DISSERTATION

RELATIVE ORIENTED CLASS GROUPS OF QUADRATIC EXTENSIONS

Submitted by

Kelly A. O'Connor

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2024

Doctoral Committee:

Advisor: Rachel Pries

Jeffrey Achter
Mark Shoemaker
Maria Rugenstein

ABSTRACT

RELATIVE ORIENTED CLASS GROUPS OF QUADRATIC EXTENSIONS

In 2018 Zemková defined relative oriented class groups associated to quadratic extensions of number fields L/K, extending work of Bhargava concerning composition laws for binary quadratic forms over number fields of higher degree. This work generalized the classical correspondence between ideal classes of quadratic orders and classes of integral binary quadratic forms to any base number field of narrow class number 1. Zemková explicitly computed these relative oriented class groups for quadratic extensions of the rationals. We consider extended versions of this work and develop general strategies to compute relative oriented class groups for quadratic extensions of higher degree number fields by way of the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the set of real embeddings of K. We also investigate the binary quadratic forms side of Zemková's bijection and determine conditions for representability of elements of K.

Another project comprising work done jointly with Lian Duan, Ning Ma, and Xiyuan Wang is included in this thesis. Our project investigates a principal version of the Chebotarev density theorem, a famous theorem in algebraic number theory which describes the splitting of primes in number field extensions. We provide an overview of the formulation of the principal density and describe its connection to the splitting behavior of the Hilbert exact sequence.

ACKNOWLEDGEMENTS

When choosing where to go to graduate school, I was given some advice. It was to remember that the six years I spent getting my PhD were still years of my life. Looking back I realize I've built an unexpectedly beautiful life here in Fort Collins. That's thanks to a lot of people, the list of which could never fit among these pages. What follows is but a glimpse of the gratitude I feel toward each person who helped me shape the past six years.

Thank you Rachel, for advising me mathematically, and advocating for me in many ways. Thank you especially for encouraging me in my passion for outreach. A lot of young women got to feel celebrated and supported mathematically because of you.

To my many other mathematical mentors. A special thank you to Lian for your kindness and guidance. To Leon, Tushar, Whitney, Susan and Eddie, thanks for inspiring me to do this in the first place.

To Mom, Dad, Paige, and Ryan. Thank you for making home a place I always miss and can never get back to fast enough. To Grandma Joyce and Nanny. Thank you for showing me the beauty of a long life. To the family members I gained here - Pat, Susie, Sean and Cathy.

To Amie Bray, a shining light and reminder of God's goodness at every turn. Out of all of the people in the world, I'm glad I got to have you as my best friend in graduate school. You challenge me to be a better number theorist, but never let me believe that's the most important part of me.

To Michael Moy, thanks for finding my mistakes and introducing me to a lot of beautiful math. You're a brilliant mathematician, Michael, but an even more brilliant friend. Every once in a while you meet someone who you feel really lucky to know. You're one of those people for me.

To the old friends who supported me from the start - Maggie, Jordan, Morgan, and Maria. To all of the friends I found here: Erin, Tatum, Seth, Kyle, Brian, Mats, Danny, Harley, Juanita, Vlad, and Wei Yu. To Nick, thanks for always encouraging me from afar.

To those who have strengthened me in my faith the past six years. A special thank you to Sister Lucia Christi for your light and your love. Your "yes" changed my life. Thank you also to Sister

Marie Veritas, Ron, Sister Pam, Hayley, Fr. Simone and Fr. Matt. To the faithful in Poland! Our Lady of Częstochowa, pray for us!

It's occurred to me there are two people I'd like to thank whose names I don't know. To the man who sits in the middle of St. Joe's every morning at 7:00 am. I've learned a lot about steadfastness from you. You've inspired my faith more than you probably will ever know. Second, to the janitor who rides the tricycle to school. One day you told me that I was your best friend, and a lot of days I'd have to say the same to you. Thank you for your joy. I hope to find joy like that someday too. Thank you both for being the most unexpected inspirations during my time in Fort Collins. I really hope I get to know you by name one day.

Lastly, thank you to my husband, Justin. Marrying you will always be the best thing that happened to me here. I love you.

DEDICATION

To the Sisters of Life

"...and nothing would again be casual and small"

TABLE OF CONTENTS

Introduction

Perhaps the most beautiful development in the theory of binary quadratic forms was the work of Gauss in his *Disquisitiones Arithmeticae* in which he described the underlying (group) structure of binary quadratic forms and what we now know as Gauss composition. The power of this discovery lies in a correspondence between classes of integral binary quadratic forms and ideal classes of quadratic orders. In 2004, a series of articles of Bhargava [1], [2], and [3] explained geometric approaches to understanding composition laws for binary quadratic forms and generalizations involving correspondences for higher degree number fields. The work of Bhargava in [1] was further generalized, for instance in [4], [5] and in 2018 by Zemková [6]. Zemková introduced the idea of *relative oriented class groups* which allows one to consider a bijection between classes of oriented ideals and primitive quadratic forms defined over a totally real number field with narrow class number 1. Zemková explicitly computed such oriented class groups for real quadratic number fields, and described totally positive definite quadratic forms in terms of oriented ideals [6, Section 2.5]. It is the generalization of Zemková from which we build our work.

This work emerged amidst a long history of human interest in quadratic forms, the study of which dates back to 1900-1600 BC. Babylonian tablets comprise possibly the earliest recorded example of humans doing math for fun, albeit with significant success: namely determining there are infinitely many primitive Pythagorean triples [7]! Fermat studied quadratic forms of the form $x^2 + ny^2$ as early as 1640, and Euler, fascinated by Fermat's theorems, dedicated decades of his life to proving them. Throughout this time, Euler developed important number theoretic concepts, most notably quadratic reciprocity (see [8, Chapter 1 Section 1]). Development of the theory of integral binary quadratic forms, as we know it today, began with the work of Lagrange, who defined the notions of discriminant, equivalence and reduced form. The primary questions regarding binary quadratic forms in the seventeenth and eighteen centuries concerned representation of numbers, a problem considered by Brahmagupta in the 7th century, and one we consider in the setting of this

work (see Chapter 4). The interested reader can learn more about the history of the study of binary quadratic forms in [7, Chapter 1] and [8, Chapter 1 Section 2].

Motivated by Proposition 2.9 of [6], we seek strategies to compute the relative oriented class groups of quadratic extensions L/K, when K is taken to be a totally real number field with narrow class number 1 and degree $\geqslant 2$. We begin by laying the foundation of our studies in Chapter 1 where we provide a review of number fields, including details about units in the rings of integers of such fields. We continue by recalling the definitions of the ideal class group and narrow class group. As a historical remark, we briefly summarize ideas involving binary quadratic forms defined over the rational numbers. This summary is meant to foreshadow our work, by outlining the classical bijection between class groups of orders in quadratic number fields and classes of binary quadratic forms.

Chapter 2 is dedicated to setting up the necessary definitions and theory for the specific setting of our investigation. We discuss the assumptions on our base field, a totally real number field with narrow class number 1. We describe the relative quadratic extensions we will be studying and define the relative oriented class group as defined in [9]. We end this chapter by recalling the bijection described by Zemková.

Chapter 3 provides the background and proofs of our main theorems. We begin by discussing a general strategy for computing relative oriented class groups in terms of the sign configurations of norms of units in L. In particular, we compute subgroups of norms of units by considering the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the set of real embeddings of K. These subgroups are important, as they give way to a relationship between the relative oriented class group of L/K with the class group of L (see [10, Proposition 2.19]). We outline cases in which our work leads to explicit descriptions of the relative oriented class group and others in which our computations reduce the question of computing the relative oriented class group to a group extension problem. Also included in Chapter 3 are some special cases we considered throughout this work. We end the chapter by describing how our computations lead to descriptions of the binary quadratic forms side of the bijection.

In Chapter 4 we consider the representation problem for the quadratic forms under consideration. We begin the chapter with results which can be viewed as natural generalizations of the classical case to our present setting. We then explain connections between the subgroups under consideration in Chapter 3 and representability of elements of the ring of integers of K.

We end our discussion about relative oriented class groups with Chapter 5 in which we outline possibilities of future work. These include utilizing tools related to the extension problem and homological algebra to classify the relative oriented class group in greater generality. These methods are reliant on understanding the systems of fundamental units of the extensions L, as such we outline one particular special case of interest, the case when $L/\mathbb{Q}$ is not Galois and not pure. We also briefly outline the possibility of extending the results in this work to cubic analogues.

One can view the motivation of the investigation outlined in Chapters 1-5 as a generalization of a classical result. In a similar way, Chapter 6 is dedicated to a second project which is a refinement of a different classical theorem. At the time of Gauss it was already observed that there are the "same number" of prime integers which satisfy the congruence conditions $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$. This phenomenon can be explained by the *Chebotarev density theorem*, which describes the distribution of primes into factorization types. Indeed, in the ring of Gaussian integers, $\mathbb{Z}[i]$, the prime $5 = (1-2i)(1+2i)$, whereas $2 = -i(1+i)^2$, and 3 remains prime. We call these three factorization types *split*, *ramified*, and *inert*. In $\mathbb{Z}[i]$, primes which are split are those congruent to $1 \bmod 4$ and those which are inert are those congruent to $3 \bmod 4$. The Chebotarev density theorem then implies the densities of split primes, those congruent to $1 \bmod 4$, and inert primes, those congruent to $3 \bmod 4$, both approach 1/2.

In joint work with Duan, Ma, and Wang [11], we considered how the density analyzed in the Chebotarev density theorem would change if we only consider primes which split into a product of *principal* prime ideals, meaning those with a single generator. We begin the chapter by recalling the natural density computed in the Chebotarev density theorem. Given a finite Galois extension K/k, we define a principal density and prove that it is well defined. We describe a connection between the splitting of the associated Hilbert exact sequence and positivity of the principal density. We

also prove an effective bound which can be used to verify the non-splitting of the Hilbert exact sequence, and provide a concrete example to demonstrate its use. Finally, we discuss a generalized version of the principal density, including its relationship with determining the structure of the class group Cl_K.

Chapter 1

Preliminaries

In this chapter we summarize various foundational concepts which will be utilized throughout our discussion. We end the chapter by presenting the classical correspondence between classes of integral quadratic forms and ideal classes of quadratic orders.

1.1 Number Fields

Let K be a number field. Then K is a finite dimensional vector space over $\mathbb{Q}$. We denote the extension $K/\mathbb{Q}$. We call the dimension of K over $\mathbb{Q}$ the *degree* of K and denote it by $[K : \mathbb{Q}]$. In a similar way, we may consider number fields L which are finite extensions of K and write L/K and $[L : K]$ for the extension and degree, respectively. Throughout our discussion, we say that such an extension is *Galois* over $\mathbb{Q}$ (or K) when $|\text{Aut}(K/\mathbb{Q})| = [K : \mathbb{Q}]$ (likewise $|\text{Aut}(L/K)| = [L : K]$). In this case, our extension is equipped with a *Galois group* written $\text{Gal}(K/\mathbb{Q}) = \text{Aut}(K/\mathbb{Q})$ (or $\text{Gal}(L/K) = \text{Aut}(L/K)$) which is the group of automorphisms of K which fix $\mathbb{Q}$ (or on L which fix K).

For a degree n number field K, there exist n embeddings $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$. It may be the case that $\sigma_i(K) \subset \mathbb{R}$ for some number of the σ_i. Denote by r_1 the number of real embeddings of K and by r_2 the number of *pairs* of complex embeddings of K. In general, for a number field with degree n, we have $n = r_1 + 2r_2$. We say K is *totally real* if all of the embeddings $\sigma_i : K \to \mathbb{C}$ lie in $\mathbb{R}$ (i.e. if $r_1 = n$) and *totally imaginary* if none of its embeddings into $\mathbb{C}$ lie in $\mathbb{R}$. Over $\mathbb{Q}$, Galois extensions must either be totally real or totally imaginary.

Throughout our main discussion, we will take $K/\mathbb{Q}$ to be a totally real number field and L to be some relative degree 2 extension of K, that is $[L : K] = 2$. If we take L to be a totally imaginary degree 2 extension of the totally real field K, as in Section 3.3.2, then L/K is a *CM extension*.

Example 1.1. Consider the Gaussian rationals, $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. One quickly sees $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, that $\mathbb{Q}(i)$ is Galois with $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, generated by complex conjugation, and that $\mathbb{Q}(i)$ is a CM extension.

As in the previous example, take F to be a degree 2 extension of $\mathbb{Q}$. Then F is called a *quadratic* number field and such extensions are well understood. For $d \in \mathbb{Z}$, square-free, $F = \mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ with $\text{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ where the nonidentity element $\sigma \in \text{Gal}(F/\mathbb{Q})$ is given by $\sigma(\sqrt{d}) = -\sqrt{d}$. We will see the analogous notion of *relative* quadratic extensions in Section 2.2. When $F/\mathbb{Q}$ is taken to be a quadratic extension, the *norm* of an element $a \in F$ is then given by $N_{F/\mathbb{Q}}(a) = a\sigma(a)$. More generally, for any Galois extension L/K, the norm of $a \in L$ is given by

$$N_{L/K}(a) = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(a).$$

Norms of units in relative quadratic extensions will be of special importance to us. As such, we now turn our attention to groups of units.

1.2 Groups of Units

Just as $\mathbb{Z} \subset \mathbb{Q}$, we denote by $\mathcal{O}_K$ the *ring of integers* of K, which consists of all elements of K which satisfy a monic polynomial with integer coefficients. Further, sitting inside $\mathcal{O}_K$ is its *group of units* which we denote by $\mathcal{U}_K$. Throughout the discussion, we may refer to the elements of $\mathcal{U}_K$ as the "units of K," though we of course mean the units of $\mathcal{O}_K$. Determining the units of $\mathcal{O}_K$ can be difficult in general, but we glean useful information from the following classical result in algebraic number theory:

Theorem 1.2 (Dirichlet's Unit Theorem)**.** *Let K be a number field. Denote by r_1 the number of real embeddings of K and by r_2 the number of pairs of complex embeddings of K. Then the group of units of $\mathcal{O}_K$ is a finitely generated abelian group of the form*

$$\mathcal{U}_K \cong \mu_{\mathcal{O}_K} \times \mathbb{Z}^R$$

where $\mu_{\mathcal{O}_K}$ is the finite cyclic group of roots of unity of $\mathcal{O}_K$ and $R = r_1 + r_2 - 1$ is the rank of $\mathcal{U}_K$.

A *system of fundamental units* is a generating set, $\{\varepsilon_1, \ldots, \varepsilon_R\}$, for $\mathcal{U}_K/(\mu_{\mathcal{O}_K})$. In particular, Dirichlet's Unit Theorem implies that every element of the unit group $\mathcal{U}_K$ can be written uniquely as $\zeta\varepsilon_1^{m_1} \cdots \varepsilon_R^{m_r}$ where ζ is some root of unity of $\mathcal{O}_K$ and $m_1, \ldots, m_R \in \mathbb{Z}$. In the case that $r_1 > 0$, note that we just have $\mu_{\mathcal{O}_K} = \{1, -1\}$ as these are the only roots of unity in the real numbers.

Example 1.3. Note that for the case of a quadratic extension $F = \mathbb{Q}(\sqrt{d})$, we have that the rank of $\mathcal{U}_F$ is 1 if $d > 0$ and 0 if $d < 0$.

For our purposes, when we take the base field K to be a real quadratic number field, we will simply have $\mathcal{O}_K = \{\pm\varepsilon_K^m\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ where ε_K is the fundamental unit of K, normalized to be greater than 1.

We end this section with an important fact about the fundamental unit of K, which foreshadows our investigation in the next two sections.

Lemma 1.4. *[[12], Exercise 7.1] Let $d > 0$ be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$. Let x_0, y_0 be the uniquely determined rational integer solution to*

$$x^2 - dy^2 = -4,$$

or in the case that no rational integer solution exists, the smallest solution $x_0, y_0 > 0$ to

$$x^2 - dy^2 = 4.$$

Then,

$$\varepsilon_K = \frac{x_0 + y_0\sqrt{d}}{2}$$

is a fundamental unit of K.

Now that we have given an overview of the structure of the unit group of a number field, we discuss signs of units. That is, the signs realized by units after being embedded into $\mathbb{R}$. Not only

will signs of units lead to a definition important to our discussion, but in many ways, signs of units lie at the heart of our main results in Chapter 3.

1.3 Signs of Units

Given a finite number field K, Dirichlet's Unit Theorem gives us a description of the group of units of K, from which we can describe individual units in terms of the generating set of $\mathcal{U}_K/(\mu_{\mathcal{O}_K})$. An important step in our investigation will be to consider the images of these units under the real embeddings of K, in particular, once embedded into the real numbers, we can consider the signs of their images. With this task in mind, we let K be a number field with r real embeddings $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$.

Definition 1.5. An element $x \in K$ is *totally positive* if $\sigma_i(x) > 0$ for all i.

Example 1.6. Let $K = \mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. The two embeddings $K \hookrightarrow \mathbb{R}$ send $\sqrt{5}$ to itself and $-\sqrt{5}$, respectively. Consider two elements 1 and $\frac{1+\sqrt{5}}{2}$. Since $\sigma_1(\frac{1+\sqrt{5}}{2}) = \frac{1+\sqrt{5}}{2} > 0$ but $\sigma_2(\frac{1+\sqrt{5}}{2}) = \frac{1-\sqrt{5}}{2} < 0$, we have that $\frac{1+\sqrt{5}}{2} \in K$ is not totally positive. However, $1 \in K$ is totally positive, since it is sent to itself under both embeddings.

The two elements $1, \frac{1+\sqrt{5}}{2} \in K$ are actually elements of $\mathcal{U}_K$, and the previous example demonstrates one of the motivating questions of our work, in particular, determining the signs of units in K. As such, we will denote by $\mathcal{U}_K^+$ the subgroup of totally positive units of K. The behavior of the units in Example 1.6 is so special, we make the following definition.

Definition 1.7. A number field K is said to have units with *independent signs* if and only if for each embedding $\sigma : K \hookrightarrow \mathbb{R}$ there is some $u \in \mathcal{U}_K$ whose image under σ is negative but whose image under every other real embedding of K is positive.

Note that totally complex number fields have no real embeddings, and thus have units with independent signs by definition.

Example 1.8. Notice that $K = \mathbb{Q}(\sqrt{5})$ has units with independent signs. For example, the image under σ_2 of $\frac{1+\sqrt{5}}{2}$ is negative, but its image under σ_1 is positive. Now, consider another unit of K, namely $\frac{1-\sqrt{5}}{2}$, whose image under σ_1 is negative, but $\sigma_2(\frac{1-\sqrt{5}}{2}) = \frac{1+\sqrt{5}}{2} > 0$.

For the general case of totally real number fields, the condition of having units of independent signs is one that can be understood in terms of the subgroup of totally positive units, $\mathcal{U}_K^+$. We turn to the following result as stated in [13, Lemma 2.12]:

Lemma 1.9. *Let K be a totally real number field. Then K has units with independent signs if and only if every element $u \in \mathcal{U}_K^+$ is a square.*

Though we will continue with some preliminary background information in Section 1.4, we pause now and look ahead to our main focus of the current investigation. Suppose we consider a tower of field extensions, namely $L/K/\mathbb{Q}$ with K a totally real extension of $\mathbb{Q}$ and L a relative quadratic extension of K. This will be part of the set-up for our main theorems. It turns out that in this setting, we can determine exactly when the extension L has units with independent signs. Although we will not require this condition on our field L, the usefulness of such a result may come into play in natural generalizations of our work, for this reason, we include the statement here.

Theorem 1.10. *[13, Theorem 12.4] Let K be a real quadratic number field and L/K a real quadratic extension, then L has units with independent signs if and only if*

1. *K has units with independent signs and*
2. *$H^0(\mathbb{Z}/2\mathbb{Z}, \mathcal{U}_L)$ is trivial.*

We have developed the definitions related to signs of units which will come into play in our investigation. In the next section we will recall the definition of two groups related to each number field.

1.4 Class Group and Narrow Class Group

Recall that for a number field K, we denote by $\mathcal{O}_K$ its ring of integers. An important fact about the rings of integers of number fields is that they are *Dedekind domains* and we can therefore describe a theory of fractional ideals on $\mathcal{O}_K$. By a *fractional ideal* of $\mathcal{O}_K$, we mean an $\mathcal{O}_K$-submodule I of K such that there exists some nonzero $\alpha \in \mathcal{O}_K$ such that αI is an (integral) ideal of $\mathcal{O}_K$.

One can define multiplication of fractional ideals in the following way:

$$IJ = \{x_1y_1 + \ldots + x_ny_n \mid x_i \in I, y_i \in J\}.$$

Further, as $\mathcal{O}_K$ is a Dedekind domain, every nonzero fractional ideal I has an inverse, some nonzero fractional ideal J such that $IJ = \mathcal{O}_K$. In fact, under this operation, the set of nonzero fractional ideals of $\mathcal{O}_K$ forms an abelian group which we denote by I_K. We denote by P_K the subgroup of nonzero *principal* fractional ideals of $\mathcal{O}_K$, those generated by a single element. From this, we define the *ideal class group* of K, which is the quotient

$$Cl_K := I_K/P_K.$$

The following is an important classical result.

Theorem 1.11. *Let K be a number field. The ideal class group of K is a finite abelian group.*

We denote the order of Cl_K order by h_K and call it the *class number* of K. Number fields with class number 1, that is with trivial class group, are those with $\mathcal{O}_K$ a unique factorization domain.

A larger quotient group called the *narrow* class group of K is defined in a similar way, taking into consideration fractional ideals generated by totally positive elements of K.

Definition 1.12. The narrow class group of K is the quotient

$$Cl_K^+ := I_K/P_K^+$$

where P_K^+ is the subgroup of totally positive principal fractional ideals, i.e. fractional ideals of the form $(\alpha) = \alpha\mathcal{O}_K$, with α a totally positive element of K.

We then say two fractional ideals I, J of $\mathcal{O}_K$ are *equivalent in the narrow sense* if and only if there is a totally positive element $\alpha \in K^\times$ such that $I = \alpha J$. Then the narrow class group of K is the group of these equivalence classes of fractional ideals of $\mathcal{O}_K$. Just as in the case of ideal class groups, we call the order of the narrow class group of K the *narrow class number* of K and denote it by h_K^+. We can relate the class number and narrow class number in the following way: there is a natural surjective map

$$\nu : Cl_K^+ \to Cl_K.$$

Consider the kernel of ν. There is no reason for ν to be bijective, that is, the kernel of this map is not necessarily trivial. However, we see our work in Section 1.3 pay off as $\ker(\nu)$ can be described in terms of the signs of units of K. In particular, K having units of independent signs is equivalent to saying that ν is an isomorphism [13, 11.2]. In general, we have $h_K^+ = 2^a h_K$ where $2^a = |\ker(\nu)|$ (see [13, Chapter 12]). Therefore, we see that h_K^+ is odd exactly when h_K is odd and K has units with independent signs. In fact, by [14, Chapter 5, 1.12] and [6, Corollary 4.3] we have that a number field K has narrow class number 1 if and only if it has class number 1 and units of independent signs. This characterization gives us a way to begin to produce data about which number fields have the property of having trivial narrow class group. This condition will be imposed on the number fields appearing in our main results. As such, we pause to consider some data, and strategies of obtaining it, concerning number fields with narrow class number 1.

Data

In this subsection we provide some data concerning totally real number fields of degree 2 or 3 over $\mathbb{Q}$ which have narrow class number 1. An algorithm for determining which totally real cubic number fields have units of independent signs is also outlined. All number field data was collected from The L-Functions and Modular Forms Database (LMFDB) [15]. Computations were completed using SageMath, the Sage Mathematics Software System (Version 9.0) [16].

Table 1.1: All real quadratic number fields up to discriminant 100 are listed in this table. The number fields with narrow class number 1 are indicated in green, and also in the third and sixth columns.

Polynomial	Discriminant	$h_K^+ = 1$	Polynomial	Discriminant	$h_K^+ = 1$
$x^2 - x - 1$	5	yes	$x^2 - x - 13$	53	yes
$x^2 - 2$	2^3	yes	$x^2 - 14$	$2^3 \cdot 7$	no
$x^2 - 3$	$2^2 \cdot 3$	no	$x^2 - x - 14$	$3 \cdot 19$	no
$x^2 - x - 3$	13	yes	$x^2 - x - 15$	61	yes
$x^2 - x - 4$	17	yes	$x^2 - x - 17$	$3 \cdot 23$	no
$x^2 - x - 5$	$3 \cdot 7$	no	$x^2 - x - 18$	73	yes
$x^2 - 6$	$2^3 \cdot 3$	no	$x^2 - 19$	$2^2 \cdot 19$	no
$x^2 - 7$	$2^2 \cdot 7$	no	$x^2 - x - 19$	$7 \cdot 11$	no
$x^2 - x - 7$	29	yes	$x^2 - 22$	$2^3 \cdot 11$	no
$x^2 - x - 8$	$3 \cdot 11$	no	$x^2 - x - 22$	89	yes
$x^2 - x - 9$	37	yes	$x^2 - 23$	$2^2 \cdot 23$	no
$x^2 - x - 10$	41	yes	$x^2 - x - 23$	$3 \cdot 31$	no
$x^2 - 11$	$2^2 \cdot 11$	no	$x^2 - x - 24$	97	yes

Upon considering this table, one may notice all real quadratic number fields with class number 1 and prime discriminant less than 100 have narrow class number 1. We note that this pattern continues only until discriminant 457. The table below contains a list of the defining polynomials of all totally real cubic number fields, $K/\mathbb{Q}$, up to discriminant 1000.

