 \) has natural density \( \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \) in \( \Omega \). Now let
\[ \Omega_3 = \{ l \in \Omega : 4\text{-rank } K_2(\mathcal{O}_Q(\sqrt{3p})) = 1 \} \]
and
\[ \Omega_4 = \{ l \in \Omega : 4\text{-rank } K_2(\mathcal{O}_Q(\sqrt{3p})) = 2 \}. \]

By Theorem 2.49,
\[ \Omega_3 = \{ l \in \Omega : l \text{satisfies } <2,p>, l \equiv 1 \text{ mod } 16 \} \cup \{ l \in \Omega : l \text{satisfies } <1,2p>, l \equiv 9 \text{ mod } 16 \}. \]
\[ \Omega_4 = \{ l \in \Omega : l \text{satisfies } <1,2p>, l \equiv 1 \text{ mod } 16 \} \cup \{ l \in \Omega : l \text{satisfies } \]
By Remark 3.87, case (ii) parts (1) and (2), \( \Omega_3 \) has natural density \( \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \) in \( \Omega \). Also from case (i) and case(ii) part (3), \( \Omega_4 \) has natural density \( \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \) in \( \Omega \).

\[ \square \]

### 3.7 The Cases \( \mathbb{Q}(\sqrt{-pl}) \) and \( \mathbb{Q}(\sqrt{-2pl}) \)

We will focus on Theorem 2.50 and Theorem 2.51. In section 4, we dealt with the Artin symbol \( (\frac{L}{\mathbb{Q}}) \). Using Corollary 1.22, restrict this symbol to the normal subfield \( N_1 N_2 \subset L \), i.e.

\[
\left. \left( \frac{L/\mathbb{Q}}{l} \right) \right|_{N_1 N_2} = \left( \frac{N_1 N_2/\mathbb{Q}}{l} \right).
\]

Set \( N = N_1 N_2 \). We now consider \( Z(\text{Gal}(N/\mathbb{Q})) \).

**Lemma 3.89.** \( Z(\text{Gal}(N/\mathbb{Q})) = \text{Gal}(N/M) \).

**Proof.** We consider the automorphisms induced by \( \sigma(\sqrt{\varepsilon}) = \pm \sqrt{\varepsilon}, \pm \sqrt{\bar{\varepsilon}} \) and \( \sigma(\sqrt{\pi}) = \pm \sqrt{\pi}, \pm \sqrt{\bar{\pi}} \) for some \( \sigma \in \text{Gal}(N/M) \). Using the relations \( \sqrt{\varepsilon} \cdot \sqrt{\bar{\varepsilon}} = \sqrt{-1} \), and \( \sqrt{\pi} \cdot \sqrt{\bar{\pi}} = \sqrt{-p} \), we have the following table of automorphisms for \( \text{Gal}(N/M) \):

<table>
<thead>
<tr>
<th></th>
<th>( \sqrt{\varepsilon} )</th>
<th>( \sqrt{\pi} )</th>
<th>( \sqrt{\bar{\varepsilon}} )</th>
<th>( \sqrt{\bar{\pi}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>( \beta )</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
</tr>
</tbody>
</table>

where \( \pm \) denotes \( \cdot \mapsto \pm \cdot \) in that order. Every \( \sigma \in \text{Gal}(N/M) \) can be written in terms of the automorphisms \( \alpha \) and \( \beta \). We see that \( \alpha \) and \( \beta \) each have order 2 and so \( |\text{Gal}(N/M)| = 4 \). Thus \( \text{Gal}(N/M) \cong < \alpha > \times < \beta > \cong C_2 \times C_2 \). For the inclusion \( \text{Gal}(N/M) \subset Z(\text{Gal}(N/\mathbb{Q})) \), it is enough to show \( \alpha, \beta \in Z(\text{Gal}(N/\mathbb{Q})) \).

65

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Since $\alpha$ fixes $\sqrt{e}$, we only check $\sqrt{\pi}$. So for any $\sigma \in \text{Gal}(N/\mathbb{Q})$,

$$\alpha \sigma(\sqrt{\pi}) = \begin{cases} 
\alpha(\sqrt{\pi}) = -\sqrt{\pi} \\
\alpha(-\sqrt{\pi}) = \sqrt{\pi} \\
\alpha(\sqrt{\pi}) = -\sqrt{\pi} \\
\alpha(-\sqrt{\pi}) = \sqrt{\pi}
\end{cases}$$

and $\sigma \alpha(\sqrt{\pi}) = \sigma(-\sqrt{\pi}) = \begin{cases} 
-\sqrt{\pi} \\
\sqrt{\pi} \\
-\sqrt{\pi} \\
\sqrt{\pi}
\end{cases}$