Table 1.2: All totally real cubic number fields up to discriminant 1000 with class number 1 which also have narrow class number 1, ordered by discriminant.

Polynomial	Discriminant	Galois	Polynomial	Discriminant	Galois
$x^3 - x^2 - 2x + 1$	7^2	yes	$x^3 - 3x - 1$	3^4	yes
$x^3 - x^2 - 3x + 1$	$2^2 \cdot 37$	no	$x^3 - x^2 - 4x - 1$	13^2	yes
$x^3 - x^2 - 4x + 2$	$2^2 \cdot 79$	no	$x^3 - x^2 - 4x + 1$	$3 \cdot 107$	no
$x^3 - x^2 - 6x + 7$	19^2	yes	$x^3 - x^2 - 5x - 1$	$2^2 \cdot 101$	no
$x^3 - x^2 - 5x + 4$	$7 \cdot 67$	no	$x^3 - 5x - 1$	$11 \cdot 43$	no
$x^3 - x^2 - 5x + 3$	$2^2 \cdot 3 \cdot 47$	no	$x^3 - x^2 - 6x - 2$	$2^3 \cdot 71$	no
$x^3 - 6x - 3$	$3^3 \cdot 23$	no	$x^3 - x^2 - 7x + 8$	733	no
$x^3 - 6x - 2$	$2^2 \cdot 3^3 \cdot 7$	no	$x^3 - x^2 - 6x + 5$	$5 \cdot 157$	no
$x^3 - 6x - 1$	$3^3 \cdot 31$	no	$x^3 - 7x - 4$	$2^2 \cdot 5 \cdot 47$	no
$x^3 - x^2 - 10x + 8$	31^2	yes	$x^3 - x^2 - 6x + 3$	$3 \cdot 331$	no

In all of the above cases, K has class number 1. To verify that K has units of independent signs, and therefore narrow class number 1 (see [6, Cor. 4.3]), we check the following three conditions:

1. $\underline{\text{sgn}}(u_i) \neq (1,1,1), (-1,-1,-1)$ for $i = 1, 2$ and
2. $\underline{\text{sgn}}(u_1) \neq \underline{\text{sgn}}(u_2)$ and
3. $\underline{\text{sgn}}(u_1) \cdot \underline{\text{sgn}}(u_2) \neq (1,1,1), (-1,-1,-1)$.

where $\{u_1, u_2\}$ is a system of fundamental units of K and where the ith entry of the tuple $\underline{\text{sgn}}(u)$ is determined by considering whether $\sigma_i(u)$ is a positive or negative real number. Such tuples of signs will be defined and utilized extensively in Section 2.4, but we use this notation now for brevity.

If all three conditions hold, K has units of all signs.

Lemma 1.13. *Let K be a totally real cubic number field with class number 1. Then K has narrow class number 1 if and only if the three conditions above hold.*

Proof. Notice that K has units of independent signs if and only if $\underline{\text{sgn}}(\mathcal{U}_K) = \{\underline{\text{sgn}}(u) \mid u \in \mathcal{U}_K\} = \langle \pm 1 \rangle^3$. Consider all elements of $\langle \pm 1 \rangle^3$:

$$(1,1,1) \qquad (-1,1,1) \qquad (1,-1,1) \qquad (1,1,-1)$$

$$(-1,-1,-1) \quad (1,-1,-1) \quad (-1,1,-1) \quad (-1,-1,1)$$

organized such that elements in the same column differ by a factor of $\underline{\text{sgn}}(-1) = (-1,-1,-1)$. Then, in order for u_1 and u_2 to satisfy the three conditions above, they must be such that

1. neither $\underline{\text{sgn}}(u_1)$ nor $\underline{\text{sgn}}(u_2)$ comes from the first column and
2. $\underline{\text{sgn}}(u_1)$ and $\underline{\text{sgn}}(u_2)$ are not the same element and
3. $\underline{\text{sgn}}(u_1)$ and $\underline{\text{sgn}}(u_2)$ can not be in the same column.

The only option then is for u_1 and u_2 to have sign configurations appearing, one each, in two of the rightmost three columns. WLOG say $\underline{\text{sgn}}(u_1)$ is an element of the second column and $\underline{\text{sgn}}(u_2)$ appears in the third column. This means $\underline{\text{sgn}}(u_1 u_2)$ appears in the third column. Therefore, since $\mathcal{U}_K$ is a group containing 1 and -1, and the sign map is multiplicative, all possible sign configurations are obtained and K has units of independent signs. For the backward direction, notice that K having units of independent signs contradicts each of the three conditions, since the negation of any of the three implies $\mathcal{U}_K$ contains units only realizing two of the four columns. □

We make note that SageMath does include a command for computing the narrow class group of a number field. Therefore, one can automatically obtain lists of number fields with narrow class number 1. Nevertheless, the above algorithm has been included in this work in order to familiarize the reader with signs of units, and is a helpful exercise in understanding related computations which arise in Chapter 3.

We now turn to our last preliminary section to consider binary quadratic forms. After developing some basic notions, we will come to understand the connection between the groups considered above and equivalence classes of binary quadratic forms.

1.5 Binary Quadratic Forms Over $\mathbb{Q}$

We will now discuss another object which will be important in our work, namely binary quadratic forms, along with brief overviews of representability and equivalence. Let K be a number field. By a *binary quadratic form defined over* K, we mean a homogeneous degree two polynomial with coefficients in $\mathcal{O}_K$:

$$Q(x, y) = ax^2 + bxy + cy^2,$$

with $a, b, c \in \mathcal{O}_K$. We will often refer to such polynomials simply as "quadratic forms." We define the *discriminant* of Q to be $\text{Disc}(Q) = b^2 - 4ac$.

Though we will eventually work with binary quadratic forms defined over more general number fields K, we begin with a brief overview of the case when $K = \mathbb{Q}$. The theory of binary quadratic forms with integer coefficients is one of the longest studied and most important topics in number theory. For more information on the historical development of the study of binary quadratic forms over $\mathbb{Q}$, we refer the reader to [7] and [8].

One of the first classes of questions regarding quadratic forms were *representation* problems.

Definition 1.14. An integral binary quadratic form Q *represents* an integer n, or n is *represented* by Q, if there exist $x_0, y_0 \in \mathbb{Z}$ such that $Q(x_0, y_0) = n$. We say n is *properly* represented by Q if x_0 and y_0 are relatively prime.

Thus, given an integral binary quadratic form and integer n, one can ask if such a pair x_0, y_0 exists such that $Q(x_0, y_0) = n$. As referenced in the introduction to this work, the representation problem is truly ancient.

Example 1.15. Brahmagupta, who lived from 598-668 studied representability of integers by binary quadratic forms including $x^2 - cy^2$ for $c \in \mathbb{Z}^+$. Given one solution to the representation problem for this form, he could produce infinitely many more!

Also mentioned in the introduction was the work of Fermat and Euler, of which we provide the following example.

Example 1.16. Many famous theorems of Fermat and Euler can be understood in the context of the representation problem. For example, the theorem that for odd primes p,

$$p = x^2 + y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1 \bmod 4$$

is a solution to infinitely many representation problems of the quadratic form $x^2 + y^2$.

A theme which will come up time and again in our investigation is that classes of binary quadratic forms are in bijection with classes of ideals. The first example of this was determined

by Gauss in his *Disquisitiones Arithmeticae*, and although we will not include all details of the bijection in our discussion, a careful development of the theory is given in [8].

Definition 1.17. A binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is called *positive definite* if Q represents only positive values and *primitive* if a, b, and c are coprime.

The condition of being positive definite is completely determined by the sign of the discriminant. That is, a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is positive definite if and only if $\text{Disc}(Q) < 0$ and $a > 0$ (see [17], Prop 2.1). We define an equivalence of positive definitive, primitive quadratic forms in the following way.

Define the action of $SL_2(\mathbb{Z})$ on a binary quadratic form by

$$(ax^2+bxy+cy^2)\cdot\begin{pmatrix} p & q \\ r & s \end{pmatrix} = a(px+qy)^2+b(px+qy)(rx+sy)+c(rx+sy)^2 = Q(px+qy, rx+sy).$$

We can write this action another way, namely for a binary quadratic form $Q(x, y)$ and a matrix $M \in SL_2(\mathbb{Z})$, we write

$$Q(x, y) \cdot M = Q(x'.y') \text{ where } \begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}.$$

We make special note that the action of $SL_2(\mathbb{Z})$ is discriminant-preserving. We say $Q_1 \sim Q_2$ if and only if there is some $M \in SL_2(\mathbb{Z})$ such that $Q_1 \cdot M = Q_2$.

Remark 1.18. One may drop the primitive and positive definite condition and instead define an action by $GL_2(\mathbb{Z})$. An element $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$ acts on a binary quadratic form $Q(x, y)$ by

$$Q(x, y) \cdot \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \frac{1}{\det M} Q(px + qy, rx + sy).$$

This action is called the *twisted* $GL_2(\mathbb{Z})$ action on binary quadratic forms (see [4] Sec. 1).

An idea which unifies the discussions of representability and equivalence of binary quadratic forms is that equivalent forms represent the same integers. Therefore, one can simplify a particular representation problem by replacing the quadratic form in question with an equivalent one. This idea, in the setting of binary quadratic forms defined over higher degree number fields, will be referenced again in Chapter 4. Also investigated in Chapter 4 is a generalization of the following lemma.

Lemma 1.19. *[8, Lemma 2.3] A form $Q(x, y)$ properly represents an integer m if and only if $Q(x, y)$ is equivalent to the form $mx^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$.*

Before we give the bijection which relates binary quadratic forms and ideal classes, we remark that an *order* in a quadratic field K is some $\mathcal{O} \subset K$ which is a subring of K containing 1, is finitely generated as a $\mathbb{Z}$ module, and contains a $\mathbb{Q}$ basis of K. We can then define the ideal class group and narrow class group of $\mathcal{O}$ in the same way we do for $\mathcal{O}_K$. The ring of integers of K, $\mathcal{O}_K$, is the maximal order of K.

We now give the correspondence between classes of binary quadratic forms over $\mathbb{Q}$ and elements of the class group of a quadratic order. What's more, we will see that a second case gives a bijection between classes of quadratic forms and the elements of the narrow class group of a quadratic order.

Theorem 1.20. *(E.g. see [18, Thms. 5.2.8 and 5.2.9] and [4, Thm. 1.1]) Let D be a non-square integer congruent to 0 or 1 $\bmod 4$. Let $\mathcal{O}$ be the unique quadratic order of discriminant D.*

1. *If $D < 0$, then there is a bijection between the $SL_2(\mathbb{Z})$-equivalence classes of positive definite, primitive, binary quadratic forms over $\mathbb{Q}$ of discriminant D and the elements of the class group of $\mathcal{O}$.*

2. *If $D > 0$, then there is a bijection between the $SL_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms over $\mathbb{Q}$ of discriminant D and elements of the narrow class group of $\mathcal{O}$.*

For more information on the classical correspondence, we refer the reader to [8, Chapter 2, Sec.7] and [19, Chapter 2, Sec. 7.5].

Although this ends our jaunt through the theory of binary quadratic forms defined over $\mathbb{Q}$, we invite the reader to revisit this section and draw analogies between the content of Theorem 1.20 and the generalizations we describe in Section 2.5 and the representation problem for integral binary quadratic forms and our work in Chapter 4. Of course, before moving to these generalizations, we will discuss the set-up of our investigation in the next chapter.

Chapter 2

Relative Quadratic Extensions and Binary Quadratic Forms

2.1 Totally Real Number Fields of Narrow Class Number 1

Throughout our discussion, we take K to be totally real. We also take K to have narrow class number 1, which is equivalent to requiring K to have class number 1 and $\mathcal{U}_K$ to contain units of all signs. This section is dedicated to providing examples of such fields and explaining the significance of this assumption on the field K. We begin with an example which will be referenced throughout our work.

Example 2.1. The number field $K = \mathbb{Q}(\sqrt{5})$ has two real embeddings given by $\sigma_1 : \sqrt{5} \mapsto \sqrt{5}$ and $\sigma_2 : \sqrt{5} \mapsto -\sqrt{5}$. In this case K has class number 1 and we see in the table below that K also has units of all signs as:

$\mu \in \mathcal{U}_K$	$\text{sgn}(\sigma_1(\mu))$	$\text{sgn}(\sigma_2(\mu))$
1	$+1$	$+1$
-1	-1	-1
$\frac{1+\sqrt{5}}{2}$	$+1$	-1
$\frac{1-\sqrt{5}}{2}$	-1	$+1$

Therefore, K is an example of a real quadratic number field with narrow class number 1.

In Chapter 3 we will prove results for real quadratic number fields with narrow class number 1. With this goal in mind, we provide the following list of such fields:

Example 2.2. If we take K to be a real quadratic number field, that is, if $K = \mathbb{Q}(\sqrt{d})$ for $d > 0$ squarefree, then K has narrow class number 1 for the following values of d (up to 100):

$$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \ldots$$

The reader is referred to sequence A003655 in the OEIS. One theme which will arise throughout our work is determining signs of units, and in particular, whether or not certain number fields contain units with norm -1. We see here the first example of why this condition relates to our current investigation, as the number fields given in Example 2.2 are exactly those which have class number 1 and fundamental unit ε_K (as in Example 1.3) with norm -1.

Lemma 2.3. *Let K be a real quadratic number field, denote by id $= \sigma_1, \sigma_2$ the two real embeddings of K. Then K has class number 1 and ε_K has norm -1 if and only if K has narrow class number 1.*

Proof. Suppose $h_K = 1$ and $\varepsilon_K > 1$ has norm -1. That is, $N_{K/\mathbb{Q}}(\varepsilon_K) = \varepsilon_K \sigma_2(\varepsilon_K) = -1$. So, the sign configuration of ε_K is either $(1, -1)$ or $(-1, 1)$ and K has units of all signs, namely 1,-1, ε_K and $\sigma_2(\varepsilon_K)$. So K has narrow class number 1. Conversely, suppose K has narrow class number 1 but that ε_K does not have norm -1. Then no unit of K has norm -1 since ε_K is the fundamental unit of K. So all units of K have norm 1 and therefore no unit can have sign $(1, -1)$ nor $(-1, 1)$. □

Thus, we see that the above list are those number fields with class number 1 and ε_K with norm -1. We note here a connection to Section 1.2, indeed an equivalent condition to this statement is that there exists a solution to the first equation of Lemma 1.4.

Determining whether or not number fields contain units of norm -1 is a well-studied question. We refer the reader to work of Maria Stadnik [20] for a list of real quadratic fields with units of norm -1. Note that by definition of narrow class number 1, each of the finitely many imaginary quadratic extensions with class number 1 also have narrow class number 1. That is, the imaginary quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163,$$

have narrow class number 1.

We can also consider higher degree number fields K which have narrow class number 1. One setting in which examples can be found is the case when L is a cyclotomic extension and K is its

maximal real subfield, as demonstrated in the next example. Number fields L and K as in the first case of the following example will be referenced in the special cases investigated in Section 3.3.2.

Example 2.4. Let $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $h_L = 1$.

1. If m is a prime power (or twice a prime power), then K has narrow class number 1. The complete list of m is

   $m = 1, 2, 4, 8, 16, 32$

   $m = 3, 5, 7, 9, 11, 13, 17, 19, 25, 27$ (or twice the value of m from this list).

2. If m is not a prime power (or twice a prime power) then K has narrow class number 2. The complete list of these m is

   $m = 12, 16, 20, 24, 28, 36, 40, 44, 48, 60, 84$

   $m = 15, 21, 33, 35, 45$ (or twice the value of m from this list).

For more details we refer the reader to [13, Corollary 3.9] and [21, Lemma 3.6].

As mentioned in our preliminary chapter, we will be interested in relative quadratic extensions L/K. We develop the necessary theory about such extensions in the next section.

2.2 Relative Quadratic Extensions

Let K be a totally real number field with narrow class number 1. Fix L to be a relative quadratic extension of K, that is $\text{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$. We denote by τ the nontrivial element of $\text{Gal}(L/K)$ and write $\overline{\alpha} := \tau(\alpha)$ for $\alpha \in L$. We now utilize the fact that K has narrow class number 1. By definition, K also has class number 1, which implies every quadratic extension of K has a relative integral basis [22, Cor pg 388]. This means there exists an $\mathcal{O}_K$-module basis of $\mathcal{O}_L$ and in particular, there exists some $\Omega \in \mathcal{O}_L$ such that $\mathcal{O}_L = [1, \Omega]_{\mathcal{O}_K}$ [6, Prop 1.1], and [23, Prop 2.24]. That is, $\mathcal{O}_L$ is a rank two $\mathcal{O}_K$-module and any fractional ideal of $\mathcal{O}_L$ has a module basis $[\alpha, \beta]_{\mathcal{O}_K}$ for some $\alpha, \beta \in L$.

Let $x^2 + wx + z \in \mathcal{O}_K[x]$ be the minimal polynomial of Ω over $\mathcal{O}_K$. The second root of this polynomial will be $\overline{\Omega}$, and thus if we let $D_\Omega = w^2 - 4z$, then without loss of generality, we may set

$$\Omega = \frac{-w + \sqrt{D_\Omega}}{2}$$

and

$$\overline{\Omega} = \frac{-w - \sqrt{D_\Omega}}{2}.$$

From this we can conclude that $L = K(\sqrt{D_\Omega})$ and make note that $D_\Omega = (\Omega - \overline{\Omega})^2$. With the given set-up, it is tempting to assume that D_Ω is squarefree in K, though this is not necessarily the case. As such, we make the following definition:

Definition 2.5. [9, Definition 2.1] An element d of $\mathcal{O}_K$ is called *fundamental* if d is a quadratic residue modulo 4 in $\mathcal{O}_K$ and

1. either d is square-free
2. or for every $p \in \mathcal{O}_K \backslash \mathcal{U}_K$ such that $p^2 | d$ the following holds: $p|2$ and $\frac{d}{p^2}$ is not a quadratic residue modulo 4 in $\mathcal{O}_K$.

Remark 2.6. Note that although D_Ω may not be squarefree, it is *fundamental* in $\mathcal{O}_K$ see [10, Lemma 2.2]. Further, any fundamental element D of $\mathcal{O}_K$ such that $L = K(\sqrt{D})$ will differ from D_Ω by the square of a unit of $\mathcal{O}_K$ (see [10, Lemma 2.3]).

In what follows unless otherwise stated, we will assume this setting, that is, when K is a totally real number field with narrow class number 1 and L a quadratic extension of K obtained by adjoining the square root of a fundamental element.

2.3 Binary Quadratic Forms Over K

We now give a generalization of our discussion in Section 1.5, and provide details of an equivalence of binary quadratic forms over K with fundamental discriminant, in the sense of Remark 2.6. In what follows, we provide the formulation given by Zemková in [10] with a slight simplification noted in Remark 2.9.

Definition 2.7. [10, Definition 2.9] Let K be a totally real number field with narrow class number 1 and let Q_1 and Q_2 be two binary quadratic forms over K. We say Q_1 and Q_2 are equivalent, denoted $Q_1 \sim Q_2$ if there exist $p, q, r, s \in \mathcal{O}_K$ and a totally positive unit $u \in \mathcal{U}_K^+$ such that $ps - qr \in \mathcal{U}_K^+$ and $Q_2(x, y) = uQ_1(px + qy, rx + sy)$.

Remark 2.8. In [6] we are given another way to view this equivalence of binary quadratic forms over K. Write $Q(x, y) = ax^2 + bxy + cy^2$ as a matrix

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

The condition $Q_1 \sim Q_2$ can be written as

$$\begin{pmatrix} x & y \end{pmatrix} Q_2 \begin{pmatrix} x \\ y \end{pmatrix} = u \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} Q_1 \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{2.1}$$

Taking Q_1, and Q_2, and the elements $p, q, r, s \in \mathcal{O}_K$ and $u \in \mathcal{U}_K^+$ as in Definition 2.7, we write $Q_2(x, y) = uQ_1(px + qy, rx + sy) = a_2x^2 + b_2xy + c_2y^2$, then

$$\begin{pmatrix} a_2 & \frac{b_2}{2} \\ \frac{b_2}{2} & c_2 \end{pmatrix} = u \begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Therefore, given equivalent quadratic forms $Q_1(x, y) = a_1x^2 + b_1xy + c_1y^2$ and

$$Q_2(x, y) = uQ_1(px + qy, rx + sy) = a_2x^2 + b_2xy + c_2y^2,$$

we can express the coefficients of Q_2 explicitly in terms of the coefficients of Q_1:

$$\begin{aligned} a_2 &= u(a_1p^2 + b_1pr + c_1r^2) \\ b_2 &= u(2a_1pq + b_1(ps + qr) + 2crs) \\ c_2 &= u(a_1q^2 + b_1qs + c_1s^2). \end{aligned}$$

From this we obtain $\text{Disc}(Q_2) = u^2(ps - qr)^2(b_1^2 - 4a_1c_1) = u^2(ps - qr)^2\text{Disc}(Q_1)$. Unlike the $\text{SL}_2(\mathbb{Z})$ equivalence of binary quadratic forms over $\mathbb{Q}$, we see that in general, the discriminants of equivalent binary quadratic forms (as in Definition 2.7 and 2.1) differ by the square of a totally positive unit. We may also write the coefficients of Q_1 in terms of those of Q_2 as follows:

$$a_1 = \frac{1}{u(ps - qr)^2}(a_2s^2 - b_2rs + c_2r^2)$$

$$b_1 = \frac{1}{u(ps - qr)^2}(-2a_2qs + b_2(ps + qr) - 2c_2pr)$$

$$c_1 = \frac{1}{u(ps - qr)^2}(a_2q^2 - b_2pq + c_2p^2).$$

Remark 2.9. We note that in the case when K is taken to be totally real and narrow class number 1, as in our desired setting, we can remove the second totally positive unit u as in [10, Definition 2.9] since in this case u is the square of some unit (see [24, Prop. 2.4]).

Definition 2.10. A binary quadratic form Q *represents* an element $\lambda \in \mathcal{O}_K$ if there exist elements $x_0, y_0 \in \mathcal{O}_K$ such that $Q(x_0, y_0) = \lambda$.

With our simplification to the equivalence given by Zemková, we also obtain the following refinement of [10, Lemma 2.10].

Lemma 2.11. *Let K be totally real with narrow class number 1. Then equivalent binary quadratic forms over K represent the same elements.*

Proof. Suppose $Q_1 \sim Q_2$ and Q_2 represents m. Then Q_1 represents some element in the set $\{um \mid u \in \mathcal{U}_K^+\}$ (see [10, Lemma 2.10]). So, there exist some $x_0, y_0 \in \mathcal{O}_K$ such that $Q_1(x_0, y_0) = um$. By our assumptions on K, u is the square of a unit, say $v \in \mathcal{U}_K$. Then $Q_1(v^{-1}x_0, v^{-1}y_0) = m$. $\square$

The following definition is analogous to the one for quadratic forms over $\mathbb{Q}$.

Definition 2.12. A binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is called *primitive* if $gcd(a, b, c) \in \mathcal{U}_K$.

One can use the fact that equivalent forms represent the same elements of $\mathcal{O}_K$ (up to a totally positive unit) to show that if $Q_1 \sim Q_2$ and Q_1 is a primitive quadratic form, then Q_2 is also primitive (see [6, Lemma 1.8]).

At this point it may not be clear how the extensions defined in Section 2.2 relate to the binary quadratic forms we have just defined. We see this relationship by considering quadratic forms of discriminant $D_\Omega = (\Omega - \overline{\Omega})^2$, and equivalent quadratic forms. As we've seen, the discriminants of equivalent quadratic forms may differ by the square of a totally positive unit. As such, we consider the set

$$\mathcal{D} = \{u^2(\Omega - \overline{\Omega})^2 \mid u \in \mathcal{U}_K^+\} \tag{2.2}$$

and quadratic forms with discriminants in $\mathcal{D}$. Then, we consider

Definition 2.13. Let K be a totally real number field with narrow class number 1 and L/K a quadratic extension with discriminant $D \in \mathcal{D}$. Define

$$\mathcal{Q}_\mathcal{D} = \{Q(x, y) = ax^2 + bxy + cy^2 \mid a, b, c \in \mathcal{O}_K, \gcd(a, b, c) \in \mathcal{U}_K, \text{Disc}(Q) \in \mathcal{D}\}/\sim$$

to be the set of equivalence classes of primitive binary quadratic forms over K with discriminant in $\mathcal{D}$, with $\sim$ as defined above.