Thus $\alpha \in Z(\text{Gal}(N/\mathbb{Q}))$. Similarly, $\beta \sigma(\sqrt{e}) = \sigma \beta(\sqrt{e})$ for every $\sigma \in \text{Gal}(N/\mathbb{Q})$ and so $\text{Gal}(N/M) \subset Z(\text{Gal}(N/\mathbb{Q}))$. For the inclusion $Z(\text{Gal}(N/\mathbb{Q})) \subset \text{Gal}(N/M)$, the arguments are the same as in the proof of Lemma 3.79 or Lemma 3.85, i.e., for $\sigma \in \text{Gal}(N/\mathbb{Q})$ such that $\sigma \not\in \text{Gal}(N/M)$, there are seven cases to check. Since $N$ is normal over $\mathbb{Q}$, we have $\forall \tau \in \text{Gal}(L/\mathbb{Q})$, $\tau|_N \in \text{Gal}(N/\mathbb{Q})$. Thus we choose $\tau$ as in cases (i)-(vii) of the proof of Lemma 3.79 and obtain $\tau|_N \sigma \neq \sigma \tau|_N$. In case (iii) consider $\sqrt{e}$ to obtain $\sigma \tau|_N(\sqrt{e}) \neq \tau|_N \sigma(\sqrt{e})$. In case (vi) take $\tau|_N = \sigma$ from case (iii) and thus $\sigma \tau|_N(\sqrt{e}) \neq \tau|_N \sigma(\sqrt{e})$.

Therefore $Z(\text{Gal}(N/\mathbb{Q})) = \text{Gal}(N/M)$.

For $l \in \Omega$, $l$ splits completely in $M$. From Lemma 3.89,

$$Z(\text{Gal}(N/\mathbb{Q}))^\prime = \text{Gal}(N/M)^\prime = M.$$ 

To illustrate the situation:

$$
\begin{array}{c|c}
N & \{1\} \\
\hline
M & \leftrightarrow \ Z(\text{Gal}(N/\mathbb{Q})) \\
\hline
\mathbb{Q} & \text{Gal}(N/\mathbb{Q}).
\end{array}
$$

So by Lemma 1.26,
Remark 3.90. For some $s \in \text{Gal}(N/Q)$, $(N/Q)_l = \{s\} \subset Z(\text{Gal}(N/Q))$.

As in section 5, we observe the following one to one correspondences. Once again there are four distinct choices for $(N/Q)_l$.

Remark 3.91. (i) $(N/Q)_l = \{id\} \iff l$ splits completely in $N$ 

\[
\begin{aligned}
&\{l \text{ splits completely in } N_1 \text{ and } N_2 \} \iff \{l \text{ satisfies } <1,32>\}.
\end{aligned}
\]

(ii) $(N/Q)_l \not= \{id\} \iff l$ does not split completely in $N$. There are three cases.

(1) \[
\begin{aligned}
&\{l \text{ splits completely in } N_1, \text{ but does not in } N_2 \} \iff \{l \text{ satisfies } <1,32>\}.
\end{aligned}
\]

(2) \[
\begin{aligned}
&\{l \text{ splits completely in } N_2, \text{ but does not in } N_1 \} \iff \{l \text{ satisfies } <1,2p>\}.
\end{aligned}
\]

(3) \[
\begin{aligned}
&\{l \text{ does not split completely in } N_1 \text{ or } N_2 \} \iff \{l \text{ satisfies } <1,32>\}.
\end{aligned}
\]

We can now answer Question 2.59.

Theorem 3.92. For the fields $Q(\sqrt{-pl})$ and $Q(\sqrt{-2pl})$, 4-rank 0 and 1 each appear with natural density $\frac{1}{2}$ in $\Omega$.

Proof. Let $X = \{l \text{ prime} : l \text{ is unramified in } N \text{ and } (N/Q)_l = C_g\}$ where $C_g$ is the conjugacy class of $g \in \text{Gal}(N/Q)$. From Remark 3.90, we have

\[
X = \{l \text{ prime} : l \text{ is unramified in } N \text{ and } (N/Q)_l = \{s\} \subset Z(\text{Gal}(N/Q))\}
\]

for some $s \in \text{Gal}(N/Q)$. By the Chebotarëv Density Theorem, the set $X$ has natural density $\frac{1}{32}$ in the set of all primes. Once again, $\Omega$ has natural density $\frac{1}{8}$ in
the set of all primes. Let
\[ \Lambda_1 = \{ l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-p})}) = 0 \} \]

and
\[ \Lambda_2 = \{ l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-p})}) = 1 \} \]