We note that although it may be tempting to simplify the equivalence of quadratic forms to one which considers forms of discriminant exactly D, the above definition is needed to obtain the bijection of Section 2.5 (see [10, Remark 2.12]).

2.4 Relative Oriented Class Groups

In order to build up to the definition of the relative oriented class group of a relative quadratic extension L/K, we discuss some results of [10] regarding ideals of the ring of integers of L. Suppose K is a totally real number field with narrow class number 1. Recall that this assumption on K implies that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module. Therefore, in this section, an ideal of $\mathcal{O}_L$ will be some fractional ideal I with $\alpha, \beta \in L$ such that $I = [\alpha, \beta]_{\mathcal{O}_K}$. If $\alpha, \beta \in \mathcal{O}_L$ then I is an integral ideal. Every other basis of I as an $\mathcal{O}_K$ module will be of the form $[p\alpha + r\beta, q\alpha + s\beta]_{\mathcal{O}_K}$ with $p, q, r, s \in \mathcal{O}_K$ with $ps - qr \in \mathcal{U}_K$ (see [6, Proposition 1.10]). In the following, we state results about non-zero ideals. One can attach an "orientation" to such an ideal in the following way.

For a fractional ideal $I = [\alpha, \beta]_{\mathcal{O}_K}$ of $\mathcal{O}_L$, let M be the 2×2 matrix with entries in K so that

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = M \begin{pmatrix} 1 \\ \Omega \end{pmatrix}.$$

Then we have

$$\begin{pmatrix} \overline{\alpha} & \alpha \\ \overline{\beta} & \beta \end{pmatrix} = M \begin{pmatrix} 1 & 1 \\ \overline{\Omega} & \Omega \end{pmatrix}.$$

From this one can easily determine $\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}}$ which generates the (necessarily principal) ideal $N_{L/K}(I) = (N_{L/K}(\alpha) \mid \alpha \in I)$ by [25, Theorem 1]. Note that if $[p\alpha + r\beta, q\alpha + s\beta]_{\mathcal{O}_K}$ were another basis for I and M' the corresponding matrix, then $\det M' = \det M(ps - qr)$. For more details, the reader is referred to [10, Section 2].

Recall our goal of building up to generalizations of Theorem 1.20 given in [1] and [10]. In this section, we consider relative oriented class groups as defined in [10], where Zemková defines

a bijection with $\mathcal{Q}_{\mathcal{D}}$ on one side, and a relative oriented class group on the other. Fix K to be a totally real number field with class number 1 and real embeddings $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$. Let L/K be a relative quadratic extension of K. We begin with the definition of an oriented ideal.

Definition 2.14. [10, Definition 2.16] For $a \in K^\times$ write $\underline{\text{sgn}}(a) = (\text{sgn}(\sigma_1(a)), \ldots, \text{sgn}(\sigma_r(a)))$ and set

$\mathcal{I}^o_{L/K} = \{(I; \epsilon_1, \ldots, \epsilon_r) \mid I \text{ a nonzero fractional } \mathcal{O}_L\text{-ideal}, \epsilon_i \in \{\pm 1\}, i = 1, \ldots, r\}$

$\mathcal{P}^o_{L/K} = \{((\gamma); \underline{\text{sgn}}(N_{L/K}(\gamma))) \mid \gamma \in L^\times\}$;

where $(I; \epsilon_1, \ldots, \epsilon_r)$ is the *oriented ideal*.

Recall multiplication of fractional ideals defined in Section 1.4. From this, one can define multiplication of oriented ideals in $\mathcal{I}^o_{L/K}$ component-wise via

$$(I; \epsilon_1, \ldots, \epsilon_r) \cdot (J; \delta_1, \ldots, \delta_r) = (IJ; \epsilon_1\delta_1, \ldots, \epsilon_r\delta_r).$$

With this operation, $\mathcal{I}^o_{L/K}$ is an abelian group with subgroup $\mathcal{P}^o_{L/K}$. Therefore, the following quotient group is well defined:

Definition 2.15. Let K be a totally real number field with r real embeddings and L/K a relative quadratic extension. The group, $Cl^o_{L/K}$, is called the *relative oriented class group* of L/K and is defined by

$$Cl^o_{L/K} := \mathcal{I}^o_{L/K}/\mathcal{P}^o_{L/K}.$$

The following relationship, shown by Zemková in [10, Proposition 2.19], between the class group of L and the new oriented class group of the extension L/K, will be crucial to our computations in Chapter 3.

Let

$$H = \{\underline{\text{sgn}}(N_{L/K}(u)) \mid u \in \mathcal{U}_L\}.$$

Then

$$Cl_L \cong Cl^o_{L/K} \Big/ \{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H \tag{2.3}$$

where $\{\mathcal{O}_L\}$ is understood to be the trivial group and $\langle \pm 1 \rangle^r$ is r copies of the group of order 2, and thought of as the group of all possible orientations. Take special note of the subgroup H above, as we will investigate this subgroup further in the next chapter.

We define classes of $Cl^o_{L/K}$ in the following way:

Lemma 2.16. *[10, Lemma 2.18] Two oriented ideals $(I; \epsilon_1, \ldots, \epsilon_r)$ and $(J; \delta_1, \ldots, \delta_r)$ are equivalent if and only if there exists some $\gamma \in L$ such that $\gamma I = J$ and $\underline{sgn}(\gamma\overline{\gamma}) = (\epsilon_1\delta_1, \ldots, \epsilon_r\delta_r)$. Moreover, if $I = J$ then γ must be a unit.*

At this point, the most natural question is: given an ideal I, how do we use its basis to define an orientation? Recall that any $\mathcal{O}_L$ ideal I has a basis, that is, some $\alpha, \beta \in L$ such that $I = [\alpha, \beta]_{\mathcal{O}_K}$ and an associated 2×2 matrix M. We determine the orientation for I by considering the signs of the images of the determinant of M under each of the real embeddings of K:

$$([\alpha, \beta]_{\mathcal{O}_K}; \underline{\text{sgn}}(\det M)) = ([\alpha, \beta]_{\mathcal{O}_K}; \text{sgn}(\sigma_1(\det M), \ldots, \text{sgn}(\sigma_r(\det(M))))).$$

Conversely, one may wonder if given an oriented ideal, we can determine a basis which corresponds with the given orientation. The following result addresses this question, and its proof relies on our assumption that K has narrow class number 1.

Lemma 2.17. *[10, Lemma 2.15] Let $(I; \epsilon_1, \ldots, \epsilon_r)$ be an oriented ideal. Then there exists a basis $[\alpha, \beta]_{\mathcal{O}_K}$ of I such that $\underline{sgn}(\det M) = (\epsilon_1, \ldots, \epsilon_r)$, where $\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}}$.*

With all of this in mind, we can make more precise the group structure of a given relative oriented class group $Cl^o_{L/K}$. The identity element of $Cl^o_{L/K}$ is $([1, \Omega]_{\mathcal{O}_K}; (1, \ldots, 1))$ and the inverse of $([\alpha, \beta]_{\mathcal{O}_K}; \underline{\text{sgn}}(\det M))$ is $([\overline{\alpha}, -\overline{\beta}]_{\mathcal{O}_K}; \underline{\text{sgn}}(\det M))$ by [10, Lemma 2.17], taken as representatives of classes of the corresponding elements of $Cl^o_{L/K}$. We also make note that the existence of a

basis of the product of ideals is another fact dependent on our narrow class number 1 assumption (see [10, pg. 9]).

2.5 The Correspondence

We now present the correspondence between classes of quadratic forms and classes of oriented ideals as given by [9, Theorem 2.3]. After giving the result we note the group structure of $\mathcal{Q}_{\mathcal{D}}$ which arises from this bijection.

Theorem 2.18. *[9, Theorem 2.3] Let K be a totally real number field with narrow class number 1. Let D be a fundamental element of $\mathcal{O}_K$. Set $L = K(\sqrt{D})$ and $\mathcal{D} = \{u^2 D \mid u \in \mathcal{U}_K^+\}$. Then there is a bijection between $\mathcal{Q}_{\mathcal{D}}$ and $Cl^o_{L/K}$ given by*

$$Q(x,y) = ax^2 + bxy + cy^2 \xrightarrow{\Psi} \left(\left[a, \frac{-b + \sqrt{Disc(Q)}}{2} \right]_{\mathcal{O}_K} ; \underline{sgn}(a) \right)$$

and

$$\left([\alpha, \beta]_{\mathcal{O}_K} ; \underline{sgn} \left(\frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}} \right) \right) \xrightarrow{\Phi} \frac{N_{L/K}(\alpha x - \beta y)}{\frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}}}.$$

where $\sqrt{Disc(Q)}$ and $\sqrt{D}$ are chosen such that $\sqrt{Disc(Q)}/\sqrt{D} \in \mathcal{U}_K^+$.

Note that the maps above are understood to be between classes. Note also that $N_{L/K}(\alpha x - \beta y) = (\alpha x - \beta y)(\overline{\alpha} x - \overline{\beta} y) = \alpha\overline{\alpha}x^2 - (\overline{\alpha}\beta + \alpha\overline{\beta})xy + \beta\overline{\beta}y^2$. The ideal $[a, (-b + \sqrt{\text{Disc}(Q)})/2]_{\mathcal{O}_K}$ is an $\mathcal{O}_L$ ideal (see [10, Proposition 3.5]). The beauty of such a bijection is that the group structure of $\mathcal{Q}_{\mathcal{D}}$ is determined by multiplication of ideals of L (see [9, pg. 5]). This is made precise in the following result.

Lemma 2.19. *[10, Corollary 3.8] Let K be a totally real number field with narrow class number 1. Let L/K be a relative quadratic extension. Suppose $\mathcal{O}_L = [1, \Omega]_{\mathcal{O}_K}$. Then, the trivial class of $Cl^o_{L/K}$ has $\Phi(([1,\Omega]; (1, \ldots, 1))) = x^2 - (\Omega + \overline{\Omega})xy + \Omega\overline{\Omega}y^2$. The inverse of the form $ax^2 + bxy + cy^2$ is $ax^2 - bxy + cy^2$.*

We note that more computations related to representatives of each class of $\mathcal{Q}_{\mathcal{D}}$ arising from this correspondence are discussed in Section 3.4.

We have now defined all of the necessary objects of our investigation. In what follows we consider our main objective, which is to explicitly compute the right hand side of this bijection. That is, given a totally real number field K of narrow class number 1 and L/K a relative quadratic extension, we wish to compute the corresponding $Cl^o_{L/K}$. One of our strategies for doing so will follow from Equation 2.3.

Chapter 3

Computing Relative Oriented Class Groups

Take the assumptions of the previous chapter: K is a totally real number field with r real embeddings and narrow class number 1 and L/K a relative quadratic extension. We describe a strategy for determining candidates for the relative oriented class groups $Cl^o_{L/K}$ as K varies based on Equation 2.3. Our approach will lay a framework for expressing the relative oriented class group of the relative quadratic extension L/K in terms of the ideal class group of L when a system of fundamental units is known and the associated group extension is split (see Section 3.2). To express the effectiveness of our strategy in special cases, we consider the case when K is a real quadratic number field and L/K a relative quadratic extension and the case of CM fields. In this way we extend the results of [10, Proposition 3.9] under certain conditions on the class number of L. Throughout, we consider specific examples to demonstrate our findings.

We begin with a result of Zemková which classifies the relative oriented class groups for quadratic extensions of $\mathbb{Q}$. This result serves as motivation for our work throughout the section.

Proposition 3.1. *[10, Proposition 3.9] Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{D_\Omega})$ for D_Ω a fundamental element of $\mathbb{Z}$.*

- *If $D_\Omega < 0$, then $Cl^o_{L/\mathbb{Q}} \cong Cl_L \times \langle \pm 1 \rangle$.*
- *If $D_\Omega > 0$ and $u\overline{u} = 1$ for every $u \in \mathcal{U}_L$ then $Cl^o_{L/\mathbb{Q}} \cong Cl_L \times \langle \pm 1 \rangle \cong Cl^+_L$.*
- *If $D_\Omega > 0$ and there exists $u \in \mathcal{U}_L$ such that $u\overline{u} = -1$, then $Cl^o_{L/\mathbb{Q}} \cong Cl_L \cong Cl^+_L$.*

The key observation which fuels our work is that one could rephrase the result above in terms of the subgroup $H \subseteq \langle \pm 1 \rangle^r$ as defined in (2.3). Indeed, the first two cases are equivalent to H being trivial. The third condition is equivalent to H being $\langle \pm 1 \rangle$. That is, if one would like to express $Cl^o_{L/K}$ explicitly in terms of Cl_L, one need only determine the corresponding subgroup H. However, outside of this case when $K = \mathbb{Q}$, we must be careful in our computations as H will not

always automatically lead to a full description of $Cl^o_{L/K}$. We will discuss such obstacles in Section 3.2. For now, we focus on computing the subgroup H in general, as it is a necessary ingredient in computing the relative oriented class group, and gives way to candidates for groups isomorphic to the relative oriented class groups.

3.1 Candidate Oriented Class Groups

In this section we develop the observation above into a strategy for determining possible subgroups $H = \{\underline{\text{sgn}}(N_{L/K}(u)) \mid u \in \mathcal{U}_L\} \subseteq \langle \pm 1 \rangle^r$. In particular, when K is taken to be totally real with narrow class number 1 and L/K a quadratic extension, if a fundamental system of units for $\mathcal{U}_L$ is known, this strategy can be used to determine the relative oriented class group, $Cl^o_{L/K}$, explicitly in terms of the ideal class group of L when the corresponding group extension problem splits. We begin with a description of the general case. To gain intuition and motivation for our assumptions, we refer the reader to the special cases outlined in Section 3.3. Our main result concerns the following group action.

Let $K/\mathbb{Q}$ be Galois, L/K a relative quadratic extension with $L/\mathbb{Q}$ Galois. Take K to have r real embeddings $K \hookrightarrow \mathbb{R}$ and label them $\sigma_1 = \text{id}, \sigma_2, \ldots, \sigma_r$. Then, $\text{Gal}(K/\mathbb{Q})$ acts transitively on the set of all σ_i by precomposition. This induces an action of $\text{Gal}(K/\mathbb{Q})$ on $(\mathbb{Z}/2\mathbb{Z})^r \cong \langle \pm 1 \rangle^r$ defined in the following way.

Definition 3.2. Let $(\varepsilon_1, \ldots, \varepsilon_r) \in \langle \pm 1 \rangle^r$. Since K has narrow class number 1, there exists some $a \in \mathcal{U}_K$ such that $(\varepsilon_1, \ldots, \varepsilon_r) = \underline{\text{sgn}}(a)$. Then $\text{Gal}(K/\mathbb{Q})$ acts on $\langle \pm 1 \rangle^r$ by

$$g \cdot \underline{\text{sgn}}(a) = \underline{\text{sgn}}(g(a)) \ \ \forall g \in \text{Gal}(K/\mathbb{Q}). \tag{3.1}$$

We verify this action is well-defined.

Lemma 3.3. *The action of Gal$(K/\mathbb{Q})$ on $\langle \pm 1 \rangle^r$ defined above is well-defined.*

Proof. It is immediate that the identity of Gal$(K/\mathbb{Q})$ acts trivially. For $g_1, g_2 \in$ Gal$(K/\mathbb{Q})$ we have

$$\begin{aligned} g_1 \cdot (g_2 \cdot \underline{\text{sgn}}(a)) &= g_1 \cdot \underline{\text{sgn}}(g_2(a)) \\ &= \underline{\text{sgn}}(g_1 g_2(a)) \\ &= (g_1 g_2) \cdot \underline{\text{sgn}}(a). \end{aligned}$$

Lastly, suppose $a, b \in K^\times$ are such that $\underline{\text{sgn}}(a) = \underline{\text{sgn}}(b)$. We have $\text{sgn}(\sigma_i(a)) = \text{sgn}(\sigma_i(b))$ for all $i = 1 \dots r$. Then, for each $i \in 1 \dots r$, there exists a unique $j \in 1, \dots, r$ such that $\sigma_j g = \sigma_i$. Therefore we have that $\text{sgn}(\sigma_j g(a)) = \text{sgn}(\sigma_j g(b))$ for all $j \in 1 \dots r$. By definition of $\underline{\text{sgn}}$ we have that $\underline{\text{sgn}}(g(a)) = \underline{\text{sgn}}(g(b))$. □

We now restrict the above action to a particular subgroup of Gal$(K/\mathbb{Q})$. Given any tower of number fields $L/K/\mathbb{Q}$ with $L/\mathbb{Q}$ and $K/\mathbb{Q}$ Galois, we obtain a short exact sequence

$$1 \to \text{Gal}(L/K) \to \text{Gal}(L/\mathbb{Q}) \to \text{Gal}(K/\mathbb{Q}) \to 1. \tag{3.2}$$

Denote the centralizer of Gal(L/K) in Gal$(L/\mathbb{Q})$ by C. That is,

$$C = \{g \in \text{Gal}(L/\mathbb{Q}) \mid gs = sg \ \forall s \in \text{Gal}(L/K)\}.$$

In our case of interest, when L/K is taken to be a relative quadratic extension, the third map in (3.2) is two-to-one. Denote by $\overline{C}$ the image of C under this map. With this in mind, we can define a group action of $\overline{C}$ on $\langle \pm 1 \rangle^r$ by restricting the group action defined in (3.1) to the subgroup $\overline{C} \subset \text{Gal}(K/\mathbb{Q})$.

We now determine how to understand the subgroups H in terms of their corresponding group actions. We first give the result, then work toward its proof by highlighting key features of norms of units. We then provide an explicit example to demonstrate our findings.

Theorem 3.4. *Let K be a totally real number field with narrow class number 1 and r real embeddings. Suppose $K/\mathbb{Q}$ is Galois. Let L/K be a relative quadratic extension with $L/\mathbb{Q}$ Galois. Define C and $\overline{C}$ as above. Then under the restriction to $\overline{C}$ of the action defined in (3.1), if $\alpha \in H$ then $Orb_{\overline{C}}(\alpha) \subset H$.*

The following is a useful lemma. Indeed, the contents of this result will allow us to show that each element of an orbit, as described above, is realized by some unit of L.

Lemma 3.5. *Let K be a totally real number field which is Galois and L/K a quadratic extension such that $L/\mathbb{Q}$ is Galois. Let $u \in \mathcal{U}_L$ and $g \in \overline{C}$. There exists some $v \in \mathcal{U}_L$ such that $N_{L/K}(v) = g(N_{L/K}(u))$.*

Proof. Let $u \in \mathcal{U}_L$ and call $N_1 = N_{L/K}(u)$ and $N_2 = g(N_1)$. Let $\tau \in \text{Gal}(L/K)$ be the generating element and denote by $\tilde{g}$ a lift of g to $\text{Gal}(L/\mathbb{Q})$ with $\tilde{g} \in C$. We wish to find some element $v \in \mathcal{U}_L$ such that $N_{L/K}(v) = g(N_1)$. Take $v = \tilde{g}(u)$. Then,

$$\begin{aligned} N_{L/K}(v) &= v\tau(v) \\ &= \tilde{g}(u)\tau(\tilde{g}(u)) \\ &= \tilde{g}(u)\tilde{g}(\tau(u)) \\ &= \tilde{g}(u\tau(u)) \\ &= \tilde{g}(N_1)) \\ &= g(N_1) \\ &= N_2. \end{aligned}$$

We use the hypothesis that $\tilde{g} \in C$ in the third equality. □

We are now ready to prove Theorem 3.4

Proof of Theorem 3.4. Let $\alpha \in H$, then there exists some $u \in \mathcal{U}_L$ such that $\alpha = \underline{\text{sgn}}(N_{L/K}(u))$. Let $g \in \overline{C} \subset \text{Gal}(K/\mathbb{Q})$, then $g \cdot \alpha = \underline{\text{sgn}}(g(N_{L/K}(u)))$. By Lemma 3.5, there exists some $v \in \mathcal{U}_L$

such that $g(N_{L/K}(u)) = N_{L/K}(v)$. So,

$$g \cdot \alpha = \underline{\text{sgn}}(N_{L/K}(v)) \in H.$$

□

The proof of the above lemma motivates the restriction of the group action defined at the start of the section. If $L/K/\mathbb{Q}$ is a *central* extension, that is when

$$\text{Gal}(L/K) \subset Z(\text{Gal}(L/\mathbb{Q})),$$

then C is all of $\text{Gal}(L/\mathbb{Q})$ and thus $\overline{C}$ is all of $\text{Gal}(K/\mathbb{Q})$. As such, we note an immediate corollary:

Corollary 3.6. *Let K be a totally real number field with narrow class number 1 and r real embeddings. Suppose $K/\mathbb{Q}$ is Galois. Let L/K be a relative quadratic extension with $L/\mathbb{Q}$ Galois such that $L/K/\mathbb{Q}$ is central. Then under the action defined in (3.1), if $\alpha \in H$ then $Orb_{Gal(K/\mathbb{Q})}(\alpha) \subset H$.*

We note that with the assumptions of the above corollary, Theorem 3.4 immediately implies the following.

Corollary 3.7. *The subgroup H as defined in equation 2.3 is a subgroup of $\langle \pm 1 \rangle^r \cong (\mathbb{Z}/2\mathbb{Z})^r$, and also the union of orbits of the group action $Gal(K/\mathbb{Q}) \circlearrowright \langle \pm 1 \rangle^r$.*

Proof. This follows immediately from Theorem 3.4 and the definition of H. □

It is important to note that this action is not transitive, and this fact is what makes Theorem 3.4 useful in deducing formulas for relative oriented class groups. We demonstrate the effectiveness of this observation in what follows.

3.1.1 Computing Orbits

In this subsection we pause to understand the significance of our work above. In particular, we provide examples in the case when $r = 3$ and $r = 4$ where our understanding of H as both

a subgroup of $\langle \pm 1 \rangle^r$, but also the union of orbits, significantly minimizes the options for the size of the associated relative oriented class groups. We note that the case $r = 2$ is handled in Section 3.3 within the context of the proof of Theorem 3.24. In cases considered below where computing H immediately yields a complete description of the associated relative oriented class group, we present its structure. We will investigate cases where more work is necessary in the next section.

We begin with an example when $r = 4$ and $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ which will be referenced throughout this section. After thoroughly investigating the particular case, we provide summaries of analogous computations for the other case when $r = 4$ and in the case when $r = 3$.

Example 3.8. Suppose $r = 4$ and $G = (\mathbb{Z}/2\mathbb{Z})^2$. We note that there are 67 subgroups of $\langle \pm 1 \rangle^4$. However, by considering the orbits of elements of $\langle \pm 1 \rangle^4$ under the action of G, we reduce the number of possible subgroups H to just 7.

There are two elements of $\langle \pm 1 \rangle^4$ fixed by the action of G, namely $(1, 1, 1, 1)$ and $(-1, -1, -1, -1)$. There are three orbits of size 2:

$$\{(-1, -1, 1, 1), (1, 1, -1, -1)\}$$

$$\{(-1, 1, -1, 1), (1, -1, 1, -1)\}$$

$$\{(-1, 1, 1, -1), (1, -1, -1, 1)\}.$$

Lastly, the two orbits of size 4 contain the elements of $\langle \pm 1 \rangle^4$ with an odd number of -1 entries:

$$\{(-1, 1, 1, 1), (1, -1, 1, 1), (1, 1, -1, 1), (1, 1, 1, -1)\}$$

and

$$\{(1, -1, -1, -1), (-1, 1, -1, -1), (-1, -1, 1, -1), (-1, -1, -1, 1)\}.$$

Then, by Theorem 3.4 we see the only possibilities for the subgroup H are the trivial subgroup, all of $\langle \pm 1 \rangle^4$, the subgroup $\langle (-1,-1,-1,-1) \rangle$, the three subgroups of order 4 of the form

$$\alpha \cup \{(1,1,1,1),(-1,-1,-1,-1)\},$$

with $\alpha \in H$ such that $|\text{Orb}(\alpha)| = 2$, and one subgroup of order 8 given by

$$\{\alpha \in H \mid |Orb(\alpha)| = 2\} \cup \{(1,1,1,1),(-1,-1,-1,-1)\}.$$

For clarity in future examples, we will denote by H_0 the trivial subgroup, H_1 the subgroup $\langle (-1,-1,-1,-1) \rangle$, by H_2 the subgroup of order 4 arising from taking $\alpha = (-1,-1,1,1)$, H_3 when $\alpha = (-1,1,-1,1)$ and H_4 when $\alpha = (-1,1,1,-1)$, and lastly the subgroup of order 8 by H_5.

We note that by the previous example, if K is a totally real biquadratic extension and L contains an element with absolute norm -1, then the relative oriented class group, $Cl^o_{L/K}$ is as small as possible.

Lemma 3.9. *Let K be a totally real biquadratic field and L/K a relative quadratic extension of K. Suppose there exists some $u \in \mathcal{U}_L$ such that $N_{L/\mathbb{Q}}(u) = -1$. Then $Cl^o_{L/K} \cong Cl_L$.*

Proof. If some element of $\mathcal{U}_L$ has absolute norm -1, then its sign configuration is an element of one of the orbits of size 4 and by the multiplicativity of sgn, H contains all elements of $\langle \pm 1 \rangle^4$. □

We end with an example of when this case arises. Note that this example also highlights the usefulness of our work describing H in terms of orbits. Indeed, by utilizing a computer algebra system to determine the system of fundamental units of L, we determine the relative oriented class group.

Example 3.10. Take L to be the number field

$$L = \mathbb{Q}[x]/\langle x^8 - 12x^6 + 30x^4 - 24x^2 + 4 \rangle$$

and K the quadratic subfield $\mathbb{Q}(\sqrt{2},\sqrt{5})$. Then we are in the case of Example 3.8 with $r = 4$ and $G = (\mathbb{Z}/2\mathbb{Z})^2$. Note that the rank of $\mathcal{U}_L$ is 7. We utilized SageMath Version 9.0 to compute the sign configuration of each element of the system of fundamental units of L, which we denote by u_i for $i = 1, \ldots, 7$. The following signs are realized by these elements:

$$\underline{\text{sgn}}(u_1) = (1,1,1,1) \qquad \underline{\text{sgn}}(u_4) = (-1,1,-1,1)$$

$$\underline{\text{sgn}}(u_2) = (1,1,1,1) \qquad \underline{\text{sgn}}(u_5) = (1,1,1,1)$$

$$\underline{\text{sgn}}(u_3) = (1,-1,1,-1) \qquad \underline{\text{sgn}}(u_6) = (-1,-1,1,-1)$$

$$\underline{\text{sgn}}(u_7) = (-1,1,-1,-1).$$

As such, we see that H contains the union of one orbit of size one, the second orbit of size 2 and the second orbit of size 4. Since H is a subgroup of $\langle \pm 1 \rangle^4$ by construction, this implies $H = \langle \pm 1 \rangle^4$. Therefore, since $h_L = 1$, we have $Cl^o_{L/K} \cong Cl_L \cong \{1\}$.

After computing the previous example, we were curious if all 7 possible subgroups H as in Example 3.8 arose as the subgroup corresponding to some extension L with quadratic subfield K a totally real biquadratic field and with narrow class number 1. In the following example we show that this is indeed the case.

Example 3.11. Indeed, every possible subgroup H as in Example 3.8 can realized by a relative quadratic extension L/K as in the previous example, that is, where L is Galois extension and K a totally real quadratic subfield of L which is itself biquadratic and has narrow class number 1. In fact, we take $K = \mathbb{Q}(\sqrt{2},\sqrt{5})$ in every example below. These examples were computed with SageMath Version 9.0 [16] with data collected from the LMFDB. We note that in the cases where $h_L = 1$, we can explicitly compute the relative oriented class group.

$H = H_0$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 2x^7 - 85x^6 + 168x^5 + 2179x^4 - 3628x^3 - 19445x^2 + 24022x + 40111 \rangle$$

has class number 1 and relative oriented class group $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^4 \cong \langle \pm 1 \rangle^4$.

$H = H_1$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 108x^6 + 4019x^4 - 58512x^2 + 249001 \rangle$$

has $Cl_L \cong (\mathbb{Z}/2\mathbb{Z})^2$. Thus, we can conclude that the relative oriented class group has order 32.

Remark 3.12. Given the conditions on the class number of L, more work needs to be done to determine the structure of the relative oriented class group in this case. We discuss this in more detail in the next section.

$H = H_2$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 2x^7 - 25x^6 + 48x^5 + 139x^4 - 208x^3 - 125x^2 + 262x - 89 \rangle$$

has class number 1 and relative oriented class group $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^2 \cong \langle \pm 1 \rangle^2$.

$H = H_3$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 2x^7 - 35x^6 + 68x^5 + 304x^4 - 478x^3 - 620x^2 + 1072x - 239 \rangle$$

has class number 1 and relative oriented class group $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^2 \cong \langle \pm 1 \rangle^2$.

$H = H_4$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 2x^7 - 15x^6 + 28x^5 + 44x^4 - 58x^3 - 20x^2 + 12x + 1 \rangle$$

has class number 1 and relative oriented class group $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^2 \cong \langle \pm 1 \rangle^2$.

Remark 3.13. We note that for the three subgroups of order 4 as in the previous three cases, distinguishing between each depends only on the ordering of the embeddings.

$H = H_5$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 8x^6 + 19x^4 - 12x^2 + 1\rangle$$

has class number 1 and relative oriented class group $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1\rangle \cong \langle \pm 1\rangle$.

$H = \langle \pm 1\rangle^4$: (see Example 3.10) The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 12x^6 + 30x^4 - 24x^2 + 4\rangle$$

has class number 1 and relative oriented class group $Cl^o_{L/K} \cong Cl_L \cong \{1\}$.

Below is a summary of analogous examples for the case that $r = 4$ and $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})$ and in the case that $r = 3$.

Example 3.14. Take $r = 4$ and $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Then there are five possible subgroups which H can be.

Namely, the trivial subgroup which we denote below by H_0, the subgroup of order two generated by $(-1,-1,-1,-1)$ denoted below by H_1, the subgroup of order four, denoted H_2, containing the orbit of $(-1,1,-1,1)$ with $(-1,-1,-1,-1)$ and $(1,1,1,1)$, the subgroup of order 8, H_3, which contains all signs with two negative entries, along with the elements $(-1,-1,-1,-1)$ and $(1,1,1,1)$ and lastly, the whole group $\langle \pm 1\rangle^4$.

Again, we see that each possible subgroup above is realized by some quadratic extension L/K such that $L/\mathbb{Q}$ and $K/\mathbb{Q}$ are Galois and K is totally real and narrow class number 1 with Galois group $\mathbb{Z}/4\mathbb{Z}$.

$H = H_0$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 64x^6 + 1280x^4 - 8192x^2 + 9409\rangle$$

has quadratic subfield $K = \mathbb{Q}[x]/\langle x^4 - 4x^2 + 2\rangle$ and class number 1. Therefore, the relative oriented class group is $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1\rangle^4 \cong \langle \pm 1\rangle^4$.

$H = H_1$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 4x^7 - 18x^6 + 68x^5 + 73x^4 - 264x^3 + 8x^2 + 136x - 34\rangle$$

has quadratic subfield $K = \mathbb{Q}[x]/\langle x^4 - 4x^2 + 2\rangle$ and class number 1. So, we compute $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1\rangle^3 \cong \langle \pm 1\rangle^3$.

$H = H_2$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 2x^7 - 23x^6 + 32x^5 + 117x^4 - 128x^3 - 164x^2 + 128x + 52\rangle$$

has quadratic subfield $K = \mathbb{Q}[x]/\langle x^4 - x^3 - 6x^2 + x + 1\rangle$ and class number 1. Thus, $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1\rangle^2 \cong \langle \pm 1\rangle^2$.

$H = H_3$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 8x^6 + 20x^4 - 16x^2 + 1\rangle$$

has quadratic subfield $K = \mathbb{Q}[x]/\langle x^4 - 4x^2 + 2\rangle$ and class number 1.
So, $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1\rangle \simeq \langle \pm 1\rangle$.

$H = \langle \pm 1\rangle^4$: The number field

$$L = \mathbb{Q}[x]/\langle x^8 - 8x^6 + 20x^4 - 16x^2 + 2\rangle$$

has quadratic subfield $K = \mathbb{Q}[x]/\langle x^4 - 4x^2 + 2\rangle$ and class number 1. So,
$Cl^o_{L/K} \cong Cl_L \cong \{1\}$.

Example 3.15. Let $r = 3$ and $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$. There are four possible subgroups for H.

That is, H_0 which denotes the trivial subgroup, the subgroup H_1 generated by $(-1,-1,-1)$, the subgroup H_2 of order 4 which contains the three sign configurations with two negatives, and the whole group $\langle \pm 1 \rangle^3$. Once again, we can find examples in each case, where L is a quadratic extension over $K = \mathbb{Q}[x]/\langle x^3 - x^2 - 2x + 1 \rangle \cong \mathbb{Q}(\zeta_7)^+$. We note that in all cases $L/\mathbb{Q}$ and $K/\mathbb{Q}$ are Galois. The number field K is totally real and has narrow class number 1 as indicated in Example 2.4. Since each example arises for some L with class number 1, we compute the associated relative oriented class group for each example.

$H = H_0$ The number field

$$L = \mathbb{Q}[x]/\langle x^6 - x^5 - 76x^4 + 76x^3 + 1618x^2 - 1618x - 7699 \rangle$$

has class number 1, so the relative oriented class group is $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^3 \cong \langle \pm 1 \rangle^3$.

$H = H_1$ The number field

$$L = \mathbb{Q}[x]/\langle x^6 - x^5 - 14x^4 + 9x^3 + 35x^2 - 16x - 1 \rangle$$

has class number 1, so the relative oriented class group is $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^2 \cong \langle \pm 1 \rangle^2$.

$H = H_2$ The number field

$$L = \mathbb{Q}[x]/\langle x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1 \rangle$$

has class number 1, so the relative oriented class group is $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle \cong \langle \pm 1 \rangle$.

$H = H_3$ The number field

$$L = \mathbb{Q}[x]/\langle x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1 \rangle$$

has class number 1, so the relative oriented class group is $Cl^o_{L/K} \cong Cl_L \cong \{1\}$.

We end this section by again emphasizing the fact that we were only able to expressly use H to determine the relative oriented class group in some of the above examples because L had class number 1. That is, given the isomorphism as in [10, Proposition 2.19]

$$Cl_L \cong Cl^o_{L/K}/\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H,$$

we actually obtain $Cl^o_{L/K} \cong \{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H$ in all but the second case of Example 3.11. We note that in the last case of each example, when H is all of $\langle \pm 1 \rangle^r$, an explicit description of the relative oriented class group would also have been possible regardless of h_L. With these examples in mind, we move to the next section where we investigate the structure of the relative oriented class group via the group extension problem.

3.2 Structure of the Relative Oriented Class Group

We take K and L with all of our usual assumptions, K is a totally real number field and L/K a quadratic extension. The proof of [10, Proposition 2.19], gives the short exact sequence

$$1 \to \{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H \to Cl^o_{L/K} \to Cl_L \to 1 \tag{3.3}$$

which yields the isomorphism

$$Cl_L \cong Cl^o_{L/K}/(1 \times \langle \pm 1 \rangle^r / H). \tag{3.4}$$

Note that in the special cases when H is the entire group $\langle \pm 1 \rangle^r$ or when $h_L = 1$, we immediately have

$$Cl^o_{L/K} \cong Cl_L \times \{\pm 1\}^r / H. \tag{3.5}$$

We therefore see, that in these two cases, one can completely determine the relative oriented class group, $Cl^o_{L/K}$, in terms of the class group of L once H is determined. Further, in any situation, once H is computed, we can say that $Cl^o_{L/K}$ is an extension of Cl_L by $\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H$ and for example, can determine the order of $Cl^o_{L/K}$. However, in general, one must consider the question of whether or not Equation 3.5 holds to explicitly compute $Cl^o_{L/K}$. That is, to classify $Cl^o_{L/K}$ in general, we must consider the extension problem corresponding to the short exact sequence (3.3). As such, we pause from our usual setting to recall some facts about group extensions.

Definition 3.16. Let A and B be groups, then G is an extension of B by A if there is a short exact sequence

$$1 \to A \xrightarrow{\iota} G \xrightarrow{\pi} B \to 1. \tag{3.6}$$

In this case, the group A is normal in G and $B \cong G/A$. We call the extension *central* if A is contained in the center of G. The *extension problem* arises when one knows A and B and wishes to determine the structure of G.

Addressing a particular extension problem requires classifying all possible extensions G of B by A. In the case when all groups in question are taken to be abelian, the set of all isomorphism classes of extensions of B by A form a group $\mathrm{Ext}^1_{\mathbb{Z}}(B, A)$ which we will discuss below in the context of our investigation.

An important type of group extension is one that is *split*. We say a group extension as in (3.6) is split if there exists a *splitting*, that is a homomorphism $s : B \to G$ which is a right inverse of π, i.e. $\pi \circ s = \mathrm{id}_B$. Split extensions are exactly those in which G is a semidirect product of B and A. In particular, if all of the groups in questions are abelian, a group extension (3.6) splits if and only if $G \cong A \times B$. This gives rise the notion of a *trivial extension*. Such extensions are of course of interest to us in order to completely classify the relative oriented class groups of quadratic extensions. For more information on group extensions and the extension problem, we refer the reader to [26, Chapter 17].

We now return to our discussion related to computing the relative oriented class group. Note that as referenced above, the groups under consideration have nice properties which make address-

ing the extension problem of (3.3) more approachable. For instance, we know that by definition, both Cl_L and $Cl^o_{L/K}$ are finite abelian groups. Further, the group $\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H$ is also a finite abelian group, and in fact, is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$ for some $s \leqslant r$. We therefore are in the case where our extension problem only involves abelian groups. Thus, we utilize an important tool of homological algebra, the Ext functors. We note important properties of this functor related to our present goal, but refer the interested reader to [26, Chapter 17] and [27] for an introduction to the tools of homological algebra and its development.

In our setting, we will consider the Ext groups

$$\text{Ext}^1_{\mathbb{Z}}(Cl_L, (\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H)).$$

These groups are in one to one correspondence with the isomorphism classes of extensions of Cl_L by $(\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H)$ (see for example [26, Chapter 17, Theorem 12] or [28, Theorem 3.4.3]). In particular, when $\text{Ext}^1_{\mathbb{Z}}(Cl_L, (\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H))$ is trivial, Equation 3.5 holds. As noted above,

$$\text{Ext}^1_{\mathbb{Z}}(Cl_L, (\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H)) \cong \text{Ext}^1_{\mathbb{Z}}(Cl_L, (\mathbb{Z}/2\mathbb{Z})^s)$$

for $s \leqslant r$. Therefore by properties of Ext [28, Proposition 3.3.4] we have

$$\begin{aligned} \text{Ext}^1_{\mathbb{Z}}(Cl_L, (\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H)) &\cong \text{Ext}^1_{\mathbb{Z}}(Cl_L, (\mathbb{Z}/2\mathbb{Z})^s) \\ &\cong \bigoplus_s \text{Ext}^1_{\mathbb{Z}}(Cl_L, (\mathbb{Z}/2\mathbb{Z})). \end{aligned}$$

Now, by the structure theorem for finite abelian groups, we have

$$Cl_L \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{m_i}\mathbb{Z}$$

for some $n \in \mathbb{Z}$ where the p_i are prime integers, the m_i are positive integers and $h_L = p_1^{m_1} \cdots p_n^{m_n}$. Then, by properties of $\text{Ext}^1_{\mathbb{Z}}$ as described in [26, Example 2 pg. 790]

$$\begin{aligned}\mathrm{Ext}^1_{\mathbb{Z}}(Cl_L, \mathbb{Z}/2\mathbb{Z}) &\cong \mathrm{Ext}^1_{\mathbb{Z}}(\bigoplus_i \mathbb{Z}/p_i^{m_i}\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \\ &\cong \bigoplus_i \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p_i^{m_i}\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \\ &\cong \bigoplus_{\{i|p_i=2\}} \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

So,

$$\mathrm{Ext}^1_{\mathbb{Z}}(Cl_L, (\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H)) \cong \mathrm{Ext}^1_{\mathbb{Z}}(Cl_L, (\mathbb{Z}/2\mathbb{Z})^s) \cong \bigoplus_{s \cdot \#\{i|p_i=2\}} \mathbb{Z}/2\mathbb{Z}.$$

Therefore, in the case that all of the p_i are odd, we obtain the trivial group.

Lemma 3.17. *If h_L is odd, $Ext^1_{\mathbb{Z}}(Cl_L, (\{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r / H))$ is trivial which corresponds to the trivial extension. So we have $Cl^o_{L/K} \cong Cl_L \times \{\pm 1\}^r / H$.*

We make two small, but important remarks.

Remark 3.18. In general, every group in Equation 3.3 is abelian. So, the existence of a splitting $\varphi : Cl_L \to Cl^o_{L/K}$ is equivalent to the condition $Cl^o_{L/K} \cong Cl_L \times \{\pm 1\}^r / H$. The second note is that one can show Lemma 3.17 directly using the Schur–Zassenhaus theorem (see for example [29, Chapter 4, Section 7]).

Now, the case when h_L is even requires more work, and it is in this case where our work with Ext is useful in determining the structure of the relative oriented class group explicitly. Of course, a natural question to ask is whether or not (3.5) holds in general, that is, one might wonder if a splitting can always be constructed. As such, we construct a counterexample to show that the sequence

$$1 \to \mathcal{O}_L \times \langle \pm 1 \rangle^r / H \to Cl^o_{L/K} \to Cl_L \to 1$$

does not split in general.

Example 3.19. Take $K = \mathbb{Q}(\sqrt{5})$, $L = K(\sqrt{101})$, that is L is the biquadratic number field $\mathbb{Q}(\sqrt{5}, \sqrt{101})$. In this case we have that $Cl_L \cong \mathbb{Z}/2\mathbb{Z}$. We compute the system of fundamental units of L using Sagemath and find that $H = \langle(-1,-1)\rangle$. With this set-up the extension problem has the form

$$1 \to \mathbb{Z}/2\mathbb{Z} \to Cl^o_{L/K} \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

By the previous calculations using Ext, there are two possibilities for $Cl^o_{L/K}$ up to isomorphism. Note that even without the computations above, we know $Cl^o_{L/K}$ has order 4 of which there are two groups up to isomorphism. In any case, we see that the two possibilities are

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$$

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1,$$

the first of which is not split. In what follows we find an element of order 4 in $Cl^o_{L/K}$, showing the first sequence is in fact the solution.

Consider the $\mathcal{O}_L$ ideal $J = (3, \sqrt{5}+\sqrt{101})$. One can verify that J is not principal. However, we know that J^2 is principal since the order of the class group is 2. Indeed J^2 is the ideal generated by $\alpha = \sqrt{101}+\frac{5}{2}\sqrt{5}-\frac{9}{2}$. So, consider the square of $(J;(1,1))$, namely the oriented ideal $((\alpha);(1,1))$. Now,

$$\begin{aligned} N_{L/K}(\alpha) &= \left(\sqrt{101} + \frac{5}{2}\sqrt{5} - \frac{9}{2}\right)\left(-\sqrt{101} + \frac{5}{2}\sqrt{5} - \frac{9}{2}\right) \\ &= -\frac{45}{2}\sqrt{5} - \frac{99}{2} \end{aligned}$$

with $\underline{\text{sgn}}\left(-\frac{45}{2}\sqrt{5} - \frac{99}{2}\right) = (-1,1)$. By [10, Lemma 2.18] we have that

$$(\mathcal{O}_L;(1,1)) \sim ((\alpha);(-1,1)).$$

So, it is not possible for the class of $((\alpha);(1,1))$ to be equivalent to the identity class since in order for $((\alpha);(1,1)) \sim ((\alpha);(-1,1)) \sim (\mathcal{O}_L;(1,1))$ there would have to exist a unit of L with sign configuration $(-1,1)$ which does not exist since $H = \langle(-1,-1)\rangle$. Therefore, the class of $(J;(1,1))$ does not have order 2 and so the relative oriented class group must be $\mathbb{Z}/4\mathbb{Z}$. That is, in this case the exact sequence

$$1 \to \mathcal{O}_L \times \langle \pm 1 \rangle^r / H \to Cl^o_{L/K} \to Cl_L \to 1$$

does not split which implies $Cl^o_{L/K} \ncong Cl_L \times \langle \pm \rangle^r / H$.

As demonstrated throughout this section, when a system of fundamental units is known for $\mathcal{U}_L$, determining H as a union of orbits is a useful tool for determining the associated relative oriented class group. The problem of determining a system of fundamental units has been investigated by many people. In the next section we consider only a small subset of the cases in which such a system is known. However, with the counterexample above in mind, we see that in many cases computing the relative oriented class group explicitly will require more work than computing H itself. Therefore, in many of the special cases considered below, we write our results in terms of H, keeping in mind that when the class number of L is odd, this yields an explicit description of the relative oriented class group. In this way, these special cases can be understood as extensions of the computations of Zemková in [10, Proposition 3.9].

Further, we note questions regarding class number parity have been studied extensively. In what follows we will consider results about H in which immediate descriptions of $Cl^o_{L/K}$ can be computed when h_L is odd. As the cases when L is a multiquadratic field or a CM extension will be considered in what follows, we note work relevant to these cases. For example, class number parity for multiquadratic number fields was considered in [30] and [31]. The case of cyclotomic extensions, those discussed in Section 3.3.2, has been investigated in depth, for example in [32] and [33].

3.3 Special Cases

We dedicate this section to special cases where we have considered computations related to the relative oriented class group. First, we consider the case when K is a real quadratic number field, L/K is a relative quadratic extension, and $L/\mathbb{Q}$ is Galois. In this case we provide an extension of Proposition 3.1 via Theorem 3.4 and information about norms of units. We then describe computations of H for quadratic extensions L/K where L is a CM field and K is its totally real subfield. We end the section by briefly noting the case when $L/\mathbb{Q}$ is a quartic extension which is not Galois, and describe the relationship between the relative oriented class group for conjugate fields.

In each of these special cases, we rely on a description of the fundamental system of units, and the respective norms arising from each system's elements, to provide general descriptions of the corresponding relative oriented class groups. As such, the reader can come to understand the motivation of Theorem 3.4 and cases where knowledge about units is itself sufficient information for computing H. For the sake of completeness, we provide descriptions of the set-up in each case. Note that we label each special case according to the corresponding conditions on the field L.

3.3.1 Galois Quartic Fields

Inspired by the work of Zemková in Proposition 3.1 and our strategy described above, we first look to the case when K is a real quadratic extension and L a quadratic extension of K with $L/\mathbb{Q}$ Galois. In this case $\mathrm{Gal}(L/\mathbb{Q})$ is either isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We call the extension $L/\mathbb{Q}$ a *cyclic* degree 4 extension or a *biquadratic* extension, respectively. Indeed, both types of extensions L arise in our setting, as demonstrated in the next example.

Example 3.20. Let $K = \mathbb{Q}(\sqrt{5})$ and $L_1 = \mathbb{Q}(\zeta_5)$. Then L_1 is Galois over $\mathbb{Q}$ with Galois group isomorphic to $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ where an integer $a \bmod 5$ maps to the automorphism determined by $\zeta_5 \mapsto \zeta_5^a$. To see that K is indeed a quadratic subfield of L_1, we note that $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ is the quadratic subfield of L_1 fixed by complex conjugation. To see that this field is actually K, let $\alpha = \zeta_5 + \zeta_5^{-1}$ and note that $\alpha^2 = 2 + \zeta_5^2 + \zeta_5^3$ which satisfies the polynomial $x^2 + x - 1$ which has roots $(-1 \pm \sqrt{5})/2$ which we know are both units of K (see Example 1.6). It is actually true

in much greater generality that extensions of the form $\mathbb{Q}(\zeta_p)$ always contain the quadratic subfield $\mathbb{Q}(\sqrt{p})$ for primes $p \equiv 1 \bmod 4$ [[34], Ch 2].

On the other hand, we can consider the relative quadratic extension L_2/K given by $L_2 = \mathbb{Q}(\sqrt{5}, \sqrt{2})$. The elements of Gal$(L_2/\mathbb{Q})$ are determined by where they send $\sqrt{5}$ and $\sqrt{2}$:

$\sigma(\sqrt{5})$	$\sigma(\sqrt{2})$
$\sqrt{5}$	$\sqrt{2}$
$\sqrt{5}$	$-\sqrt{2}$
$-\sqrt{5}$	$\sqrt{2}$
$-\sqrt{5}$	$-\sqrt{2}$

From this it is not hard to see that Gal$(L_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein four group. We could generalize this example as one might expect. Suppose a and b are relatively prime squarefree integers and consider $K = \mathbb{Q}(\sqrt{a})$ and $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Then the elements of Gal$(L/\mathbb{Q})$ are given by where they send $\sqrt{a}$ and $\sqrt{b}$, determined analogously to the above table.

Of course, in both cases $L/\mathbb{Q}$ is an abelian extension, and thus our work in the previous section applies. In either case, there are two real embeddings $K \hookrightarrow \mathbb{R}$, which we will denote by id and σ and the elements of H are generated by tuples $(\text{sgn}(\text{id}(N_{L/K}(u))), \text{sgn}(\sigma(N_{L/K}(u))))$, for each element u in the fundamental system of units of L. We sometimes relax notation and omit the id in the first entry of our tuples. In these cases we still consider the first entry to be the sign of an element after being embedded into $\mathbb{R}$ by id.