By Theorem 2.50,
\[ \Lambda_1 = \{ l \in \Omega : l \text{ satisfies } < 1, 32 > \text{ and } < 2, p > \} \cup \{ l \in \Omega : l \text{ does not satisfy } < 1, 32 >, l \text{ satisfies } < 1, 2p > \} \]
\[ \Lambda_2 = \{ l \in \Omega : l \text{ satisfies } < 1, 32 > \text{ and } < 1, 2p > \} \cup \{ l \in \Omega : l \text{ does not satisfy } < 1, 32 >, l \text{ satisfies } < 2, p > \} \]

Thus by Remark 3.91, case (ii) parts (1) and (2), \( \Lambda_1 \) has natural density \( \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \) in \( \Omega \).

From case (i) and case (ii) part (3), \( \Lambda_2 \) has natural density \( \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \) in \( \Omega \).

Now let
\[ \Lambda_3 = \{ l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-2p})}) = 0 \} \]

and
\[ \Lambda_4 = \{ l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-2p})}) = 1 \} \]

By Theorem 2.51,
\[ \Lambda_3 = \{ l \in \Omega : l \equiv 1 \mod 16, l \text{ satisfies } < 1, 32 > \text{ and } < 2, p > \} \cup \{ l \in \Omega : l \equiv 1 \mod 16, l \text{ does not satisfy } < 1, 32 >, l \text{ satisfies } < 1, 2p > \} \cup \{ l \in \Omega : l \equiv 9 \mod 16, l \text{ satisfies } < 1, 32 > \text{ and } < 1, 2p > \} \cup \{ l \in \Omega : l \equiv 9 \mod 16, l \text{ does not satisfy } < 1, 32 >, l \text{ satisfies } < 2, p > \} \]
\[ \Lambda_4 = \{ l \in \Omega : l \equiv 1 \mod 16, l \text{ satisfies } < 1, 32 > \text{ and } < 1, 2p > \} \cup \{ l \in \Omega : l \equiv 1 \mod 16, l \text{ does not satisfy } < 1, 32 >, l \text{ satisfies } < 2, p > \} \cup \{ l \in \Omega : l \equiv 9 \mod 16, l \text{ satisfies } < 1, 32 > \text{ and } < 2, p > \} \cup \{ l \in \Omega : l \equiv 9 \mod 16, l \text{ does
not satisfy \(<1, 32>, l\) satisfies \(<1, 2p>\).

By Remark 3.91 and Theorem 1.29, \(A_3\) and \(A_4\) each have natural density 
\[
\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}
\]
in \(\Omega\).

Remark 3.93. We conclude with two questions:

(i) Is it possible to classify the 4-rank (or higher 2-power ranks) of the tame kernel in terms of positive definite binary quadratic forms for other quadratic number fields?

(ii) Do density results exist for higher 2-power ranks of tame kernels of quadratic number fields?

The methods used in [C-H] and [H-K] might serve as a basis for further investigation of these questions.
References


Appendix 1: Possible Densities

The following pages contain tables which motivated possible density results of 4-ranks of tame kernels. Let

$$\Omega = \{l \text{ rational prime} : l \equiv 1 \mod 8 \text{ and } \left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) = 1\}$$

and consider primes $l \in \Omega$ with $l \leq N$ for a fixed prime $p \equiv 7 \mod 8$ and positive integer $N$. For Tables 1, 2, and 3 we let $E_1 = \mathbb{Q}(\sqrt{p l})$ and $E_2 = \mathbb{Q}(\sqrt{2 p l})$ and consider the sets:

$$\Omega_1 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{E_1}) = 1\},$$
$$\Omega_2 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{E_1}) = 2\},$$
$$\Omega_3 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{E_2}) = 1\},$$
$$\Omega_4 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{E_2}) = 2\}.$$

Also, we let $F_1 = \mathbb{Q}(\sqrt{-pl})$ and $F_2 = \mathbb{Q}(\sqrt{-2pl})$ and consider the sets:

$$\Lambda_1 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{F_1}) = 0\},$$
$$\Lambda_2 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{F_1}) = 1\},$$
$$\Lambda_3 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{F_2}) = 0\},$$
$$\Lambda_4 = \{l \in \Omega : \text{4-rank } K_2(\mathcal{O}_{F_2}) = 1\}.$$

For Tables 4, 5, and 6, we let

$$I_1 = \{l \in \Omega : \text{4-rank tuple is } (1, 1, 0, 0)\}$$
$$I_2 = \{l \in \Omega : \text{4-rank tuple is } (1, 1, 1, 1)\}$$
$$I_3 = \{l \in \Omega : \text{4-rank tuple is } (2, 1, 1, 0)\}$$
\[ I_4 = \{ l \in \Omega : \text{4-rank tuple is } (2,1,0,1) \} \]

\[ I_5 = \{ l \in \Omega : \text{4-rank tuple is } (1,2,1,0) \} \]

\[ I_6 = \{ l \in \Omega : \text{4-rank tuple is } (1,2,0,1) \} \]

\[ I_7 = \{ l \in \Omega : \text{4-rank tuple is } (2,2,0,0) \} \]

\[ I_8 = \{ l \in \Omega : \text{4-rank tuple is } (2,2,1,1) \}. \]
Table 1: $p = 7$

| Cardinality $|\Omega|$ | $N = 6620$ | $\%$ | $N = 25000$ | $\%$ | $N = 1000000$ | $\%$ |
|---|---|---|---|---|---|---|---|
| $|\Omega_1|$ | 53 | 55.79 | 168 | 51.38 | 4866 | 50.01 |
| $|\Omega_2|$ | 42 | 44.21 | 159 | 48.62 | 4864 | 49.99 |
| $|\Omega_3|$ | 52 | 54.74 | 167 | 51.07 | 4866 | 50.01 |
| $|\Omega_4|$ | 43 | 45.26 | 160 | 48.93 | 4864 | 49.99 |
| $|\Lambda_1|$ | 46 | 48.42 | 167 | 51.07 | 4878 | 50.13 |
| $|\Lambda_2|$ | 49 | 51.58 | 160 | 48.93 | 4852 | 49.87 |
| $|\Lambda_3|$ | 53 | 55.79 | 172 | 52.60 | 4878 | 50.13 |
| $|\Lambda_4|$ | 42 | 44.21 | 155 | 47.40 | 4852 | 49.87 |
Table 2: \( p = 23 \)

<table>
<thead>
<tr>
<th>Cardinality</th>
<th>( N = 6620 )</th>
<th>%</th>
<th>( N = 25000 )</th>
<th>%</th>
<th>( N = 1000000 )</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>\Omega</td>
<td>)</td>
<td>98</td>
<td>328</td>
<td>9742</td>
<td></td>
</tr>
<tr>
<td>(</td>
<td>\Omega_1</td>
<td>)</td>
<td>52</td>
<td>53.06</td>
<td>171</td>
<td>4905</td>
</tr>
<tr>
<td>(</td>
<td>\Omega_2</td>
<td>)</td>
<td>46</td>
<td>46.94</td>
<td>157</td>
<td>4837</td>
</tr>
<tr>
<td>(</td>
<td>\Omega_3</td>
<td>)</td>
<td>60</td>
<td>61.22</td>
<td>167</td>
<td>4911</td>
</tr>
<tr>
<td>(</td>
<td>\Omega_4</td>
<td>)</td>
<td>38</td>
<td>38.78</td>
<td>161</td>
<td>4831</td>
</tr>
<tr>
<td>(</td>
<td>\Lambda_1</td>
<td>)</td>
<td>54</td>
<td>55.10</td>
<td>164</td>
<td>4912</td>
</tr>
<tr>
<td>(</td>
<td>\Lambda_2</td>
<td>)</td>
<td>44</td>
<td>44.90</td>
<td>164</td>
<td>4830</td>
</tr>
<tr>
<td>(</td>
<td>\Lambda_3</td>
<td>)</td>
<td>50</td>
<td>51.02</td>
<td>168</td>
<td>4876</td>
</tr>
<tr>
<td>(</td>
<td>\Lambda_4</td>
<td>)</td>
<td>48</td>
<td>48.98</td>
<td>160</td>
<td>4866</td>
</tr>
</tbody>
</table>