Applying Theorem 3.4 to this case implies that for any tower of extensions $L/K/\mathbb{Q}$, with $[L : K] = [K : \mathbb{Q}] = 2$ and $L/\mathbb{Q}$ Galois, the subgroup H can not contain only one of $(-1, 1)$ or $(1, -1)$, as these elements are in the same orbit of (3.1). As such, in this special case, determining the signs of norms of units (and consequently determining elements of H) will depend on our ability to determine when units in L have absolute norm -1. Extensive work has been done to understand when number fields contain a unit with absolute norm -1, for instance, the work of

Maria Stadnik [20]. The following result, [20, Proposition 7.2], demonstrates an important fact about the relationship between norms of units in a number field and norms of units in its subfields.

Lemma 3.21. *[20, Proposition 7.2] If L is a number field containing a unit of absolute norm -1, then every subfield K of L must also contain a unit of absolute norm -1.*

Proof. Let $u \in \mathcal{U}_L$ such that $N_{L/\mathbb{Q}}(u) = -1$. Take $v = N_{L/K}(u)$, then
$N_{K/\mathbb{Q}}(v) = N_{K/\mathbb{Q}}(N_{L/K}(u)) = N_{L/\mathbb{Q}}(u) = -1$. □

Armed with this result, Theorem 3.4 immediately yields a condition for the oriented class group of L/K to coincide with the class group of L.

Lemma 3.22. *Let K be a real quadratic number field with narrow class number 1 and L/K a relative quadratic extension with $L/\mathbb{Q}$ Galois. If L contains a unit of absolute norm -1, then $H = \langle \pm 1 \rangle^2$. That is, $Cl^o_{L/K} \cong Cl_L$.*

Proof. Suppose $u \in \mathcal{U}_L$ such that $N_{L/\mathbb{Q}}(u) = -1$. Then, by Lemma 3.21, there exists $v \in \mathcal{U}_K$ such that $N_{K/\mathbb{Q}}(v) = -1$. In particular, take $v = N_{L/K}(u)$. So, $v\sigma(v) = -1$, and thus $(\text{sgn}(v), \text{sgn}(\sigma(v))) = (-1, 1)$ or $(\text{sgn}(v), \text{sgn}(\sigma(v))) = (1, -1)$. We have $(-1, 1) \in H$ or $(1, -1) \in H$. By Theorem 3.4, $H = \langle \pm 1 \rangle^2$. In this case, we have that $Cl^o_{L/K} \cong Cl_L$. □

We are left to address the case when all units of L have norm $+1$. The following result gives a condition on the oriented class group of L/K which depends on the signs of the relative norms of units in L.

Lemma 3.23. *Let K be a real quadratic number field with narrow class number 1 and L/K a relative quadratic extension with $L/\mathbb{Q}$ Galois. Suppose $N_{L/\mathbb{Q}}(u) = 1$ for all $u \in \mathcal{U}_L$.*

(a) If $\exists u \in \mathcal{U}_L$ such that $id(N_{L/K}(u)) < 0$, then $H = \langle (-1, -1) \rangle$.

(b) Otherwise, H is trivial.

Proof. Let $u \in \mathcal{U}_L$, then $N_{L/\mathbb{Q}}(u) = N_{K/\mathbb{Q}}(N_{L/K}(u)) = 1$ by assumption. As K is a quadratic extension, we can write this condition as

$$N_{L/\mathbb{Q}}(u) = N_{K/\mathbb{Q}}(N_{L/K}(u)) = N_{L/K}(u)\sigma(N_{L/K}(u)) = 1.$$

Thus, it must be the case that either both $\text{sgn}(N_{L/K}(u))$ and $\text{sgn}(\sigma(N_{L/K}(u)))$ equal -1 or $\text{sgn}(N_{L/K}(u))$ and $\text{sgn}(\sigma(N_{L/K}(u)))$ equal $+1$. Thus, H is either generated by $(-1,-1)$ or is trivial, with the first case occurring if and only if $\exists u \in \mathcal{U}_L$ such that $\text{id}(N_{L/K}(u)) < 0$. Then conditions (a) and (b) follow directly from the definition of H.

□

Putting this all together, we obtain the following result, note that by Example 3.19, the condition on the class number in the second and third cases is necessary, as Case 2 is known to fail in general.

Theorem 3.24. *Let K be a real quadratic number field with narrow class number 1. Let L be a relative quadratic extension of K with $L/\mathbb{Q}$ Galois.*

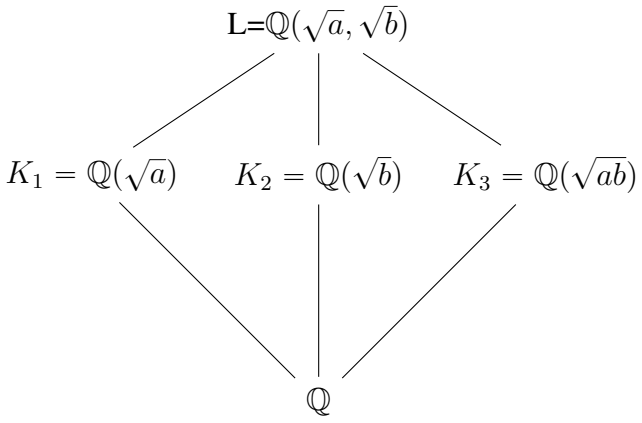
1. *If there exists some $u \in \mathcal{U}_L$ such that $N_{L/\mathbb{Q}}(u) = -1$ then $Cl^o_{L/K} \cong Cl_L$.*
2. *If $N_{L/\mathbb{Q}}(u) = 1$ for all $u \in \mathcal{U}_L$ and there exists some $u \in \mathcal{U}_L$ such that id$(N_{L/K}(u)) < 0$ and h_L is odd, then $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle$.*
3. *If $N_{L/\mathbb{Q}}(u) = 1$ and id$(N_{L/K}(u)) > 0$ for all $u \in \mathcal{U}_L$ and h_L is odd, then $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^2$.*

Proof. The first case holds by Lemma 3.22. The second two cases follow from Lemma 3.23 and Lemma 3.17. □

Therefore, this result gives us conditions when completely determining the relative oriented class group for L/K with K a real quadratic number field with narrow class number one is possible.

Example 3.25. Each case outlined in Theorem 3.24 is possible. In fact, we may construct examples, all of which come from the case that L is a totally real biquadratic field. Recall, a totally real

biquadratic field is a degree 4 extension of $\mathbb{Q}$ with Galois group $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. That is, for positive squarefree integers a and b we have $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with three quadratic subfields as described below:



We fix $K = \mathbb{Q}(\sqrt{5})$, which by Example 2.1 has narrow class number 1. We consider quadratic extensions of K which are Galois over $\mathbb{Q}$ and realize each case of Theorem 3.24.

Case 1: Take $L = \mathbb{Q}(\sqrt{5}, \sqrt{2})$. The group of units of L has rank 3, which means there are three units in a system of fundamental units for L. Consider one such unit

$$u = \sqrt{2} + \frac{1 - \sqrt{5}}{2} \in \mathcal{U}_L.$$

Since $N_{L/\mathbb{Q}}(u) = -1$, we have $H = \langle \pm 1 \rangle^2$ and thus $Cl^o_{L/K} \cong Cl_L$. The field L has class number 1, and so in this case the relative oriented class group is trivial.

Case 2: Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{7})$. We compute the fundamental units of L to be

$$u_1 = \frac{-1 - \sqrt{5}}{2},$$

$$u_2 = \left(-\frac{1}{2}\sqrt{5} + \frac{3}{2}\right)\sqrt{7} - \frac{3}{2}\sqrt{5} + \frac{7}{2}$$

and

$$u_3 = \left(-\frac{1}{2}\sqrt{5} - \frac{3}{2}\right)\sqrt{7} + \frac{3}{2}\sqrt{5} + \frac{7}{2}.$$

Then $N_{L/\mathbb{Q}}(u_i) = 1$ for $i = 1, 2, 3$ yet $N_{L/K}(u_2) = -1$, so $H = \langle(-1, -1)\rangle$ and since L again has class number 1, $Cl^o_{L/K} \cong Cl_L \times \langle\pm 1\rangle \cong \langle\pm 1\rangle$.

Case 3: Lastly, take $L = \mathbb{Q}(\sqrt{5}, \sqrt{11})$. Consider the system of fundamental units of L, given by

$$u_1 = \frac{-1 - \sqrt{5}}{2},$$

$$u_2 = 2\sqrt{11} - 3\sqrt{5}$$

and

$$u_3 = -10 - 3\sqrt{11}.$$

We note that $N_{L/\mathbb{Q}}(u_i) = 1$ for $i = 1, 2, 3$. Further, $N_{L/K}(u_1) = \frac{3+\sqrt{5}}{2}$ is positive under both real embeddings of K and $N_{L/K}(u_2) = N_{L/K}(u_3) = 1$. Thus, we have that H is trivial and $Cl^o_{L/K} \cong Cl_L \times \langle\pm 1\rangle^2 \cong \langle\pm 1\rangle^2$, as L has class number 1.

It may be interesting to consider whether or not given a biquadratic extension, we can determine a relationship between the relative oriented class groups for the three extensions L/K_i as in Example 3.25. It turns out the answer to this question can be understood by investigating the relationship between $\mathcal{U}_L$ and the $\mathcal{U}_{K_i}$. In the case of a totally real biquadratic field, the unit group structure was completely classified by Kubota [35] (see also [20]). We consider one of these cases in the following result.

Lemma 3.26. *Suppose L is a totally real biquadratic field such that every quadratic subfield of L has a unit with norm -1. Then L contains a quadratic subfield whose class number is not 1.*

Proof. Denote by K_1, K_2, and K_3 the three quadratic subfields of L. Denote by $\varepsilon_1, \varepsilon_2, \varepsilon_3$ their respective fundamental units, and their respective class numbers by h_1, h_2, and h_3. Since each quadratic subfield of L has a unit with norm -1, by [35] we have that any system of fundamental units of L is of the form $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ or $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}\}$. As such, we proceed in two cases.

If the fundamental units of L are of the form $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$, then by Kuroda's class number formula [36],

$$h_L = \frac{1}{4} h_1 h_2 h_3$$

and some $h_i \neq 1$. Similarly, if fundamental units of L are of the form $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_1 \varepsilon_2 \varepsilon_3}\}$, then Kuroda's class number formula yields

$$h_L = \frac{1}{2} h_1 h_2 h_3$$

and again some $h_i \neq 1$ else $h_L \notin \mathbb{Z}$. □

Example 3.27. Consider the totally real biquadratic number field $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Then the three quadratic subfields of L are $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{5})$ and $K_3 = \mathbb{Q}(\sqrt{10})$, (see Example 3.25). The fundamental units of these subfields are $\varepsilon_1 = \sqrt{2} + 1$, $\varepsilon_2 = \frac{1}{2}\sqrt{5} - \frac{1}{2}$, and $\varepsilon_3 = \sqrt{10} + 3$, respectively. One can easily verify the norm of each ε_i is -1. Therefore, each subfield of L has a unit with norm -1, and indeed, one of the subfields of L, namely K_3 has $h_{K_3} = 2$.

Therefore, we see that in general, we can not determine a relationship among the relative oriented class groups of quadratic subfields of such fields L. Indeed, in the case explored above, the condition of having narrow class number 1 is not met by all three K_i.

We now move on to a particularly special case, when L/K is CM. Here, the subgroup H can be determined in general.

3.3.2 CM Fields

Recall that a number field E is totally real if all of the embeddings $E \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$ and totally imaginary if none of its embeddings $E \hookrightarrow \mathbb{C}$ lie in $\mathbb{R}$. A CM field is a totally imaginary quadratic extension of a totally real field. We now consider the relative oriented class groups of CM extensions L/K, once again restricting to the case when the totally real field K is taken to have narrow class number 1. We note that in this special case general facts about norms of units in L allow us to compute the subgroup H by definition.

Example 3.28. Consider the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ of the nth cyclotomic field over its maximal real subfield as in Example 2.4. Then $\mathbb{Q}(\zeta_n)$ is an example of a CM field since the minimal polynomial of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is given by $x^2 - (\zeta + \zeta^{-1})x + 1$ and $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of $\mathbb{Q}(\zeta_n)$ fixed by conjugation. So in particular, all fields $\mathbb{Q}(\zeta_n)$ are CM fields. In general, one can build a CM field by adjoining to a totally real field the square root of some number for which all conjugates are negative (see for instance [34, Ch. 1 and 2]).

Let p be a prime integer and $L = \mathbb{Q}(\zeta_p)$ and K its maximal real subfield $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. From [34, Prop 1.5], any unit of L can be written as $\zeta_p^m v$ for some $m \in \mathbb{Z}$ and $v \in \mathcal{U}_K$. Therefore, for any $u \in \mathcal{U}_L$ there are $m \in \mathbb{Z}$ and $v \in \mathcal{U}_K$ such that we compute the norm of u to be

$$N_{L/K}(u) = N_{L/K}(\zeta_p^r v) = (\zeta_p^r v)(\zeta_p^{-r} v) = v^2 \in K.$$

Since the norm of u is a square in K, its image under each of the $\frac{p-1}{2}$ real embeddings of K is positive. Therefore, the only element in H is the trivial element of $\langle \pm 1 \rangle^{(p-1)/2}$. So H is trivial by definition for all cyclotomic extensions $\mathbb{Q}(\zeta_p)$ over their maximal real subfields.

In general, for the case when L/K is CM, the relationship between the unit groups of L and K is well understood. For example, even without our usual restrictions on the field K, one can say the following, where Q is called the Hasse unit index.

Theorem 3.29. *[34, Theorem 4.12] Denote by L some CM field, K its maximal real subfield, and $\mu_{\mathcal{O}_L}$ the group of roots of unity of L. Then*

$$Q = [\mathcal{U}_L : \mu_{\mathcal{O}_L}\mathcal{U}_K] = 1 \text{ or } 2.$$

In particular, when $L = \mathbb{Q}(\zeta_n)$ with n a prime power, $Q = 1$ (see [Cor 4.13, [34]]). Thus, we can replace p with a prime power in the discussion following Example 3.28. However, it turns out that once we restrict K to have narrow class number 1, we can say even more about the relationship between $\mathcal{U}_L$ and $\mathcal{U}_K$ (see for example, [21, Lemma 3.1]).

Lemma 3.30. *[21, Lemma 3.1] Suppose K is a totally real field with narrow class number 1 and L/K a CM extension. Then*

$$\mathcal{U}_K^2 \subseteq N(\mathcal{U}_L) \subseteq \mathcal{U}_K^+ \subseteq \mathcal{U}_K. \tag{3.7}$$

Which immediately allows us to extend our discussion in this section to all CM fields L with maximal real subfield K with narrow class number 1.

Proposition 3.31. *Let K be a totally real field with narrow class number 1 with r real embeddings and L/K a CM extension. Then H is trivial, that is, the size of the relative oriented class group is as large as possible.*

Proof. As every element $v \in \mathcal{U}_L$ has $N_{L/K}(v) \in \mathcal{U}_K^+$ by Lemma 3.30, the result follows from the definition of H and Definition 2.14. □

Therefore, throughout this section we have shown that every CM extension L/K where the class number of L is odd has relative oriented class group given by $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^r$. For example, those extensions L/K as in the first part of Example 2.4 satisfy this property.

3.3.3 Non-Galois Quartic Fields

We briefly consider the case when K is a real quadratic extension and L/K is quadratic with $L/\mathbb{Q}$ not Galois. The purpose for this special case is of a different flavor from the previous two. In particular, we depart from our focus on computations of the relative oriented class group for a given L/K and investigate the relationship of relative oriented class groups for conjugate fields. We include this information as it may prove useful in further cases where L is known to not be Galois over $\mathbb{Q}$. For more details related to this case and ideas for computing the relative oriented class group for L/K where L is a quartic extension of $\mathbb{Q}$ and not Galois, we refer the reader to Chapter 5.

Let K be a real quadratic number field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \langle \sigma \rangle$ and L/K be a degree 2 extension such that $L/\mathbb{Q}$ is not Galois. We begin by determining the Galois closure of $L/\mathbb{Q}$. First, we note that since $L/\mathbb{Q}$ is not Galois, $\sigma(L) \neq L$ and call $\sigma(L) = L'$. Then $LL' = \tilde{L}$ is the Galois closure

of L with $[\tilde{L} : \mathbb{Q}] = 8$. Then, $\tilde{G} = \text{Gal}(\tilde{L}/\mathbb{Q})$ is a nonabelian group of order 8, so we have two candidates, D_4 or Q_8. Since $\tilde{G}$ must contain two subgroups of order 2 which are not normal, we conclude that $\text{Gal}(\tilde{L}/\mathbb{Q}) \cong D_4$.

We can thus determine fields L which fit into our discussion by considering D_4 extensions, which are well studied (see for example [37]). In this section we consider those which are *pure* quartic extensions. The other case is noted in Chapter 5.

Definition 3.32. A field L is a pure quartic extension of $\mathbb{Q}$ if $L = \mathbb{Q}(\alpha)$ where α is the root of an irreducible polynomial $x^4 - m \in \mathbb{Z}[x]$ with $\arg(\alpha) = 0$ if $m > 0$ and $\arg(\alpha) = \pi/4$ if $m < 0$.

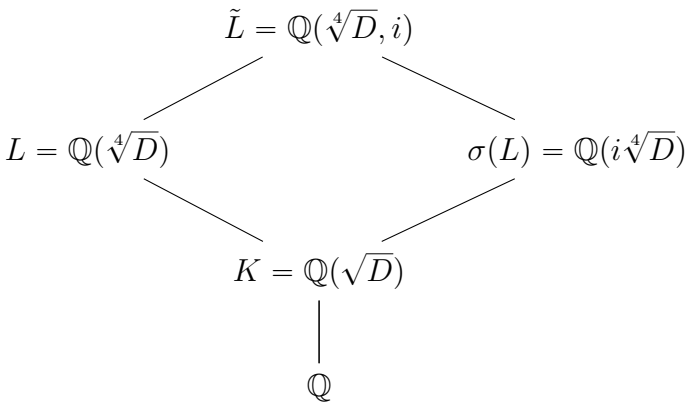
Remark 3.33. As discussed in [38], it is sufficient to consider the case when

- $m = ab^2c^3 \neq -4$ with $a \neq 1$
- b and c are taken to be positive and square free with $(b, c) = 1$
- $|a| \geqslant c$ if a is odd and c odd

where $a, b, c \in \mathbb{Z}$.

An interesting connection to our discussion on biquadratic fields then arises in the following way: $K = \mathbb{Q}(\alpha^2/bc)$ is a quadratic subfield of L and $L/\mathbb{Q}$ is Galois if and only if $ac = -1$. In this case, we have $m = -b^2$ and L is a biquadratic extension $\mathbb{Q}(i, \sqrt{2b})$ ([38] Lemma 4).

In any case, we consider towers of fields of the following form.



Note that both L and L' are quadratic extensions of the number field K which is assumed to be totally real and of narrow class number 1. In the setting of this special case, we consider whether or not the oriented class group of these two extensions coincide. That is, we are interested in the relationship between the oriented class groups of *conjugate* fields.

Conjugate fields

Let E/F be a finite Galois extension with Galois group $G = \text{Gal}(E/F)$. Let M be an intermediate field, $F \subseteq M \subseteq E$, which corresponds with the subgroup N of G. Let $\sigma \in G$, then $\sigma(M)$ corresponds to the subgroup $\sigma N \sigma^{-1}$. We refer to $\sigma(M)$ as a *conjugate field* of M. In the case that N is a normal subgroup of G, then $\sigma N \sigma^{-1} = N$ and $\sigma(M) = M$ for all $\sigma \in G$, which is exactly the condition which makes M/F a Galois extension, with Galois group G/N. However, if N is not normal, there is some $\sigma \in G$ with $\sigma(M) \neq M$, we can consider the conjugate field $\sigma(M)$ which is distinct from M.

Rephrasing this in our setting of interest, we have K a real quadratic number field of narrow class number 1 and L/K a relative quadratic extension with Galois closure $\tilde{L}$. Recall, $\text{Gal}(\tilde{L}/\mathbb{Q}) \cong D_4 \cong \langle \sigma, \tau \rangle$, where

$$\sigma(\sqrt[4]{D}) = i\sqrt[4]{D}, \;\; \sigma(i) = i$$

$$\tau(\sqrt[4]{D}) = \sqrt[4]{D}, \;\; \tau(i) = -i.$$

The Galois correspondence for these fields is given by

$$\mathbb{Q} \longleftrightarrow D_4, \;\; K \longleftrightarrow \langle \sigma^2, \tau \rangle,$$

$$L \longleftrightarrow \langle \tau \rangle, \;\; \sigma(L) \longleftrightarrow \sigma \langle \tau \rangle \sigma^{-1} = \langle \sigma^2 \tau \rangle,$$

and

$$\tilde{L} \longleftrightarrow \langle \text{id} \rangle.$$

The generators for Gal(L/K) and Gal$(\sigma(L)/K)$ lift to $\sigma^2\tau$ and τ, respectively. In the following result, we compute the relative oriented class group for conjugate fields.

Lemma 3.34. *Let K be a real quadratic number field with L/K a relative degree two extension which is not Galois over $\mathbb{Q}$. Then, $Cl^o_{L/K} \cong Cl^o_{\sigma(L)/K}$.*

Proof. Let $u \in \mathcal{U}_L$ and consider $v = \sigma(u) \in \mathcal{U}_{\sigma(L)}$. Denote by ρ_1 and ρ_2 the nontrivial elements of Gal(L/K) and Gal$(\sigma(L)/K)$. Then,

$$\begin{aligned} N_{\sigma(L)/K}(v) &= N_{\sigma(L)/K}(\sigma(u)) \\ &= \sigma(u)\rho_2(\sigma(u)) \\ &= \sigma(u\rho_1(u)) \\ &= \sigma(N_{L/K}(u)) \\ &= N_{L/K}(u), \end{aligned}$$

where the third equality follows from $\sigma^{-1}\rho_2\sigma = \rho_1$. By the fact that the class groups of conjugate fields are isomorphic, we obtain the result. □

As mentioned above, such a relationship will come into play in future work based on extending our computations of the relative oriented class group when $L/\mathbb{Q}$ is not Galois (see Chapter 5).

We now turn to the final section of this chapter in which we consider the binary quadratic form interpretation of our computations of the relative oriented class group. In particular, we provide a method for determining representatives of each class of binary quadratic forms corresponding to the classes of the associated relative oriented class group. In this way one can view the next section as a natural extension of the calculations of Lemma 2.19.

3.4 Binary Quadratic Form Interpretation

We now have a good understanding of the relative oriented class groups for various types of degree two extensions of number fields. In this section, we consider the other side of the

Theorem 2.18, that is, the equivalence classes of binary quadratic forms defined over a totally real number field K with narrow class number 1 with discriminant in some $\mathcal{D}$ (see Equation 2.2). We begin with a summary of known facts regarding an important class of quadratic forms, namely the totally positive definite ones. We continue by computing explicitly the classes of quadratic forms corresponding to the oriented class groups computed in Section 3.3.

Totally Positive Definite Binary Quadratic Forms

Let K be a totally real number field. Recall that an element $a \in K$ is totally positive if $\sigma(a) > 0$ for all real embeddings σ of K and define *totally negative* elements analogously. Let $L = K(\sqrt{D_\Omega})$ with D_Ω totally negative. In Section 1.5 we considered quadratic forms which were positive definite, that is, which represented only positive values. A related condition is as follows:

Definition 3.35. Let $Q(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form defined over a number field K. Then $Q(x, y)$ is totally positive definite if $\sigma(Q(x, y)) = \sigma(a)x^2 + \sigma(b)xy^2 + \sigma(c)y^2$ is positive definite for every real embedding $\sigma : K \hookrightarrow \mathbb{R}$.

The quadratic form $Q(x, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_\mathcal{D}$ is totally positive definite exactly when a is totally positive, and in this case, the corresponding oriented ideal is given by

$$\left(\left[a, \frac{-b + \sqrt{Disc(Q)}}{2} \right]_{\mathcal{O}_K} ; +1, \ldots, +1 \right)$$

see [10, Section 4]. Further, with the current set-up (with D_Ω totally negative) any two oriented ideals in the same class of $Cl^o_{L/K}$ have the same orientation [10, Lemma 4.1]. Define

$$\mathfrak{F}(c_1 + c_2\sqrt{D_\Omega}) = c_2$$

for any $c_1, c_2 \in K$ as in [10, Proposition 4.2 (iii)], then the following result classifies totally positive definite forms via the bijection of Theorem 2.18.

Proposition 3.36. *[10, Proposition 4.2] Let D_Ω be totally negative and $Q \in \mathcal{Q}_\mathcal{D}$ and let $i \in \{1, \ldots, r\}$. Then the following are equivalent*

(i) $\sigma_i(Q)$ *is positive definite*

(ii) Q *is the image under the map* Φ *of an oriented ideal* $([\alpha, \beta]; \underline{sgn}(\det M))$ *such that* $\sigma_i(\det M) > 0$

(iii) Q *is the image under the map* Φ *of an oriented ideal* $([\alpha, \beta]; \underline{sgn}(\det M))$ *such that* $\sigma_i\left(\mathfrak{F}\left(\frac{\beta}{\alpha}\right)\right) > 0$.

Biquadratic Extensions

We revisit Example 3.25 to understand the classes of binary quadratic forms corresponding to the oriented class group in each of the 3 cases. That is, we take a and b to be squarefree integers and consider $K = \mathbb{Q}(\sqrt{a})$, a real quadratic field of narrow class number 1, and $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Define $a_0 = a/\gcd(a, b)$ and $b_0 = b/\gcd(a, b)$. Note that

$$\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{a_0 b_0}) = \mathbb{Q}(\sqrt{b}, \sqrt{a_0 b_0}) = \mathbb{Q}(\sqrt{b}, \sqrt{a}). \tag{3.8}$$

We would like to first determine an integral basis for $\mathcal{O}_L$ as an $\mathcal{O}_K$-module, so that we can explicitly write down Ω for a given extension. Recall that we know such a basis exists since $h_K = 1$. Work in determining integral bases of biquadratic number fields over $\mathbb{Q}$ has been done by several people, with an explicit description of such bases given in [39]. The case we are interested in, in which we consider a biquadratic field with a quadratic subfield, was completed by Bird and Parry in [40]. The integral bases will depend on congruence $\bmod 4$, and Equation 3.8 implies that we must consider only the following congruences of $(a, b) \bmod 4$

$$(a, b) \equiv (1, 1), (1, 2), (2, 3) \text{ or } (3, 3) \bmod 4.$$

Such an integral basis of L/K need not exist, but will exactly when $L = K(\sqrt{D})$ where D is the discriminant of L/K [25]. The discriminant of L/K is computed in [[40], Lemma 1] to be

1. b_0 if $b \equiv 1 \bmod 4$

2. $4b_0$ when $a \equiv 1 \bmod 4$ and $b \not\equiv 1 \bmod 4$

3. $2b_0$ when $a \not\equiv 1 \bmod 4$ and $b \not\equiv 1 \bmod 4$.

In what follows, we utilize Theorem 1, Theorem 2, and Tables I and II from [40] to compute an integral basis of L over K. We begin with a general description of representatives of each class of $Cl^o_{L/K}$ for K a real quadratic field and L a biquadratic number field obtained as a quadratic extension of K by the square root of some fundamental element of $\mathcal{O}_K$. By Theorem 3.24, we know three cases arise in describing the possible structure of $Cl^o_{L/K}$. In what follows, we describe representatives for each of these three cases, simplifying each case by further assuming L has class number 1. Recall the three cases under consideration

1. L contains a unit with absolute norm -1. In this case, $Cl^o_{L/K} \cong Cl_L$.

2. All units of L have absolute norm 1, but there exists some unit of L whose relative norm is negative (that is, after being embedded into $\mathbb{R}$). In this case, when h_L is odd, $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle$.

3. All units of L have absolute norm 1 and all relative norms of units of L are positive when considered as real numbers. In this case, when h_L is odd, $Cl^o_{L/K} \cong Cl_L \times \langle \pm 1 \rangle^2$.

In what follows we denote by ε_K the fundamental unit of $K = \mathbb{Q}(\sqrt{a})$ and by $\tilde{\varepsilon}_K$ its image under the embedding which sends $\sqrt{a} \mapsto -\sqrt{a}$.

Proposition 3.37. *Take $K = \mathbb{Q}(\sqrt{a})$ be a real quadratic field of narrow class number 1 and $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ of class number 1 where a and b are relatively prime with $a \equiv 1 \bmod 4$ and $b \not\equiv 1 \bmod 4$. In the three cases of Theorem 3.24, the following are representatives of each class of quadratic forms in $\mathcal{Q}_\mathcal{D}$ (where $D = 4b$):*

1. *There is one class of quadratic forms, represented by*

$$Q_1(x, y) = x^2 - by^2.$$

2. *There are two classes of quadratic forms. The trivial class represented by*

$$Q_1(x, y) = x^2 - by^2$$

and the nontrivial class represented by

$$Q_2(x, y) = \varepsilon_K x^2 + b\tilde{\varepsilon}_K y^2.$$

3. *There are four classes of quadratic forms. The trivial class is represented by*

$$Q_1(x, y) = x^2 - by^2$$

and the three remaining classes by

$$Q_2(x, y) = \varepsilon_K x^2 + b\tilde{\varepsilon}_K y^2$$

$$Q_3(x, y) = -b\tilde{\varepsilon}_K x^2 - \varepsilon_K y^2$$

$$Q_4(x, y) = bx^2 - y^2.$$

Proof. By [40, Table I and Lemma II] we have that $\left[1, \sqrt{b}\right]_{\mathcal{O}_K}$ is an integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$. Since $(a, b) \equiv (1, b) \bmod 4$ with $b \not\equiv 1 \mod 4$ we have that $D = 4b$.

Case 1: By Theorem 2.18 and Example 2.19 we have that $Q_1(x, y) = x^2 - by^2$ is a representative of the only class of $Cl^o_{L/K}$.

Case 2: Again by Theorem 2.18 and Example 2.19 we have that $Q_1(x, y) = x^2 - by^2$ is a representative of the trivial class of $Cl^o_{L/K}$. In this case, the subgroup H has order two, and by Theorem 3.4 is thus generated by $\langle(-1, -1)\rangle$. So, consider the oriented ideal $((u); (1, -1))$ where $u \in \mathcal{U}_L$. We

note that by Lemma 2.16 this ideal is not in the trivial class of $Cl^o_{L/K}$. That is, the oriented ideal $((u);(1,-1))$ can not be equivalent to the oriented ideal $\left(\left[1,\sqrt{b}\right]_{\mathcal{O}_K};(1,1)\right)$, as $H=\langle(-1,-1)\rangle$ and so no unit of L has a relative norm whose sign configuration is equal to $(1,-1)$.

Denote by ε_K the fundamental unit of K and by $\tilde{\varepsilon}_K$ its conjugate. Then $\left[\varepsilon_K,\sqrt{b}\right]_{\mathcal{O}_K}$ is a basis for (u) over $\mathcal{O}_K$ since $(u)=\mathcal{O}_L$ and ε_K is invertible. Then, the matrix M as in 2.4 is

$$M=\begin{pmatrix}\epsilon_K & 0\\ 0 & 1\end{pmatrix}$$

with $\underline{\text{sgn}}(\det M)=(1,-1)$. So, by Theorem 2.18

$$Q_2(x,y)=\varepsilon_K x^2+b\tilde{\varepsilon}_K y^2$$

is a representative of the nontrivial class of $Cl^o_{L/K}$. Indeed, Q_2 is integral over K. Further, since K has narrow class number 1, $\varepsilon_K\tilde{\varepsilon}_K=-1$ by (1.4), so Q_2 has discriminant $-4\varepsilon_K\tilde{\varepsilon}_K b=4b$.

Case 3: We determine Q_1 and Q_2 as in the previous cases. To determine representatives for the third and fourth classes, we consider the image of the classes of the oriented ideals $((u);(-1,1))$ and $((u);(-1,-1))$ where again $u\in\mathcal{U}_L$.

To determine a representative of the class of $\mathcal{Q}_{\mathcal{D}}$ corresponding to the class of $((u);(-1,1))$, we take as our basis $[b,\varepsilon_K]_{\mathcal{O}_K}$, so

$$M=\begin{pmatrix}0 & 1\\ \varepsilon_K & 0\end{pmatrix}$$

with $\underline{\text{sgn}}(\det M)=(-1,1)$. So,

$$Q_3(x,y)=-b\tilde{\varepsilon}_K x^2-\varepsilon_K y^2$$

is a representative for the class corresponding to the class of $((u);(-1,1))$.

To determine a representative for the class corresponding to the class of $((u);(-1,-1))$, we take as basis $[\varepsilon_K b, \varepsilon_K]$. Thus, we obtain

$$M = \begin{pmatrix} 0 & \varepsilon_K \\ \varepsilon_K & 0 \end{pmatrix}$$

which has $\underline{\text{sgn}}(\det M) = (-1,-1)$. Then, under the bijection we obtain

$$Q_4(x,y) = bx^2 - y^2$$

as a representative of the last class of $\mathcal{Q}_{\mathcal{D}}$.

□

We end by considering the three examples of extensions L/K which realized the three cases as discussed in Example 3.25.

Example 3.38. We briefly describe the resulting representatives for the fields considered in Example 3.25. Recall that we fix $K = \mathbb{Q}(\sqrt{5})$ and consider L as a relative quadratic extension of K.

Case 1: Take $L = \mathbb{Q}(\sqrt{5}, \sqrt{2})$, then $\mathcal{O}_L = \left[1, \sqrt{2}\right]_{\mathcal{O}_K}$ and $D_\Omega = (\sqrt{2} - (-\sqrt{2}))^2 = 8$. The class group of L, Cl_L, is trivial, and thus by Equation 2.3, $Cl^o_{L/K}$ is trivial. The binary quadratic form $Q(x,y) = x^2 - 2y^2$ is a representative for the only class of $\mathcal{Q}_{\mathcal{D}}$. We note that this form is integral and indeed $\text{Disc}(Q(x,y)) = 8$.

Case 2: Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{7})$, then $\mathcal{O}_L = \left[1, \sqrt{7}\right]_{\mathcal{O}_K}$. We will consider the image of classes of oriented ideals in $Cl^o_{L/K}$, which will be elements of $\mathcal{Q}_{\mathcal{D}}$ where $D_\Omega = 28$. We have $h_L = 1$ and thus $Cl^o_{L/K} \cong \langle \pm 1 \rangle$. By Example 2.19, the trivial class of $Cl^o_{L/K}$ corresponds to the class with $x^2 - 7y^2$ as a representative.

We now determine a representative for the class corresponding to the nontrivial element of $Cl^o_{L/K}$. To do so, we consider the oriented ideal $((u_2);(1,-1))$ as $(1,-1) \notin H$. Recall $\varepsilon_K = \frac{\sqrt{5}}{2} - \frac{1}{2}$ is the fundamental unit of K. Now, let $\alpha = \varepsilon_K$ and $\beta = \sqrt{7}$ and notice that

$$u_2 = \left(-2 + 2\left(\frac{1+\sqrt{5}}{2}\right)\right)\alpha + \left(2 - \left(\frac{1+\sqrt{5}}{2}\right)\right)\beta.$$

Since $\left[1, \sqrt{7}\right]_{\mathcal{O}_K}$ is a basis for $\mathcal{O}_L$ and α is invertible, we have that $[\alpha, \beta]$ is also a basis. We have $M = \begin{pmatrix} \epsilon_K & 0 \\ 0 & 1 \end{pmatrix}$ with $\underline{\text{sgn}}(\det M) = (1,-1)$ as desired. Then, under the bijection of Theorem 2.18 we obtain the following as a representative of the nontrivial class of $\mathcal{Q}_{\mathcal{D}}$:

$$Q(x,y) = \varepsilon_K x^2 + 7\tilde{\varepsilon_K} y^2$$

where $\tilde{\epsilon_K} = \frac{1-\sqrt{5}}{2}$. Notice that $Q(x,y)$ is integral over K and has discriminant 28 as desired.

Case 3: Lastly, take $L = \mathbb{Q}(\sqrt{5}, \sqrt{11})$ with $\mathcal{O}_L = \left[1, \sqrt{11}\right]_{\mathcal{O}_K}$. The binary quadratic forms we compute will be representatives of $\mathcal{Q}_{\mathcal{D}}$ with $D_\Omega = 44$. We have $h_L = 1$ and thus $Cl^o_{L/K} \cong \langle \pm 1 \rangle^2$. The trivial class of $Cl^o_{L/K}$ corresponds to the class of quadratic forms equivalent to $x^2 - 11y^2$.

As H is trivial in this case, we need to determine representatives for the three non-trivial classes of $\mathcal{Q}_{\mathcal{D}}$. Consider the oriented ideal $((u_2);(1,-1))$ and note that $(1,-1) \notin H$. Recall, $\varepsilon_K = \frac{\sqrt{5}-1}{2}$ is the fundamental unit of K. Let $\alpha = \varepsilon_K$ and $\beta = \Omega$. Then we can write

$$u_2 = \left(-6 - 3\left(\frac{1+\sqrt{5}}{2}\right)\right)\alpha + 2\beta.$$

As in Case 2 we can show that $[\alpha, \beta]$ is an integral basis for the $\mathcal{O}_L$-ideal (u_2). Take $M = \begin{pmatrix} \varepsilon_K & 0 \\ 0 & 1 \end{pmatrix}$, which has $\underline{\text{sgn}}(\det M) = (1,-1)$. Under the bijection Φ we determine a representative of the corresponding class to be

$$\varepsilon_K x^2 + 11\tilde{\varepsilon_K} y^2.$$

If we instead take $\alpha = \Omega$ and $\beta = \varepsilon_K$, we again obtain a basis for the ideal (u_2), but here $M = \begin{pmatrix} 0 & 1 \\ \varepsilon_K & 0 \end{pmatrix}$ with $\underline{\text{sgn}}(\det M) = (-1, 1)$. Then under the bijection Φ, we obtain the class of the following quadratic form $-11\tilde{\varepsilon_K}x^2 - \varepsilon_K y^2$.

To obtain a representative of the fourth class of $\mathcal{Q}_{\mathcal{D}}$, consider the oriented ideal $((u_2); (-1, -1))$. We have that $[\varepsilon_K\Omega, \varepsilon_K]$ is a basis for (u_2) with $M = \begin{pmatrix} 0 & \varepsilon_K \\ \varepsilon_K & 0 \end{pmatrix}$ which has $\underline{\text{sgn}}(\det M) = (-1, -1)$. Then, under the bijection we obtain $11x^2 - y^2$ as a representative of the last class of $\mathcal{Q}_{\mathcal{D}}$.

This ends our discussion related to computing the objects on the relative oriented class groups side of the bijection in Theorem 2.18. In the next chapter, we continue our investigation related to the binary quadratic forms side of the bijection, this time considering questions of representability. In doing so, we will see a connection to our work computing the subgroups H and the usefulness of considering equivalent quadratic forms. These ideas will converge, yielding generalizations and extensions to the ideas first presented in Section 1.5.

Chapter 4

Representability

We again take K to be a totally real number field with narrow class number 1 and L/K a relative quadratic extension. In this section, we will consider representability (i.e. the representation problem) for primitive binary quadratic forms defined over K, that is, forms $Q(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathcal{O}_K$ and $\gcd(a, b, c) \in \mathcal{U}_K$. For an element $\lambda \in \mathcal{O}_K$, we want to determine whether or not there exist $x_0, y_0 \in \mathcal{O}_K$ such that $Q(x_0, y_0) = \lambda$. This question is well understood when the base field is taken to be $\mathbb{Q}$, and one considers an imaginary quadratic extension $L/\mathbb{Q}$ (see [8, Theorem 7.7 (iii)]).

Theorem 4.1. *Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic number field L. Then a positive integer m is represented by a primitive positive definite form $Q(x, y)$ of discriminant D if and only if m is the norm $N(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$ of some ideal $\mathfrak{a}$ in the corresponding ideal class in $Cl_{\mathcal{O}}$.*

The setting of the above result is that of the classical bijection outlined in the first case of Theorem 1.20. As such, we seek an analogous result regarding representability of binary quadratic forms defined over higher degree number fields with are totally positive and have narrow class number 1, as considered in the bijection of Theorem 2.18.

4.1 Generalizations of the Classical Case

Work has recently been done to investigate representability conditions for algebraic integers of totally real number fields of narrow class number 1 by binary quadratic forms defined over such fields. In particular, we thank Li, Monotovan, Pries, and Tang for discussions related to these questions, particularly concerning Lemma 4.2 and Theorem 4.4. In this section we determine conditions for representability which can be understood via the work done in Chapter 3. Indeed,

the subgroup H of sign configurations realized by norms of units, as defined in Equation 2.3, will again play a crucial role.

Recall from Section 2.3 that equivalent quadratic forms represent the same elements up to the square of a totally positive unit and their discriminants can differ up to the square of a totally positive unit. As remarked, our assumption that K is totally real with narrow class number 1 implies that every totally positive unit is a square of a unit. So, if $Q_1 \sim Q_2$ then the forms represent the same elements (see Lemma 2.11). Therefore, one particular strategy for determining whether or not a quadratic form represents some element is to determine an equivalent form which represents that element.

Recall Lemma 1.19, which the following result generalizes. We include the proof, though it follows analogously from the classical case.

Lemma 4.2. *Let K be a totally real number field with narrow class number 1. Suppose*

$$Q(x, y) = ax^2 + bxy + cy^2$$

is a primitive quadratic form over $\mathcal{O}_K$. Let $\lambda \in \mathcal{O}_K$. Then the following are equivalent

- *There exist $x_0, y_0 \in \mathcal{O}_K$ such that $Q(x_0, y_0) = \lambda$;*
- *Q is equivalent to the quadratic form $Q_0(x, y) = \lambda x^2 + b_0xy + c_0y^2$ for some $b_0, c_0 \in \mathcal{O}_K$.*

Proof. Suppose there exist $x_0, y_0 \in \mathcal{O}_K$ such that $Q(x_0, y_0) = \lambda$. Then since Q is primitive, we must have that x_0 and y_0 are relatively prime. Since K has class number 1, there exist $s, q \in \mathcal{O}_K$ such that $x_0s - y_0q = u$ where $u \in \mathcal{U}_K$ is the gcd of x_0 and y_0. Upon replacing s by $u^{-1}s$ and q by $u^{-1}q$, we obtain $x_0s - y_0q = 1$. Now, consider $Q(x_0x + qy, y_ox + sy)$ and note the coefficient on x^2 is $ax_0^2 + bx_0y_0 + cy_0^2 = \lambda$. Further, $b_0 = 2ax_0q + b(x_0s + qy_0) + 2cy_0s$ and $c_0 = Q(q, s)$. So, Q is equivalent to a quadratic form of the desired form. To show the other direction, suppose there exists some quadratic form Q_0 such that $Q \sim Q_0$. Then, since Q and Q_0 represent the same elements by Lemma 2.11 and $Q_0(1, 0) = \lambda$, Q also represents λ. □

This lemma immediately implies that if Q represents $u\lambda$ with $u \in \mathcal{U}_K^+$, then Q represents λ.

Lemma 4.3. *Let K be a totally real number field with narrow class number 1. Suppose $Q(x,y) = ax^2 + bxy + cy^2$ is a primitive quadratic form over $\mathcal{O}_K$. Then Q represents λ if and only if Q represents $u\lambda$ for $u \in \mathcal{U}_K^+$.*

Proof. Suppose Q represents $u\lambda$ where $u \in \mathcal{U}_K^+$. Then Q is equivalent to

$$Q_0(x,y) = u\lambda x^2 + b_0xy + c_0y^2$$

as in Lemma 4.2. We note that $Q_0(x,y) = uQ_1(x,y)$ where $Q_1(x,y) = \lambda x^2 + + \frac{b_0}{u}xy + \frac{c_0}{u}y^2$ and $Q_1(1,0) = \lambda$. Thus, $Q_0 \sim Q_1$ and therefore $Q \sim Q_1$. So Q represents λ. The backward direction follows analogously since the inverse of a totally positive unit is again totally positive. □

We utilize Lemma 4.2 in the following theorem. The result relies on the structure of the associated relative oriented class group and Theorem 2.18. In particular, given our usual set-up, an element λ is represented by Q if and only if it gives rise to a representative of the class of $Cl^o_{L/K}$ equivalent to the image of the class of Q under Zemková's bijection. In this way, one can consider what follows as a natural generalization of Theorem 4.1 to the present setting. We again acknowledge Li, Monotovan, Pries, and Tang for the proof of the following result.

Theorem 4.4. *Let K be a totally real number field of narrow class number 1. Let D be a fundamental element of $\mathcal{O}_K$. Let $L = K(\sqrt{D})$ and $\mathcal{D} = \{u^2D \mid u \in \mathcal{U}_K\}$. Let $Q(x,y)$ be a primitive binary quadratic form defined over K with discriminant in $\mathcal{D}$. Denote by I_Q the image of the class of Q under the bijection in Theorem 2.18. Let $\lambda \in \mathcal{O}_K$ be irreducible. Then the following are equivalent*

1. *The element λ is represented by Q.*
2. *λ is the norm of some ideal J such that the oriented ideal $(J; \underline{sgn}(\lambda))$ is in the class of I_Q.*

Proof. Suppose λ is represented by Q. By Lemma 4.2, Q must be equivalent to some quadratic form $Q_0(x,y) = \lambda x^2 + b_0xy + c_0y^2$ with $b_0, c_0 \in \mathcal{O}_K$. Denote by I_{Q_0} the representative corresponding to the class of Q_0 as in Theorem 2.18. Then $I_{Q_0} = \left(\left[\lambda, \frac{-b_0+\sqrt{\text{Disc}(Q_0)}}{2}\right]_{\mathcal{O}_K}; \underline{\text{sgn}}(\lambda)\right)$. Note that the matrix of $\left[\lambda, \frac{-b_0+\sqrt{\text{Disc}(Q_0)}}{2}\right]_{\mathcal{O}_K}$ has determinant λ. We know by [10, Lemma 2.6] that $\langle\lambda\rangle = N_{L/K}\left(\left[\lambda, \frac{-b_0+\sqrt{\text{Disc}(Q_0)}}{2}\right]_{\mathcal{O}_K}\right)$ and since $Q_0 \sim Q$, we have that I_{Q_0} is in the class of I_Q.

To show the backward direction suppose there exists some ideal J of $\mathcal{O}_L$ such that $\langle\lambda\rangle = N_{L/K}(J)$ as $\mathcal{O}_K$ ideals. Suppose also that $(J; \underline{\text{sgn}}(\lambda))$ is in the class of I_Q. We can find a basis for J, $[\alpha,\beta]_{\mathcal{O}_K}$, with matrix M such that $\det(M)$ has the same sign configuration as λ [10, Lemma 2.15]. In fact, since both $\det(M)$ and λ generate $N_{L/K}(J)$, they differ at most by some $u \in \mathcal{U}_K^+$. Then, after possibly adjusting the basis element α by $\frac{1}{u}$, the quadratic form corresponding to $[\alpha,\beta]_{\mathcal{O}_K}$ is given by

$$Q_1(x,y) = \frac{\alpha\overline{\alpha}x^2 - (\overline{\alpha}\beta + \alpha\overline{\beta})xy + \beta\overline{\beta}y^2}{\det(M)} = \frac{N_{L/K}(\alpha x - \beta y)}{\lambda}.$$

Since λ is contained in the ideal $N_{L/K}([\alpha,\beta]_{\mathcal{O}_K})$, there exist $x_0, y_0 \in \mathcal{O}_K$ such that $\lambda = \alpha x_0 + \beta y_0$. But then

$$Q_1(x_0,y_0) = \frac{\lambda\overline{\lambda}}{\lambda} = \frac{\lambda^2}{\lambda} = \lambda.$$

Since $Q_1 \sim Q$, we have that Q also represents λ.

□

Remark 4.5. We immediately obtain the fact that if λ is represented by Q, then $\langle\lambda\rangle$ splits in $\mathcal{O}_L$. Further, if $\langle\lambda\rangle$ splits as JJ' such that one of $(J; \underline{\text{sgn}}(\lambda))$ or $(J'; \underline{\text{sgn}}(\lambda))$ is in the class of I_Q, then λ is represented by Q.

We briefly note that Theorem 4.4 immediately implies a sufficient condition for Q to belong to the important class of totally positive definite binary quadratic forms as discussed in Section 3.4.

Lemma 4.6. *With the assumptions of Theorem 4.4 and D totally negative, if λ is totally positive and Q represents λ, then Q is totally positive definite.*

Proof. Suppose λ has $\underline{\text{sgn}}(\lambda) = (1, \ldots, 1) \in \langle \pm 1 \rangle^r$, then there exists some ideal J of $\mathcal{O}_L$ such that $(J; \underline{\text{sgn}}(\lambda)) \equiv I_Q$. Then, by [10, Lemma 4.1], it must be that a is totally positive. So Q is totally positive definite. □

The above results therefore generalize our discussion at the end of Section 1.5 to the case when the base field is taken to be a totally real number field with narrow class number 1. Further, the result above yields a sufficient condition for Q to be as in Proposition 3.36. In what follows we consider a relationship between the subgroups H analyzed in Chapter 3 and the representation problem in our usual setting.

4.2 Representability via Cosets

As discussed in the previous section, the correspondence between oriented ideal classes and classes of forms can be a useful tool in investigating representability (i.e. the representation problem). Based on the key role the subgroups H (see Equation 2.3) played in determining the corresponding oriented class groups, we seek relationships between these subgroups and representability. In particular, we discuss representability conditions which can be described via cosets of the subgroup H. The cosets in question are determined via the sign map, which we now describe.

Write $\mu_2 = \{\pm 1\}$ and define

$$\Upsilon : K^\times \to \mu_2^r$$

via

$$a \mapsto \underline{\text{sgn}}(a).$$

Lemma 4.7. *Let K be a totally real number field of narrow class number 1. The sign map, Υ, as defined above is a surjective group homomorphism with* $\ker(\Upsilon) = K^+$.