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Table 3: $p = 31$

<table>
<thead>
<tr>
<th>Cardinality</th>
<th>$N = 6620$</th>
<th>%</th>
<th>$N = 25000$</th>
<th>%</th>
<th>$N = 1000000$</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Omega</td>
<td>$</td>
<td>97</td>
<td>325</td>
<td></td>
<td>9754</td>
</tr>
<tr>
<td>$</td>
<td>\Omega_1</td>
<td>$</td>
<td>49</td>
<td>50.52</td>
<td>169</td>
<td>52.00</td>
</tr>
<tr>
<td>$</td>
<td>\Omega_2</td>
<td>$</td>
<td>48</td>
<td>49.48</td>
<td>156</td>
<td>48.00</td>
</tr>
<tr>
<td>$</td>
<td>\Omega_3</td>
<td>$</td>
<td>52</td>
<td>53.61</td>
<td>170</td>
<td>52.31</td>
</tr>
<tr>
<td>$</td>
<td>\Omega_4</td>
<td>$</td>
<td>45</td>
<td>46.39</td>
<td>155</td>
<td>47.69</td>
</tr>
<tr>
<td>$</td>
<td>\Lambda_1</td>
<td>$</td>
<td>54</td>
<td>55.67</td>
<td>168</td>
<td>51.69</td>
</tr>
<tr>
<td>$</td>
<td>\Lambda_2</td>
<td>$</td>
<td>43</td>
<td>44.33</td>
<td>157</td>
<td>48.31</td>
</tr>
<tr>
<td>$</td>
<td>\Lambda_3</td>
<td>$</td>
<td>47</td>
<td>48.45</td>
<td>159</td>
<td>48.92</td>
</tr>
<tr>
<td>$</td>
<td>\Lambda_4</td>
<td>$</td>
<td>50</td>
<td>51.55</td>
<td>166</td>
<td>51.08</td>
</tr>
</tbody>
</table>
Table 4: $p = 7$

<table>
<thead>
<tr>
<th>Cardinality</th>
<th>$N = 6620$</th>
<th>%</th>
<th>$N = 25000$</th>
<th>%</th>
<th>$N = 1000000$</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Omega</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>327</td>
<td>9730</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_1</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>43</td>
<td>1215</td>
<td>12.49</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_2</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>43</td>
<td>1213</td>
<td>12.46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_3</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>40</td>
<td>1228</td>
<td>12.62</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_4</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>41</td>
<td>1210</td>
<td>12.44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_5</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>44</td>
<td>1210</td>
<td>12.44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_6</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>38</td>
<td>1228</td>
<td>12.62</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_7</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>45</td>
<td>1225</td>
<td>12.59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_8</td>
<td>$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>33</td>
<td>1201</td>
<td>12.34</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 5: p = 23

<table>
<thead>
<tr>
<th>Cardinality</th>
<th>$N = 6620$</th>
<th>%</th>
<th>$N = 25000$</th>
<th>%</th>
<th>$N = 1000000$</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Omega</td>
<td>$</td>
<td>98</td>
<td>328</td>
<td>9742</td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_1</td>
<td>$</td>
<td>17</td>
<td>17.35</td>
<td>39</td>
<td>11.89</td>
</tr>
<tr>
<td>$</td>
<td>I_2</td>
<td>$</td>
<td>15</td>
<td>15.31</td>
<td>51</td>
<td>15.55</td>
</tr>
<tr>
<td>$</td>
<td>I_3</td>
<td>$</td>
<td>13</td>
<td>13.27</td>
<td>40</td>
<td>12.20</td>
</tr>
<tr>
<td>$</td>
<td>I_4</td>
<td>$</td>
<td>15</td>
<td>15.31</td>
<td>37</td>
<td>11.28</td>
</tr>
<tr>
<td>$</td>
<td>I_5</td>
<td>$</td>
<td>9</td>
<td>9.18</td>
<td>41</td>
<td>12.50</td>
</tr>
<tr>
<td>$</td>
<td>I_6</td>
<td>$</td>
<td>11</td>
<td>11.22</td>
<td>40</td>
<td>12.19</td>
</tr>
<tr>
<td>$</td>
<td>I_7</td>
<td>$</td>
<td>11</td>
<td>11.22</td>
<td>48</td>
<td>14.63</td>
</tr>
<tr>
<td>$</td>
<td>I_8</td>
<td>$</td>
<td>7</td>
<td>7.14</td>
<td>32</td>
<td>9.76</td>
</tr>
</tbody>
</table>
Table 6: $p = 31$

<table>
<thead>
<tr>
<th>Cardinality</th>
<th>$N = 6620$</th>
<th>%</th>
<th>$N = 25000$</th>
<th>%</th>
<th>$N = 1000000$</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Omega</td>
<td>$</td>
<td>97</td>
<td>325</td>
<td>9754</td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>I_1</td>
<td>$</td>
<td>14</td>
<td>14.43</td>
<td>38</td>
<td>11.69</td>
</tr>
<tr>
<td>$</td>
<td>I_2</td>
<td>$</td>
<td>12</td>
<td>12.37</td>
<td>49</td>
<td>15.08</td>
</tr>
<tr>
<td>$</td>
<td>I_3</td>
<td>$</td>
<td>11</td>
<td>11.34</td>
<td>38</td>
<td>11.69</td>
</tr>
<tr>
<td>$</td>
<td>I_4</td>
<td>$</td>
<td>15</td>
<td>15.47</td>
<td>45</td>
<td>13.85</td>
</tr>
<tr>
<td>$</td>
<td>I_5</td>
<td>$</td>
<td>10</td>
<td>10.31</td>
<td>40</td>
<td>12.31</td>
</tr>
<tr>
<td>$</td>
<td>I_6</td>
<td>$</td>
<td>13</td>
<td>13.40</td>
<td>42</td>
<td>12.92</td>
</tr>
<tr>
<td>$</td>
<td>I_7</td>
<td>$</td>
<td>12</td>
<td>12.37</td>
<td>43</td>
<td>13.23</td>
</tr>
<tr>
<td>$</td>
<td>I_8</td>
<td>$</td>
<td>10</td>
<td>10.31</td>
<td>30</td>
<td>9.23</td>
</tr>
</tbody>
</table>