Proof. By the multiplicativity of $\underline{\text{sgn}}$ and the fact that $\underline{\text{sgn}}(1) = 1_{\mu_2^r}$, we have that Υ is a group homomorphism. Note that the elements sent to the identity element are exactly the totally positive

elements of the field K. Since K is assumed to have narrow class number 1, each sign configuration is obtained. □

Fix Q as in Theorem 4.4, and let $\lambda \in \mathcal{O}_K$ irreducible. For ease in computations, we will hereafter assume that λ is totally positive.

Consider the set $S_\lambda = \{u\lambda \mid u \in \mathcal{U}_K\}$ and the restriction of Υ to S_λ :

$$\Upsilon_\lambda : S_\lambda \to \mu_2^r. \tag{4.1}$$

Since K has units of independent signs, the map Υ_λ is surjective. However, it is highly non-injective. For any $\tau \in \mu_2^r$ there are infinitely many $v \in \mathcal{U}_K$ such that $v\lambda \mapsto \tau$, each obtained by adjusting $v\lambda$ by some totally positive unit of K. Said another way, the fiber over the identity element of μ_2^r, i.e. $\Upsilon_\lambda^{-1}(1_{\mu_2^r})$, is all of $\mathcal{U}_K^+$. Given some $v \in \mathcal{U}_K$ such that $v\lambda \in S_\lambda$ with $\Upsilon_\lambda(v\lambda) = \tau$, the fiber $\Upsilon_\lambda^{-1}(\tau) = v\lambda\mathcal{U}_K^+$. We would like to consider images under Υ_λ to characterize represented elements. As such, we consider the subset of elements of S_λ represented by Q :

$$R_\lambda = \{u\lambda \mid u \in \mathcal{U}_K \text{ and } u\lambda \text{ is represented by } Q\}.$$

Lemma 4.8. *Let K be a totally real number field of narrow class number 1, Q defined over K, and $\lambda \in \mathcal{O}_K$ irreducible and totally positive. Let Υ_λ be the restriction of the sign map as defined in (4.1). Then the set R_λ is the union of fibers of μ_2^r, that is*

$$R_\lambda = \Upsilon_\lambda^{-1}(\Upsilon_\lambda(R_\lambda)) \tag{4.2}$$

holds.

Proof. It is immediate that $R_\lambda \subseteq \Upsilon_\lambda^{-1}(\Upsilon_\lambda(R_\lambda))$. The other inclusion follows immediately from Lemma 4.3. □

A surprisingly beautiful fact about the sets R_λ is that their images under the associated maps Υ_λ correspond to cosets of the subgroups H as computed in the previous chapter. In particular, one can interpret the following result as a proof of two facts

1. All represented elements of S_λ land in the same coset of H.

2. All elements which land in the coset of a represented element are also represented.

We now give the result and its proof. We then express its usefulness in some special cases.

Theorem 4.9. *Let K be a totally real number field of narrow class number 1, Q be defined over K, and $\lambda \in \mathcal{O}_K$ irreducible and totally positive. Let Υ_λ be the restriction of the sign map as defined in (4.1). The set R_λ is either empty or its image, $\Upsilon_\lambda(R_\lambda) \subset \mu_2^r$, is a coset of H.*

Proof. If Q does not represent $u\lambda$ for any $u \in \mathcal{U}_K$ then R_λ is empty. Suppose $R_\lambda \neq \varnothing$, so there exists some $u \in \mathcal{U}_K$ such that Q represents $u\lambda$. By Theorem 4.4, there exists an ideal J of $\mathcal{O}_L$ such that $N_{L/K}(J) = \langle u\lambda \rangle$ as ideals of $\mathcal{O}_K$ and $(J; \underline{\text{sgn}}(u\lambda)) \sim I_Q$ in $Cl^o_{L/K}$. We wish to show $\Upsilon_\lambda(R_\lambda) = \underline{\text{sgn}}(u)H$.

Let $\alpha \in \Upsilon_\lambda(R_\lambda)$, then there exists some $v \in \mathcal{U}_K$ such that $v\lambda$ is represented by Q and

$$\alpha = \underline{\text{sgn}}(v)\underline{\text{sgn}}(\lambda) = \underline{\text{sgn}}(v).$$

By Theorem 4.4, there exists an ideal T of $\mathcal{O}_L$ such that $N_{L/K}(T) = \langle v\lambda \rangle$ in $\mathcal{O}_K$ and $(T; \underline{\text{sgn}}(v\lambda)) \sim I_Q$. So, we have

$$N_{L/K}(T) = \langle v\lambda \rangle = \langle \lambda \rangle = \langle u\lambda \rangle = N_{L/K}(J)$$

as ideals of $\mathcal{O}_K$ and

$$(T; \underline{\text{sgn}}(v\lambda)) \sim I_Q \sim (J; \underline{\text{sgn}}(u\lambda)).$$

Since λ is taken to be totally positive, we can simplify these equivalences to be

$$(T; \underline{\text{sgn}}(v)) \sim I_Q \sim (J; \underline{\text{sgn}}(u)),$$

which by [10, Lemma 2.18] implies there exists some $\gamma \in L^\times$ such that $\gamma J = T$ and $\underline{\text{sgn}}(\gamma\overline{\gamma}) = \underline{\text{sgn}}(N_{L/K}(\gamma)) = \underline{\text{sgn}}(v)\underline{\text{sgn}}(u)$. But, since

$$N_{L/K}(T) = N_{L/K}(\gamma J) = N_{L/K}(J),$$

$\gamma \in \mathcal{U}_L$. Thus, we have $\gamma \in \mathcal{U}_L$ with

$$\underline{\text{sgn}}(N_{L/K}(\gamma)) = \underline{\text{sgn}}(v)\underline{\text{sgn}}(u).$$

The left hand side is in H by definition, and since $\underline{\text{sgn}}(u)$ is its own inverse in μ_2^r, this implies $\underline{\text{sgn}}(v) = \alpha \in \underline{\text{sgn}}(u)H$.

To see the other inclusion, we take $h \in H$, so there exists some $v \in \mathcal{U}_L$ such that $h = \underline{\text{sgn}}(N_{L/K}(v))$. We wish to show $uN_{L/K}(v)\lambda$ is represented by Q. We first note that $N_{L/K}(J) = \langle u\lambda \rangle = \langle uN_{L/K}(v)\lambda \rangle$ as $N_{L/K}(v) \in \mathcal{U}_K$. Further, since $v \in \mathcal{U}_L$ with $vJ = J$ and $\underline{\text{sgn}}(N_{L/K}(v)) = \underline{\text{sgn}}(u^2\lambda^2 N_{L/K}(v))$, by [10, Lemma 2.18], we have

$$(J; \underline{\text{sgn}}(u\lambda)) \sim (J; \underline{\text{sgn}}(uN_{L/K}(v)\lambda)) \sim I_Q.$$

So, $uN_{L/K}(v)\lambda$ is represented by Q and of the form $u\lambda$ with $u \in \mathcal{U}_K$. Thus, $\underline{\text{sgn}}(uN_{L/K}(v)\lambda) = \underline{\text{sgn}}(u)h \in \Upsilon_\lambda(R_\lambda)$. So, $\Upsilon_\lambda(R_\lambda) = \underline{\text{sgn}}(u)H$. □

We end the section by highlighting three special cases of Theorem 4.9.

Corollary 4.10. *If $1_{\mu_2^r} \in \Upsilon_\lambda(R_\lambda)$ then Q represents λ. In this case $\Upsilon_\lambda(R_\lambda) = H$.*

Proof. Suppose $1_{\mu_2^r} \in \Upsilon_\lambda(R_\lambda)$ then there exists some $u \in \mathcal{U}_K^+$ such that $u\lambda$ is represented by Q. Then, by Theorem 4.4 there exists some ideal J of $\mathcal{O}_L$ such that $N(J) = \langle u\lambda \rangle = \langle \lambda \rangle$ and $(J; \underline{\text{sgn}}(u\lambda)) \equiv I_Q$. Since $(J; \underline{\text{sgn}}(u\lambda)) = (J; \underline{\text{sgn}}(\lambda))$, the result follows by Theorem 4.4. Note that in this case $\Upsilon_\lambda(R_\lambda) = \underline{\text{sgn}}(u)H = H$. □

The last two special cases arise when H is as small as possible, the trivial subgroup, and the second when H is as large as possible.

Corollary 4.11. *Assume H is the trivial subgroup of $\langle \pm 1 \rangle^r$. If Q represents an element $u\lambda \in S_\lambda$, then Q represents exactly those elements with sign configuration $\underline{sgn}(u)$.*

Proof. This follows immediately from Theorem 4.9 as each possible sign configuration yields a different coset of size 1. That is, either R_λ is empty or $|\Upsilon_\lambda(R_\lambda)| = 1$. □

Corollary 4.12. *If H is the whole group $\langle \pm 1 \rangle^r$, that is, if $Cl^o_{L/K} \cong Cl_L$, then Q either represents no elements of S_λ or Q represents them all.*

Proof. In this case we have R_λ is empty or $\Upsilon_\lambda(R_\lambda) = \mu_2^r$. □

This ends our discussion on the relationship between the subgroups H and representability of elements of the ring of integers of K. In the following chapter we outline ideas for future work, including directions for work concerning the representation problem for binary quadratic forms in our setting of interest.

Chapter 5

Future Directions

We end our discussion by outlining ongoing and future work related to the project. In particular, we discuss three future directions for our work. The first involves extending computations of the relative oriented class group to the case when the class number of L is taken to be even. Second, we discuss extending our work in Chapter 3 to more cases when $L/\mathbb{Q}$ is not Galois. Related to this goal, we note an example where such an extension can be made. Lastly, we discuss a third direction for future work regarding a cubic analogue to the motivation of our present investigation as it relates to [2].

The Group Extension Problem

As mentioned in Chapter 3, in the case when the class number of L is even, more work is needed to conclude the explicit structure of the relative oriented class group of L/K. Therefore, a natural future direction would be to consider the group extension problem

$$1 \to \mathcal{O}_L \times \langle \pm 1 \rangle^r / H \to Cl^o_{L/K} \to Cl_L \to 1$$

when Cl_L is known to have even order. Deducing conditions on when the sequence splits are of particular interest, since our method for computing H would immediately yield explicit descriptions of the relative oriented class group in these cases. In cases where the extension is known to not split, as in Example 3.19, determining the structure of the relative oriented class group via tools of homological algebra is another interesting path forward. In any case, we can sum up this future direction by asking the following question.

Question 5.1. When K is taken to be totally real with narrow class number 1 and L/K a quadratic extension with h_L even, what conditions are necessary for the short exact sequence

$$1 \to \mathcal{O}_L \times \langle \pm 1 \rangle^r / H \to Cl^o_{L/K} \to Cl_L \to 1$$

to split?

We mention that related to this direction is the question of classifying the relative oriented class group when the extension L/K is taken to be of higher degree. Indeed, Zemková remarks that the definition of the relative oriented class group could be defined for any finite Galois extension so long as we impose the narrow class number 1 condition on the base field (see [10, Remark 2.20]). With this in mind, we have hope for further developing the theory and computing examples of the relative oriented class group for higher degree extensions.

When L is not Galois

Our work done in Section 3.1 to deduce the subgroups H as the union of orbits is completed under the assumption that $L/\mathbb{Q}$ is a Galois extension. As such, we would like to deduce the general structure of the relative oriented class group for quadratic extensions L/K when $L/\mathbb{Q}$ is not Galois. We outline an example of future work along these lines.

We can consider the case is when K is a real quadratic number field and L/K is a degree two extension for which $L/\mathbb{Q}$ is not Galois. We note that in this case the Galois closure of L has D_4 as its Galois group.

In order to determine what such fields L look like, we consider D_4 extensions of $\mathbb{Q}$ and consider subfields of such extensions which have the following properties:

1. $[L : \mathbb{Q}] = 4$
2. L is not Galois over $\mathbb{Q}$
3. L has K as a quadratic subfield.

Determining generic D_4 extensions is a well-understood problem, with an explicit description of such extensions given in [37].

Theorem 5.2. *[37, Theorem 5] Let k be a field of characteristic not 2. Then D_4-extensions of k are of the form*

$$k(\sqrt{-1}, \sqrt{r}a^{1/4})/k$$

where $a, r \in k^\times$ *are such that* $-1, a$, *and* $a-1$ *are not squares in* k.

or

$$k(\sqrt{a}, \sqrt{a-1}, \sqrt{r(a+\sqrt{a})})/k$$

where $a, r \in k^\times$ *are such that* $a, a-1$, *and* $a(a-1)$ *are not squares in* k.

This is a fruitful direction of study, as systems of fundamental units for some classes of fields L which arise in this setting have been computed. For example, in the case that $L = \mathbb{Q}(\sqrt[4]{m})$ with $m \in \mathbb{Z}^+$ is a pure quartic extension with real quadratic subfield, a system of fundamental units for L is known (see [41], [42] and [43]).

Let $\varepsilon > 0$ denote the fundamental unit of K and $u > 1$ the smallest unit of L such that $u\overline{u} = 1$, where $\overline{u}$ is the conjugate of u with respect to K. Then, we obtain the following:

Lemma 5.3. *[41, Lemma 1] One of* $\{u, \varepsilon\}$ *or* $\{u, \sqrt{\varepsilon u}\}$ *forms a system of fundamental units of* L. *The former case occurs if and only if neither* ε *nor* $-\varepsilon$ *is the norm of a unit of* L *to* K.

From such descriptions, we can determine H by computing the relative norms of each element in the system. For example, we see that the former case yields a trivial subgroup H, and so the relative oriented class group is as large as possible in that case. Under certain conditions on the class number of L, we can explicitly compute the relative oriented class group of L/K.

We note that in the case when L is not a pure quartic extension, we do not know of explicit descriptions of systems of fundamental units. Continuing to investigate cases where L is not Galois in order to compute the associated relative oriented class group is ongoing work.

Given a number field K and relative quadratic extension L/K with all of the assumptions of Chapter 4, we related the representation problem for quadratic forms defined over the base field K to the subgroups H associated to L/K. As such, gaining understanding about the structure of $Cl^o_{L/K}$ in in the case when $L/\mathbb{Q}$ is not Galois may lead to interesting questions about representability. For example:

Question 5.4. How do varying the conditions on the quartic extension L, for instance requiring $L/\mathbb{Q}$ to be Galois, or not Galois but pure, change representability conditions?

We end by discussing another possible direction for generalizing the work completed in this thesis.

Cubic Analogues

The work done in this thesis is based off of a generalization of the bijection presented in Section 3.2 of [1]. We are interested in developing a similar generalization, but for some of the "cubic analogies" given by Bhargava in [2]. In this setting we instead consider binary *cubic* forms, by which we mean homogeneous degree 3 polynomials in two variables:

$$Q(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

There is already a familiar looking bijection between equivalence classes of binary cubic forms and classes in rings. By work of Zagier, Delone and Faddeev [44] and Gan-Gross-Savin [45], we have

Theorem 5.5. *There is a canonical bijection between the set of $GL_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings which is discriminant preserving.*

The main object of study in [1] are $2 \times 2 \times 2$ cubes of integers with an action of $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ with the unique SL_2-invariant being the discriminant. In [2], Bhargava instead considers $2 \times 3 \times 3$ boxes with an associated action by $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$. Here, he shows that the unique $SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$ invariant is now the cubic form f which classifies orders in cubic fields. The classes of boxes with a fixed value of f form a group under a composition law which Bhargava defines. This group is then isomorphic to the ideal class group of the corresponding cubic order.

Our hope is to determine a generalization of this work from [2], defined over the rings of integers of number fields K. We will begin our investigation with K a quadratic number field. De-

termining the proper conditions on K to make such a generalization possible will be a preliminary step in this process.

Chapter 6

The Principal Chebotarev Density Theorem[1]

In this chapter, we provide many of the details regarding a second project which is currently in submission and joint work with Lian Duan, Ning Ma and Xiyuan Wang. For details not included in this chapter, we refer the reader to the full article, Nonsplitting of the Hilbert exact sequence and the principal Chebotarev density theorem, [11]. In what follows, we consider a principal version of the Chebotarev density theorem and its dependence on the splitting of a particular short exact sequence related to a given field extension.

6.1 Background and Problem Set-up

Let K/k be a finite Galois extension of number fields, with Galois group $G = \text{Gal}(K/k)$. Denote by $\mathcal{P}_K$ the set of prime ideals of the ring of integers $\mathcal{O}_K$. For a prime ideal $\mathfrak{P} \in \mathcal{P}_K$ we denote by $N_{K/k}\mathfrak{P}$ the relative norm and omit the subscript in the case that $k = \mathbb{Q}$.

Definition 6.1. For $\mathfrak{p} \in \mathcal{P}_k$, and $\mathfrak{P} \in \mathcal{P}_K$ unramified over $\mathfrak{p}$, the Artin symbol $\left(\frac{K/k}{\mathfrak{P}}\right)$ is the unique $\sigma \in G$ such that for all $x \in K$, we have

$$\sigma(x) \equiv x^{N\mathfrak{p}} \mod \mathfrak{P}.$$

The values of $\left(\frac{K/k}{\mathfrak{P}}\right)$ for all $\mathfrak{P}$ lying over $\mathfrak{p}$ are all conjugate. We denote by $\left(\frac{K/k}{\mathfrak{p}}\right)$ the conjugacy class of $\left(\frac{K/k}{\mathfrak{P}}\right)$ for all $\mathfrak{P}$ lying above $\mathfrak{p}$ and call $\left(\frac{K/k}{\mathfrak{p}}\right)$ the *Frobenius class associated to* $\mathfrak{p}$.

For a given conjugacy class C of G and $\mathfrak{p} \in \mathcal{P}_k$ unramified in K. Let

$$\mathcal{P}_{k,C} := \left\{ \mathfrak{p} \in \mathcal{P}_k \mid \left(\frac{K/k}{\mathfrak{p}}\right) = C \right\},$$

[1]This project is joint work with Lian Duan, Ning Ma and Xiyuan Wang. The manuscript is currently in submission and available as arXiv:2109.01217.

then the *natural density* of $\mathcal{P}_{k,C}$ is given by

$$\mu_{K/k}(C) := \lim_{N\to\infty} \frac{\#\left\{\mathfrak{p} \mid N\mathfrak{p} \leqslant N, \left(\frac{K/k}{\mathfrak{p}}\right) = C\right\}}{\#\left\{\mathfrak{p} \mid N\mathfrak{p} \leqslant N\right\}}.$$

The Chebotarev density theorem describes this natural density purely in terms of the size of the Galois group of K/k and the size of the conjugacy class C.

Theorem 6.2 (The Chebotarev density theorem)**.** *Let K/k be a finite Galois extension of number fields with $G = Gal(K/k)$ and C a conjugacy class of G. Then*

$$\mu_{K/k}(C) = \frac{|C|}{|G|}.$$

The Chebotarev density theorem is of great importance in the field of algebraic number theory, for instance as a means to generalize Dirichlet's theorem on primes in arithmetic progressions. We refer the interested reader to [46] for more information about the life and legacy of Chebotarev and his theorem.

We now introduce one of the main objects of our discussion, namely the *Hilbert exact sequence*.

Definition 6.3. Let K/k be a finite Galois extension of number fields. The *Hilbert class field of* K is the maximal abelian unramified extension of K, denoted H_K.

The field H_K is Galois over k, and there is a natural restriction map

$$\pi : \text{Gal}(H_K/k) \to \text{Gal}(K/k)$$

$$\tau \mapsto \tau|_K.$$

We note that $\ker(\pi) \cong \text{Gal}(H_K/K)$, which is isomorphic to Cl_K. From this, we obtain the Hilbert short exact sequence (HES):

$$1 \to Cl_K \to \text{Gal}(H_K/k) \xrightarrow{\pi} \text{Gal}(K/k) \to 1. \tag{6.1}$$

To ease notation, we will hereafter set $G = \text{Gal}(K/k)$ and $E = \text{Gal}(H_K/k)$.

At one time it was believed that the HES always splits when the base field is taken to be $\mathbb{Q}$. However, in 1973 Wyman proved this belief to be false [47]. In particular, Wyman proved the HES does split when k has class number 1 and K/k is cyclic. In 1977, Gold found another proof of Wyman's result [48] which was later improved by Cornell and Rosen in 1988 [49]. Cornell and Rosen proved a necessary condition for the splitting of the HES that in the case of K/k abelian of odd degree is equivalent to whether or not the Hasse norm theorem holds for K. We are thus motivated by the question of whether or not the HES splits.

6.2 The Principal Density

We begin by defining a version of the natural density which represents the density of primes $\mathfrak{p}$ of k which realize the desired conjugacy class C and factor principally in K:

$$\mu^1_{K/k}(C) := \lim_{N\to\infty} \frac{\#\left\{\mathfrak{p} \in \mathcal{P}_k \mid N\mathfrak{p} \leqslant N,\ \left(\frac{K/k}{\mathfrak{p}}\right) = C, \mathfrak{P} \text{ is principal}\right\}}{\#\{\mathfrak{p} \in \mathcal{P}_k \mid N\mathfrak{p} \leqslant N\}}$$

for every prime ideal $\mathfrak{P}$ of K lying above $\mathfrak{p}$. We make the following related definition:

Definition 6.4. Let K/k be a finite Galois extension of number fields. We say a prime $\mathfrak{p}$ of k *principally realizes* a conjugacy class $C \subset \text{Gal}(K/k)$ (or C is *principally realized* by $\mathfrak{p}$) if $\mathfrak{p}$ satisfies the following

- $\mathfrak{p}$ is unramified in K,
- $\mathfrak{p}$ is a product of principal prime ideals in $\mathcal{O}_K$, and
- $\left(\frac{K/k}{\mathfrak{p}}\right) = C$.

One can see the relationship between this principal density and the natural density of Chebotarev's theorem. Indeed, some of the important examples considered in this summary will involve

only this principal density, however, in our project, we considered a generalized version of the principal density, in which the natural questions of well-definedness and positivity can be answered. As such, we present these generalized densities now.

A Generalized Version

Let $\mathfrak{p}$ be an unramified prime in k lying below a prime $\mathfrak{P}$ in K. We can then define the K/k-principal order of $\mathfrak{p}$ to be the smallest positive integer $n_{K/k,\mathfrak{p}}$ such that $\mathfrak{P}^{n_{K/k,\mathfrak{p}}}$ is principal in K. Therefore, we can define the following densities for each $m \in \mathbb{Z}_{>0}$.

$$\mu^m_{K/k}(C) := \lim_{N\to\infty} \frac{\#\left\{\mathfrak{p} \in \mathcal{P}_k \mid N\mathfrak{p} \leqslant N,\ \left(\frac{K/k}{\mathfrak{p}}\right) = C, n_{K/k,\mathfrak{p}} | m\right\}}{\#\{\mathfrak{p} \in \mathcal{P}_k \mid N\mathfrak{p} \leqslant N\}}.$$

Remark 6.5. A set of closely related densities are given by

$$\theta^m_{K/k}(C) := \lim_{N\to\infty} \frac{\#\left\{\mathfrak{p} \in \mathcal{P}_k \mid N\mathfrak{p} \leqslant N,\ \left(\frac{K/k}{\mathfrak{p}}\right) = C, n_{K/k,\mathfrak{p}} = m\right\}}{\#\{\mathfrak{p} \in \mathcal{P}_k \mid N\mathfrak{p} \leqslant N\}}$$

and many of the results discussed below can be rephrased for these densities.

6.3 Main Results

Natural questions arise after making the definition of such densities. As such, we include the main results of our work, addressing questions of well-definedness, conditions for when $\mu^m_{K/k}(C)$ is positive, and determining an explicit formula in the style of the classical Chebotarev density theorem. Along the way we highlight connections to the splitting of the associated Hilbert exact sequence and highlight special cases which are of interest.

Proposition 6.6. *For every conjugacy class C of G, and every positive integer m, the density $\mu^m_{K/k}(C)$ is well defined and*

$$\mu^m_{K/k}(C) = \frac{|\{\sigma \in E | \pi(\sigma) \in C \text{ and } \sigma^{d_G(C)m} = id_E\}|}{|E|} \tag{6.2}$$

where $d_G(C)$ denotes the common order of elements of C.

Proof. Note that $\mathfrak{P}$ is of principal order n if and only if $d_{Cl_K}\left(\frac{H_K/K}{\mathfrak{P}}\right) = n$, or equivalently, if and only if $d_E\left(\frac{H_K/k}{\mathfrak{p}}\right) = d_G\left(\frac{K/k}{\mathfrak{p}}\right) n$. We have

$$\begin{aligned}
\mu^m_{K/k}(C) &= \lim_{N\to\infty} \sum_{n|m} \frac{\#\left\{\mathfrak{p} \in \mathcal{P}_k \middle| N\mathfrak{p} \leqslant N, \left(\frac{K/k}{\mathfrak{p}}\right) = C, d_E\left(\frac{H/k}{\mathfrak{p}}\right) = d_G(C)n\right\}}{\#\{\mathfrak{p} \in \mathcal{P}_k | N\mathfrak{p} \leqslant N\}} \\
&= \sum_{n|m} \sum_{\substack{\pi(C')=C \\ d_E(C')=d_G(\pi(C'))n}} \lim_{N\to\infty} \frac{\#\left\{\mathfrak{p} \in \mathcal{P}_k \middle| N\mathfrak{p} \leqslant N, \left(\frac{H_K/k}{\mathfrak{p}}\right) = C'\right\}}{\#\{\mathfrak{p} \in \mathcal{P}_k | Nm\mathbb{Q}(\mathfrak{p}) \leqslant N\}} \\
&= \sum_{n|m} \sum_{\substack{\pi(C')=C \\ d_E(C')=d_G(\pi(C'))n}} \frac{|C'|}{|E|} \\
&= \frac{|\{\sigma \in E | \pi(\sigma) \in C \text{ and } \sigma^{d_G(C)m} = \mathrm{id}_E\}|}{|E|}.
\end{aligned}$$

Where C' is a conjugacy class of E. □

From this result we see that $\mu^m_{K/k}(C)$ depends on the union of conjugacy classes of $\mathrm{Gal}(H_K/k)$. In particular, the density is determined by $\{\sigma \in E | \pi(\sigma) \in C \text{ and } \sigma^{d_G(C)m} = \mathrm{id}_E\}$ which we hereafter denote by C_m. Consider the following important lemma.

Lemma 6.7. *Let h_K be the class number of K and C be a conjugacy class of G.*

1. *We have $\mu^{h_K}_{K/k}(C) = \mu_{K/k}(C)$.*
2. *If $m_1 \mid m_2$, then $\mu^{m_1}_{K/k}(C) \leqslant \mu^{m_2}_{K/k}(C)$.*
3. *For every $m > 0$, let $m_0 = \gcd(m, h_K)$. Then $\mu^m_{K/k}(C) = \mu^{m_0}_{K/k}(C) \leqslant \mu^{h_K}_{K/k}(C)$.*

Thus, we are only interested in $\mu^m_{K/k}$ where m divides the class number of K.

Conditions for $\mu^m_{K/k}(C) > 0$

We now consider the second question stated above, that is when the density $\mu^m_{K/k}(C)$ is positive. Before stating the result, we introduce the notion of a subexact sequence. For any element $g \in G$, we can construct the associated subexact sequence of the HES,

$$1 \to Cl_K \to E_g \to \langle g \rangle \to 1,$$

where $E_g = \pi^{-1}(\langle g \rangle) \subset E$. Further, let $Cl^0_K[n]$ be the subgroup of Cl_K generated by the elements of order exactly n. This group $Cl^0_K[n]$ may not exist. If it exists, there is a short exact sequence

$$1 \to Cl_K/Cl^0_K[n] \to E_g/Cl^0_K[n] \to \langle g \rangle \to 1. \tag{6.3}$$

Theorem 6.8. *Fix a conjugacy class C of G, the density $\mu^m_{K/k}(C) > 0$ if and only if there exists a positive divisor i of m such that the short exact sequence*

$$1 \to Cl_K/Cl^0_K[i] \to E_g/Cl^0_K[i] \to \langle g \rangle \to 1 \tag{6.4}$$

exists and splits for some $g \in C$.

As a consequence, $\mu^m_{K/k}(C) > 0$ for all conjugacy classes if and only if for every maximal cyclic subgroup U of G, there exists a divisor i_U of m such that the short exact sequence

$$1 \to Cl_K/Cl^0_K[i_U] \to \pi^{-1}(U)/Cl^0_K[i_U] \to U \to 1 \tag{6.5}$$

exists and splits.

Proof. Assume that $\mu^m_{K/k}(C) > 0$. Then there is an element σ such that $\pi(\sigma) \in C$ and $d_E(\sigma) = d_G(C)i$ for a positive divisor i of m. So the group $Cl^0_K[i]$ exists and $\pi(\sigma) \mapsto \sigma Cl^0_K[i]$ defines a splitting of the short exact sequence

$$1 \to Cl_K/Cl^0_K[n] \to E_g/Cl^0_K[n] \to \langle \pi(\sigma) \rangle \to 1.$$

For the other direction, assume that there is a split short exact sequence

$$1 \to Cl_K/Cl_K^0[i] \to E_g/Cl_K^0[i] \to \langle g \rangle \to 1$$

for some $g \in C$ and some divisor i of m. Let $\sigma Cl_K^0[i]$ be the image of g under the splitting map. Then $\sigma Cl_K^0[i]$ and g have the same order. We have $\frac{d_E(\sigma)}{d_G(C)} \mid m$. So σ is an element in C_m and $\mu_{K/k}^m(C) > 0$.

To see the second part, suppose that $\mu_{K/k}^m(C) > 0$ for every C. Let U be a maximal cyclic group with a generator g. Let C_0 be the conjugacy class containing g. Since $\mu_{K/k}^m(C_0) > 0$, using the above arguments one can find an element $g_0 \in C_0$ such that the associated short exact sequence

$$1 \to Cl_K/Cl_K^0[i] \to E_{g_0}/Cl_K^0[i] \to \langle g_0 \rangle \to 1$$

splits. Since g_0 and g are in the same conjugacy class C_0, there exists an element $h \in G$ such that $g = h^{-1}g_0h$. Take $\tau \in \pi^{-1}(h)$ to be an arbitrary lift of h in E, it is not hard to check that (6.5) can be recovered by conjugating

$$1 \to Cl_K/Cl_K^0[i] \to E_{g_0}/Cl_K^0[i] \to \langle g_0 \rangle \to 1$$

by τ. This proves the splitting of (6.5). Conversely, assume that (6.5) splits for all maximal cyclic subgroups U of G. One can deduce the splitting of (6.5) for every (not necessarily maximal) cyclic group U. Then for each conjugacy class C, take U to be any cyclic subgroup of G which intersects C nontrivially, and take $g \in U \cap C$. Then the splitting of

$$1 \to Cl_K/Cl_K^0[i_U] \to E_g/Cl_K^0[i_U] \to \langle g \rangle \to 1$$

is deduced from the splitting of (6.5). So $C_m \neq \varnothing$, hence the proof is complete. □

The following result follows from the arguments above, and provides our first connection between the notions of the principal densities and the splitting of the Hilbert exact sequence.

Proposition 6.9. *If the Hilbert exact sequence*

$$1 \to Cl_K \to E \xrightarrow{\pi} G \to 1$$

splits, then $\mu^1_{K/k}(C) > 0$ *for every conjugacy class* C.

Proof. Note that if the Hilbert exact sequence splits, then for every subgroup $H \subset G$, the corresponding subsequence

$$1 \to Cl_K \to \pi^{-1}(H) \to H \to 1$$

also splits. In particular, let H run over all maximal cyclic subgroups U of G, then this corollary follows as an immediate consequence of Theorem 6.8. □

Explicit Formulas

As indicated above, one of our goals was to determine an explicit formula for the principal densities in the style of the classical Chebotarev density theorem.

Fix an element $\sigma \in E$ such that $\pi(\sigma) \in C$ and σ has order dividing $d_G(C)m$. Hence σ is an element in the set C_m. Consider the following group homomorphism (one can check it is well defined),

$$\begin{aligned} \mathrm{N}_{\sigma,m} : Cl_K &\to Cl_K \\ x &\mapsto (x\sigma)^{d_G(C)m} \\ &= x\sigma \cdot x\sigma \cdots x\sigma \quad (d_G(C)m \text{ copies}) \\ &= x \cdot \sigma x \sigma^{-1} \cdot \sigma^2 x \sigma^{-2} \cdots \sigma^{d_G(C)m-1} x \sigma^{-(d_G(C)m-1)}. \end{aligned} \tag{6.6}$$

Then $\ker(\mathrm{N}_{\sigma,m}) = \{x \in Cl_K | (x\sigma)^{d_G(C)m} = \mathrm{id}_E\}$ and $\ker(\mathrm{N}_{\sigma,m}) \cdot \sigma = \{\tau \in E | \tau \in C_m \text{ and } \pi(\tau) = \pi(\sigma)\}$.

Proposition 6.10. *Assume that $\mu^m_{K/k}(C) > 0$. For any element $\sigma \in \pi^{-1}(C)$, we have*

$$\mu^m_{K/k}(C) = \frac{|C|}{|G|} \frac{|\ker(\mathrm{N}_{\sigma,m})|}{h_K}.$$

Proof. Note that $\ker(\mathrm{N}_{\sigma,m}) = \tau \ker(\mathrm{N}_{\tau\sigma\tau^{-1},m})\tau^{-1}$ for any element $\tau \in E$. We have $|\ker(\mathrm{N}_{\sigma,m})| = |\ker(\mathrm{N}_{\tau\sigma\tau^{-1},m})|$. Moreover, if $\pi(\sigma) \neq \pi(\tau\sigma\tau^{-1})$ then $\ker(\mathrm{N}_{\sigma,m})\sigma$ and $\ker(\mathrm{N}_{\tau\sigma\tau^{-1},m})(\tau\sigma\tau^{-1})$ are disjoint. By this observation and the set C_m, if for every $g \in C \subset G$, we choose a lift $\sigma_g \in \pi^{-1}(g)$ such that σ_g is conjugate with the given σ in E, then

$$C_m = \bigsqcup_{g \in C} \ker(\mathrm{N}_{\sigma_g,m})\sigma_g.$$

So $|C_m| = |C||\ker(\mathrm{N}_{\sigma,m})|$ for $\sigma \in \pi^{-1}(C)$. Combining this with (6.2) proves the result. □

Let $g = \pi(\sigma) \in G$, then $\langle g \rangle$ acts on K. We denote by $F = K^{\langle g \rangle}$ the fixed field of K by $\langle g \rangle$, then by genus theory [50], there exists an intermediate field $H_K \supset K_F \supset K$ which is maximal among all such possible intermediate fields whose Galois group over F is abelian. This K_F is called the *genus field of K over F* . We call the degree $[K_F : K]$ the *genus number* of K over F. Now we are equipped to state the following result.

Theorem 6.11. *For every conjugacy class C of G such that $\mu^1_{K/k}(C) > 0$, let $\sigma \in \pi^{-1}(g) \subset E_g$ be an element that has order $d_G(C)$ for some $g \in C$, take F to be the subfield of K fixed by g and take K_F to be the genus field of K over F, then*

$$\frac{|\ker(\mathrm{N}_{\sigma,1})|}{h_K} = \frac{|H^1(\langle g \rangle, Cl_K)|}{[K_F : K]}.$$

As a consequence, we have

$$\mu^1_{K/k}(C) = \frac{|C|}{|G|} \frac{|H^1(\langle g \rangle, Cl_K)|}{[K_F : K]}.$$

Proof. First the element σ exists by Theorem 6.8. Note that E_g acts on Cl_K naturally by conjugation, and this action factors through $\langle \sigma \rangle \simeq \langle g \rangle$. By the theory of the Tate cohomology/homology

[51, Chapter 8, Section 1, Section 4], it follows that

$$H^1(\langle g\rangle, Cl_K) \simeq H^1(\langle\sigma\rangle, Cl_K) = \hat{H}^1(\langle\sigma\rangle, Cl_K) = \hat{H}_0(\langle\sigma\rangle, Cl_K) = \frac{\ker(\mathrm{N}_{\sigma,1})}{D(Cl_K)}, \tag{6.7}$$

where $D(Cl_K)$ is the subgroup of $\ker(\mathrm{N}_{\sigma,1})$ generated by $xsx^{-1}s^{-1}$ as x and s run over Cl_K and $\langle\sigma\rangle$ respectively. Easy calculation shows that $D(Cl_K)$ is the commutator subgroup $[E_g, E_g]$ of E_g. Hence using Galois theory, one sees that $D(Cl_K)$ corresponds to the genus field K_F. Hence

$$[K_F : K] \cdot d_G(C) = |\mathrm{Gal}(K_F/F)| = |E_g|/|D(Cl_K)|.$$

Applying (6.7), we get

$$|H^1(\langle g\rangle, Cl_K)| = \frac{|\ker(\mathrm{N}_{g,1})|}{|D(Cl_K)|} = \frac{|\ker(\mathrm{N}_{\sigma,1})|[K_F : K]d_G(C)}{|E_g|}.$$

Since $|E_g| = h_K d_G(C)$, we thus get

$$|H^1(\langle g\rangle, Cl_K)| = \frac{|\ker(\mathrm{N}_{\sigma,1})|[K_F : K]}{h_K} = [K_F : K]\frac{|\ker(\mathrm{N}_{\sigma,1})|}{h_K}.$$

Then the last equation follows immediately from Proposition 6.10. □

Special Cases

Consider Theorem 6.11 in the case when we take $C = \{\mathrm{id}_G\}$. Here,

$$H^1(\langle \mathrm{id}_G\rangle, Cl_K) = \mathrm{Hom}(\mathrm{id}_G, Cl_K)$$

which is trivial and $F = K^{\mathrm{id}_G} = K$ and so $K_F = H_K$. We summarize this case in the following result:

Corollary 6.12. *Let K/k be a Galois extension with Gal$(K/k) = G$. Then, the probability of finding a prime ideal of k which splits principally in K is $\frac{1}{|G|h_K}$.*

A general version of Theorem 6.11 for all $m > 1$ holds with slight modifications (see [11, Corollary 3.4.1]). We again highlight the special case when C is taken to be $\{\mathrm{id}_G\}$ in the more general result.

Corollary 6.13. *Take $C = \{id_G\}$ to be the trivial conjugacy class in G, for every prime integer p and every positive integer r, we have*

$$\frac{\mu_{K/k}^{p^r}(\{id_G\})}{\mu_{K/k}^{p^{r-1}}(\{id_G\})} = \frac{|Cl_K[p^r]|}{|Cl_K[p^{r-1}]|}$$

where $Cl_K[m] = \{x \in Cl_K \mid x^m = id\}$.

That is, we see that by computing generalized principal densities, we can deduce the group structure of Cl_K.

An effective version

In our project, we also investigated an effective version of the principal density. Effective versions of the Chebotarev density theorem have been studied by various people, for instance [52]. In our next result, we utilize the effective version of Bach and Sorenson in [53]. We note that the following effective bound is actually dependent on conjugacy classes of the Galois group of the extension H_K/k.

Theorem 6.14. *Fix a Galois extension K/k. There is an effective bound B_K, such that if any conjugacy class C of Gal(K/k) cannot be principally realized by at least one prime $\mathfrak{p}$ of k with $N_{k/\mathbb{Q}}(\mathfrak{p}) \leqslant B_K$, then the HES does not split.*

In particular, under the assumption of GRH, one can take

$$B_K = (4h_K \log|\Delta_K| + 2.5 \cdot [K : \mathbb{Q}] \cdot h_K + 5)^2,$$

where $|\Delta_K|$ is the absolute discriminant of K and h_K is the class number of K.

Proof. It is sufficient to find a bound to realize every conjugacy class of $\mathrm{Gal}(H_K/k)$. By [53, Theorem 3.1, 3.2, 5.1, and Corollary 3.3] we are left only to bound the absolute degree and the absolute discriminant of H_K. In fact, $[H_K : \mathbb{Q}] = h_K \cdot [K : \mathbb{Q}]$. Hence the only nontrivial part of this proof is to give an estimation of $|\Delta_{H_K/\mathbb{Q}}|$.

For this purpose, we recall [12, Chapter 3 Section 2] that there is a fractional ideal $\mathfrak{D}_{H_K/K}$ of $\mathcal{O}_{H_K}$ such that a prime ideal $\widetilde{\mathfrak{P}}$ of $\mathcal{O}_{H_K}$ is ramified over K if and only if $\widetilde{\mathfrak{P}}|\mathfrak{D}_{H_K/K}$ [12, Chapter 3, Theorem 2.6]. Moreover, we have that [12, Chapter 3, Theorem 2.9] the discriminant $\Delta_{H_K/\mathbb{Q}}$ is the norm of the different $\mathfrak{D}_{H_K/\mathbb{Q}}$, i.e.,

$$\Delta_{H_K/\mathbb{Q}} = N\mathfrak{D}_{H_K/\mathbb{Q}}$$

and [12, Chapter 3, Proposition 2.2]

$$\mathfrak{D}_{H_K/\mathbb{Q}} = \mathfrak{D}_{H_K/K}\mathfrak{D}_{K/\mathbb{Q}}.$$

Note that since H_K is unramified over K, we know that $\mathfrak{D}_{H_K/K} = (1)$ is the trivial ideal of $\mathcal{O}_{H_K}$. Thus $\mathfrak{D}_{H_K/\mathbb{Q}} = \mathfrak{D}_{K/\mathbb{Q}}$ (considered as an ideal of $\mathcal{O}_{H_K}$). Hence we know that in this case,

$$\Delta_{H_K} = N\mathfrak{D}_{H_K/\mathbb{Q}} = N\mathfrak{D}_{K/\mathbb{Q}}\mathcal{O}_{H_K} = (N\mathfrak{D}_{K/\mathbb{Q}})^{h_K} = \Delta_K^{h_K}.$$

Applying the theorem of Bach and Sorenson with $L = H_K$, we get an effective bound to cover all the conjugacy classes of $\mathrm{Gal}(H_K/k)$. That is

$$B_K = (4h_K \log|\Delta_K| + n \cdot h_K + 5)^2.$$

Now we take

$$S = \{\mathfrak{p} \mid N\mathfrak{p} \leqslant B_K \text{ and } \mathfrak{p} \text{ factors principally in } K\}.$$

Then by the same arguments as in the proof of Proposition 6.6, one can easily check that the Frobenius classes of prime ideals in S realize every conjugacy class $C \subset \text{Gal}(K/k)$ as long as $\mu^1_{K/k}(C) > 0$. This completes the proof. $\square$

Before moving on to the final example of this chapter, we make two important remarks. The first is to note that even without the assumption of GRH, an effective bound B_K exists. Further, in cases when the class number of K is difficult to compute, one can use [54, Theorem 6.5]:

$$h_K \leqslant \frac{d(n-1+\log d)^{n-1}}{(n-1)!}, \tag{6.8}$$

where $d = (2/\pi)^s\sqrt{|\Delta_K|}$ and s the number of complex embeddings of K.

We end this chapter by considering an example where the bound computed above is utilized to verify the non-splitting of a particular Hilbert exact sequence.

Verification of non-splitting

Recall, one of the motivations of our project was to give an algorithm for verifying the nonsplitting of the Hilbert exact sequence for certain K/k. With the above result, we have accomplished our goal. To demonstrate this, we include Example 4.2 of [11]

Example 6.15. [11, Example 4.2] Consider the biquadratic field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$ which has $h_K = 2$ and $|\Delta_K| = 1521$. One of the three quadratic subfields of K is $L = \mathbb{Q}(\sqrt{-3 \times 13})$. Denote by σ the generator of $\text{Gal}(K/L)$ and consider the conjugacy class $C = \{\sigma\}$. The sub-exact sequence

$$1 \to Cl_K \to E_\sigma \to \langle\sigma\rangle \to 1$$

splits if and only if one can find a prime integer p which is

- unramified in K,

- totally split in L,
- not totally split in K, and
- factors principally in K.

By Theorem 6.14, if such a p exists, it can be found under

$$B_K = (4 \times 2 \times \log|1521| + 2.5 \times 4 \times 2 + 5)^2 < 6992.$$

One can use a computer to verify that no such prime exists, so $\mu^1_{K/\mathbb{Q}}(\sigma) = 0$ and the associated Hilbert exact sequence does not split.

Bibliography

[1] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.

[2] Manjul Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2):865–886, 2004.

[3] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

[4] Melanie Matchett Wood. Gauss composition over an arbitrary base. *Adv. Math.*, 226(2):1756–1771, 2011.

[5] Michael William Mastropietro. *Quadratic forms and relative quadratic extensions*. ProQuest LLC, Ann Arbor, MI, 2000. Thesis (Ph.D.)–University of California, San Diego.

[6] Kristỳna Zemková. Composition of quadratic forms over number fields. 2018.

[7] Larry J. Gerstein. *Basic quadratic forms*, volume 90 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[8] David A. Cox. *Primes of the form* $x^2 + ny^2$. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[9] Kristýna Zemková. Composition of bhargava's cubes over number fields. *Expositiones Mathematicae*, 41(4):125515, 2023.

[10] Kristỳna Zemková. Composition of binary quadratic forms over number fields. *arXiv preprint Version 3 arXiv:1712.00741*, 2023.

[11] Lian Duan, Kelly Emmrich, Ning Ma, and Xiyuan Wang. Nonsplitting of the Hilbert exact sequence and the principal Chebotarev density theorem. *arXiv preprint arXiv:2109.01217*, 2021.

[12] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[13] P. E. Conner and J. Hurrelbrink. *Class number parity*, volume 8 of *Series in Pure Mathematics*. World Scientific Publishing Co., Singapore, 1988.

[14] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[15] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online].

[16] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. `https://www.sagemath.org`.

[17] François Séguin. Composition of binary quadratic forms: Understanding the approaches of Gauss, Dirichlet and Bhargava. *Resonance: Journal of Science Education*, 24(6), 2019.

[18] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[19] A. I. Borevich and I. R. Shafarevich. *Number theory*, volume Vol. 20 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1966. Translated from the Russian by Newcomb Greenleaf.

[20] Maria Elena Salcedo Stadnik. *Ray Class Fields of Conductor p*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–Northwestern University.

[21] Wanlin Li, Elena Mantovan, and Rachel Pries. Data for Shimura varieties intersecting the Torelli locus. *arXiv preprint arXiv:2105.02286*, 2021.

[22] Władysł aw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Monografie Matematyczne, Tom 57. PWN—Polish Scientific Publishers, Warsaw, 1974.

[23] James S Milne. *Algebraic number theory*. JS Milne, 2008.

[24] H. M. Edgar, R. A. Mollin, and B. L. Peterson. Class groups, totally positive units, and squares. *Proc. Amer. Math. Soc.*, 98(1):33–37, 1986.

[25] Henry B. Mann. On integral bases. *Proc. Amer. Math. Soc.*, 9:167–172, 1958.

[26] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[27] Charles A. Weibel. History of homological algebra. In *History of topology*, pages 797–836. North-Holland, Amsterdam, 1999.

[28] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[29] Hans J. Zassenhaus. *The theory of groups*. Chelsea Publishing Co., New York, 1958. 2nd ed.

[30] Michal Bulant. On the parity of the class number of the field $\mathbf{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$. *J. Number Theory*, 68(1):72–86, 1998.

[31] Michal Bulant. Class number parity of a compositum of five quadratic fields. *Acta Math. Inform. Univ. Ostraviensis*, 10(1):25–34, 2002.

[32] Peter Stevenhagen. Class number parity for the pth cyclotomic field. *Math. Comp.*, 63(208):773–784, 1994.

[33] Ken-Ichi Yoshino. Class number parity for cyclotomic fields. *Proc. Amer. Math. Soc.*, 126(9):2589–2591, 1998.

[34] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[35] Tomio Kubota. Über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, 10:65–85, 1956.

[36] Sigekatu Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, 1:1–10, 1950.

[37] Ian Kiming. Explicit classifications of some 2-extensions of a field of characteristic different from 2. *Canad. J. Math.*, 42(5):825–855, 1990.

[38] Takeo Funakura. On integral bases of pure quartic fields. *Math. J. Okayama Univ.*, 26:27–41, 1984.

[39] Kenneth S. Williams. Integers of biquadratic fields. *Canad. Math. Bull.*, 13:519–526, 1970.

[40] Robert H. Bird and Charles J. Parry. Integral bases for bicyclic biquadratic fields over quadratic subfields. *Pacific J. Math.*, 66(1):29–36, 1976.

[41] Akira Endô. On units of pure quartic number fields. *Pacific J. Math.*, 109(2):327–333, 1983.

[42] M. Ljunggren. Uber die Losung einiger unbestimmten Gleichung vierten Grades. *Avh. Norske Vid.-Akad. Oslo*, 1(14):1–35, 1934.

[43] M. Ljunggren. Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahlkorper mit Anwendung au. *Skr. Norske Vid.-Akad,Oslo*, 1(12):1–73, 1936.

[44] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree*. Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[45] Wee Teck Gan, Benedict Gross, and Gordan Savin. Fourier coefficients of modular forms on G_2. *Duke Math. J.*, 115(1):105–169, 2002.

[46] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[47] Bostwick F. Wyman. Hilbert class fields and group extensions. *Scripta Math.*, 29:141–149, 1973.

[48] Robert Gold. Hilbert class fields and split extensions. *Illinois J. Math.*, 21(1):66–69, 1977.

[49] Gary Cornell and Michael Rosen. A note on the splitting of the Hilbert class field. *J. Number Theory*, 28(2):152–158, 1988.

[50] Yoshiomi Furuta. The genus field and genus number in algebraic number fields. *Nagoya Math. J.*, 29:281–285, 1967.

[51] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[52] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[53] Eric Bach and Jonathan Sorenson. Explicit bounds for primes in residue classes. *Math. Comp.*, 65(216):1717–1735, 1996.

[54] H. W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992.