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Appendix 2: The Program

Given a prime $p$ congruent to 7 modulo 8, class number for $\mathbb{Q}(\sqrt{-2p})$, and upper bound $N$, the following program written in C++ generates the numerical values found in Tables 1-6 in Appendix 1:

```cpp
#include <stdio.h>
#include <math.h>
long root(long l)
{
    return (long) sqrt((double) l);
}
int prime(long l)
{
    long k, limit;
    limit = root(l);
    for (k = 3; k <= limit; k += 2)
        if (l%k == 0 || l%2 == 0)
            return 0;
    return 1;
}
int check1a(long int l, int q)
{
    int e,f,i,x,w,m,res[1000];
    long int y;
```
if (prime(l)) {
    y = 0;
    for (e = 1; e < 10000; e++) {
        if (y == 1)
            break;
        for (f = -1; f > -10000; f--)
            y = 8 * e + (q) * f;
        if (y == 1)
            break;
    }
    break;
}
for (i = 1; i < ((q + 1)/2); i++) {
    x = (i * i) mod (q);
    m = ((8 * x * (e - 1)) + (q * f)) mod (8 * (q));
    res[i - 1] = m;
}
if (prime(l)) {
    for (w = 0; w < (((q) + 1)/2); w++) {
        if (l % ((q) * 8) == res[w])
            return 1;
    }
    return 0;
}
return 0;
}

int check0(long l, int q)
{
    if (check0(l, q) && l%16 == 1)
        return 1;
    else
        return 0;
}

int check1(long l, int q)
{
    if (check0(l, q) && l%16 == 9)
        return 1;
    else
        return 0;
}

int check2(long l, int q)
{
    long i;
    int z;
    double y;
    z=0;
    if (l%8 == 1 && check0(l, q))
    {
        for (i = 1; i <= sqrt((double)((double)l)); i++)
        {
            ...
        }
    }
}
\[ y = \sqrt{(l - \text{pow}((\text{double})i,2))/32}; \]

if \( y == ((\text{long})y) \) {
    \[ z = 1; \]
    break;
}

return z;

int check3(long l, int q, int hk)
{
    long i;
    int z;
    double y;
    z = 0;
    if (check1a(l,q)) {
        for (i = 1; i <= \sqrt{\text{pow}((\text{double})l,(\text{hk}/4))/2}; i++) {
            y = \sqrt{\text{pow}((\text{double})l,(\text{hk}/4)) - 2*((\text{double}i*\text{double}i))/(\text{double}q)};
            if (y == ((\text{long})y) && !(((\text{long})y)\%l == 0)) {
                z = 1;
                break;
            }
        }
    }
    return z;
}
int check4(long l, int q, int hk) {
    long i;
    int z;
    double y;
    z = 0;
    if (check1a(l, q)) {
        for (i = 1; i <= sqrt(pow((double)l, (hk / 4))); i++) {
            y = sqrt((pow((double)l, (hk / 4)) - ((double)i * (double)i)) / (2 * (double)q));
            if (y == ((long)y) && (!(((long)y) % l == 0))){
                z = 1;
                break;
            }
        }
    }
    return z;
}

int check5(long l, int q, int hk) {
    if (check1a(l, q) && ((check2(l, q) && check3(l, q, hk)) || (!(check2(l, q)) && check4(l, q, hk))))
    
        return 1;
    else
        return 0;
    }
int check6(long l, int q, int hk)
{
    if (check1a(l, q) && ((check2(l, q) && check4(l, q, hk)) || (!(check2(l, q)) && check3(l, q, hk))))
        return 1;
    else
        return 0;
}

int check7(long l, int q, int hk)
{
    if ((check0(l, q) && check5(l, q, hk)) || (check1(l, q) && check6(l, q, hk)))
        return 1;
    else
        return 0;
}

int check8(long l, int q, int hk)
{
    if ((check0(l, q) && check6(l, q, hk)) || (check1(l, q) && check5(l, q, hk)))
        return 1;
    else
        return 0;
}

int check9(long l, int q, int hk)
{
    if ((check0(l, q) && check3(l, q, hk)) || (check1(l, q) && check4(l, q, hk)))
return 1;
else
    return 0;
}

int checkl0(long l, int q, int hk)
{
    if ((check0(l, q) && check4(l, q, hk)) || (check1(l, q) && check3(l, q, hk)))
        return 1;
    else
        return 0;
}

void main (void)
{
    int primes, cn;
    long int i, k, bound;
    int counter, countB, countCa, countCb, countFa, countFb, countGa;
    int countGb, countHa, countHb, countDa, countDb, countEa, countEb
        , countIa, countIb, countIc, countId, countIf, countIg, countIf;
    double y;
    y = 0;
    bound = 1;
    countB = 0;
    printf("Enter a prime p equal to 7 mod 8, class number for Q(sqrt(-2p))
        , and an upper bound for computation: \n");
    scanf("%d", &primes);
scanf("%d", &cn);
scanf("%ld", &bound);
for(k = 3; k <= bound; k+= 2){
    if (check1a(k,primes)){
        countB++;
        printf("%d. %ld is in list B. \n", countB, k);
    }
}

countCa = 0;
y = 0;
printf("\n");
for (k = 3; k <= bound; k+= 2){
    if (check0(k, primes)){
        countCa++;
        printf("%d. %ld is in list C1. \n", countCa, k);
    }
}

countCb = 0;
y = 0;
printf("\n");
for (k = 3; k <= bound; k+= 2){
    if (check1(k, primes)){
        countCb++;
        printf("%d. %ld is in list C2. \n", countCb, k);
    }
}
countDa = 0;
y = 0;
printf("\n");
for(k = 9; k <= bound; k += 8){
    if (check1a(k, primes))
        for (i = 1; i <= sqrt((double)((double)k)); i++){
            y = sqrt((k - pow((double)i, 2))/32);
            if (y == ((long)y)){
                countDa++;
                printf("%d. %ld is of the form (%ld)^2 + 32(%ld)^2. \n", countDa, k, i, (long) y);
                break;
            }
        }
}

countDb = 0;
y = 0;
printf("\n");
for(k = 9; k <= bound; k += 8){
    if (check1a(k, primes) && !(check2(k, primes))){
        countDb++;
        printf("%d. %ld is not of the form x^2 + 32y^2. \n", countDb, k);
    }
}
countEa = 0;
y = 0;
printf("\n");
for (k = 9; k <= bound; k += 8) {
    if (checkla(k, primes))
        for (i = 1; i <= sqrt(pow((double)k, (cn/4))); i++) {
            y = sqrt((pow((double)k, (cn/4)) - ((double)i * (double)i)) / (2 * (double)primes));
            if (y == ((long)y) && !( ((long)y) % k == 0 )) {
                countEa ++;
                printf("%d. (%ld)² is of the form %ld² + 2*%ld*%ld². \n", countEa, k, i, primes, (long)y);
                break;
            }
        }
}

countEb = 0;
y = 0;
printf("\n");
for (k = 9; k <= bound; k += 8) {
    if (checkla(k, primes))
        for (i = 1; i <= sqrt((pow((double)k, (cn/4))) / 2); i++) {
            y = sqrt((pow((double)k, (cn/4)) - 2 * ((double)i * (double)i)) / (double)primes);
            if (y == ((long)y) && !( ((long)y) % k == 0 )) {
                countEb ++;
                printf("%d. 2(%ld)² is of the form 2(%ld)² + %d(%ld)². \n", countEb, k, i, primes, (long)y);
                break;
            }
        }
}
countFa = 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+ = 8){
    if (check1a(k,primes) & & ((check2(k,primes) & & check3(k,primes,cn)) | |
     (!(check2(k,primes)) & & check4(k,primes,cn)))){
        countFa++;
        printf("%d. %ld is in list F1. \n",countFa, k);
    }
}

countFb = 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+ = 8){
    if (check1a(k,primes) & & ((check2(k,primes) & & check4(k,primes,cn)) | |
     (!(check2(k,primes)) & & check3(k,primes,cn)))){
        countFb++;
        printf("%d. %ld is in list F2. \n",countFb, k);
    }
}
countGa = 0;
y = 0;
printf("\n");
for(k = 9; k <= bound; k += 8){
    if ((check0(k, primes) && check5(k, primes, cn)) || (check1(k, primes) &&
        check6(k, primes, cn))){
        countGa++;
        printf("%d. %ld is in list G1. \n", countGa, k);
    }
}

countGb = 0;
y = 0;
printf("\n");
for(k = 9; k <= bound; k += 8){
    if ((check0(k, primes) && check6(k, primes, cn)) || (check1(k, primes) &&
        check5(k, primes, cn))){
        countGb++;
        printf("%d. %ld is in list G2. \n", countGb, k);
    }
}

countHa = 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+= 8){
    if ((check0(k, primes) && check3(k, primes)) || (check1(k, primes) &&
     check4(k, primes))){
        countHa++;
        printf("%d. %ld is in list H1. \n", countHa, k);
    }
}

countHb= 0;
y=0;
printf("\n");
for(k= 9; k <= bound; k+= 8){
    if ((check0(k, primes) && check4(k, primes)) || (check1(k, primes) &&
     check3(k, primes))){
        countHb++;
        printf("%d. %ld is in list H2. \n", countHb, k);
    }
}

countIa= 0;
y =0;
printf("\n");
for(k= 9; k <= bound; k+= 8){
    if (check3(k, primes) && check9(k, primes) && check5(k, primes) &&
     check7(k, primes)) {
        countIa++;
        printf("%d. %ld is in list I1. \n", countIa, k);
    }
}
countIb = 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+ = 8){
    if (check3(k,primes,cn) && check9(k, primes,cn) && check6(k, primes,cn)
        && check8(k, primes,cn)){
        countIb++;
        printf("%d. %ld is in list I2. \n",countIb, k);
    }
}

countIc = 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+ = 8){
    if (check4(k,primes,cn) && check9(k, primes,cn) && check6(k, primes,cn)
        && check7(k, primes,cn)){
        countIc++;
        printf("%d. %ld is in list I3. \n",countIc, k);
    }
}

countId = 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+= 8) {
    if (check4(k,primes,cn) && check9(k, primes,cn) && check5(k, primes,cn)
       && check8(k, primes,cn)) {
        countId++;
        printf("%d. %ld is in list 14. \n",countId, k);
    }
}

countIe= 0;
printf("\n");
for(k= 9; k <= bound; k+= 8) {
    if (check3(k,primes,cn) && check10(k, primes,cn) && check6(k, primes,cn) &&
       check7(k, primes,cn)) {
        countIe++;
        printf("%d. %ld is in list 15. \n",countIe, k);
    }
}

countIf= 0;
y = 0;
printf("\n");
for(k= 9; k <= bound; k+= 8) {
    if (check3(k,primes,cn) && check10(k, primes,cn) && check5(k, primes,cn)
       && check8(k, primes,cn)) {
        countIf++;
        printf("%d. %ld is in list 16. \n",countIf, k);
    }
}
countIg = 0;
y = 0;
printf("\n");
for(k = 9; k <= bound; k + = 8){
    if (check4(k, primes.cn) && check10(k, primes.cn) && check5(k, primes.cn)
        && check7(k, primes.cn)){
        countIg++;
        printf("%d. %ld is in list 17. \n", countIg, k);
    }
}

countIh = 0;
y = 0;
printf("\n");
for(k = 9; k <= bound; k + = 8){
    if (check4(k, primes.cn) && check10(k, primes.cn) && check6(k, primes.cn)
        && check8(k, primes.cn)){
        countIh++;
        printf("%d. %ld is in list 18. \n", countIh, k);
    }
}

printf("SUMMARY:\nB-%d \nC1-%d \nC2-%d \nD1-%d \nD2-%d \nE1-%d \nE2-%d \nF1-%d \nF2-%d \nG1-%d \nG2-%d \nH1-%d \nH2-%d \nI1-%d \nI2-%d \nI3-%d \nI4-%d \nI5-%d
97

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
\nI6-%d \nI7-%d \nI8-%d\n", countB, countCa, countCb, countDa, countDb
, countEa, countEb, countFa, countFb, countGa, countGb, countHa, countHb,
countIa, countIb, countIc, countId, countIe, countIf, countIg, count Ih);
printf("End. \n");
}
Vita

Robert B. Osburn was born on December 11, 1973 in Eunice, Louisiana. He received a bachelor of science and master of science degree in mathematics from Louisiana State University in August 1996 and December 1998 respectively. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in May 2001.
Candidate: Robert B. Osburn

Major Field: Mathematics

Title of Dissertation: Densities of 4-Ranks of \( K_2 \) of Rings of Integers

Approved:

J. Hurrelbrink
Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

[Signatures]

Date of Examination:

4/4/01