University of Groningen

Bachelor's Project Mathematics

On the divisibility of class numbers of quadratic number fields

Author:
Prakhar Agarwal
(s5171431)

Supervisor 1:
Ekin Özman
Supervisor 2:
Pınar Kiliçer

$$\begin{array}{c} \mathbb{Q}(\sqrt{d}) \\ | \\ \mathbb{Q} \end{array}$$

July 2025

Abstract

In this thesis, we study aspects of the divisibility of the class numbers of quadratic number fields. We prove that there are infinitely many quadratic fields K such that $g \mid h(K)$ for $g \geq 2$. Of special interest is the case $g = 2$, where we are able to provide an elementary proof, due to Gauss. We also establish quantitative estimates on the density of quadratic number fields K with $g \mid h(K)$ for $g > 2$. Finally, we consider the problem of constructing quadratic fields with high p-rank in their class group. We compute explicit examples of imaginary quadratic fields with 5-rank ≥ 3, and prove a lower bound on the p-rank of the class group of a general number field.

Contents

Introduction

The study of the class numbers of quadratic number fields was begun by Gauss in his Disqusitiones Arithmeticae [23], where he first developed the theory of binary quadratic forms. In this thesis, we study aspects of the divisibility of class numbers of quadratic number fields. One motivation for studying the divisibility of class numbers comes from Diophantine equations, which are polynomial equations over the integers. For instance, for an odd prime p, the equation

$$x^p + y^p = z^p$$

has no nontrivial integer solutions if the number ring $\mathbb{Z}[\zeta_p]$ has class number not divisible by p – this is a special case of Fermat's Last Theorem, proven by Kummer. The general strategy for solving a Diophantine equation is to factor one (or both) sides in some suitable number ring, and in order to obtain solutions from this factorization, we need knowledge of the class number of this number ring.

This thesis is structured as follows: Chapter 1 provides an introduction to the basic objects and tools of algebraic number theory. In particular, we define the ideal class group of a number field in section 1.4. Chapter 2 provides an overview of class field theory, first working out the Artin map explicitly over $\mathbb{Q}$ in section 2.2, then outlining the general theory in section 2.3. We also briefly discuss the Chebotarev density theorem in section 2.4. Chapters 3 and 4 are dedicated to solving the following question:

> Given $g \geq 2$, how many quadratic number fields have class number divisible by g?

Chapter 3 is where we first tackle this question, in the simple case where $g = 2$. First, we establish the theory of quadratic forms, then the correspondence between (classes of) reduced forms and ideal classes. This allows us to prove that there are infinitely many quadratic number fields with even class number. Chapter 4 answers this question in the general case $g > 2$. We show that there are infinitely many quadratic fields K with $g \mid h(K)$ in the imaginary and real cases, where the proofs are due to Ankeny-Chowla [1] and Weinberger [52]. We also mention quantitative estimates of the number of quadratic fields K with $g \mid h(K)$, due to Murty [40].

In chapter 5 we study the p-rank of the class group. The problem of finding quadratic number fields with high p-rank is linked to class field theory via a theorem of Golod and Shafarevich [26]. Section 5.1 discusses this link. In section 5.2, we compute examples of imaginary quadratic number fields with 5-rank greater than 2. The method of this section is due to Mestre [36], and is based on the theory of elliptic curves. Finally in section 5.3, we provide a lower bound for the p-rank of a general number field of degree n, due to Connell and Sussman [15].

Acknowledgements

I would like to thank the following people for their invaluable contributions to the production of this thesis:

- My first supervisor, dr. Ekin Özman, for her guidance throughout the process, suggesting such an interesting research direction, and allowing me the freedom to explore deeply.
- My second supervisor, Prof dr. Pınar Kılıçer for her supervision, and for her excellent teaching of the course *Group Theory* which first got me interested in algebra, from which my interest in number theory sprang.
- Prof. dr. Steffen Müller, for his excellent teaching of the course on local fields that gave me a first exposure to the basic objects of number theory, which has given my understanding a sound foundation.
- My mother, for her support through difficult times.
- My friends, for being there for me and always giving me a reason to smile.
- Finally, a special mention to the association T.F.V. 'Professor Francken', where I spent many days playing klaverjas while thinking about a problem.

Number theory is truly the queen of mathematics, and I have been fortunate that this thesis has allowed me to explore so much of it. I hope that the joy this subject brings me is reflected in my exposition.

Chapter 1

Number fields

In this chapter, we introduce the basic notions from algebraic number theory that we will need for the rest of this thesis. In the first section, we define number fields and number rings – these are the essential objects of study in algebraic number theory. The next section discusses aspects of linear algebra in a number field, including norms, traces and discriminants. This is followed by a brief section discussing the unit group of the ring of integers.

One of the most striking phenomena that one first encounters in algebraic number theory is the loss of unique factorization in an arbitrary number ring. In section 1.4, we discuss this phenomena and define Dedekind domains, which are integral domains where every nonzero ideal factors into a product of prime ideals. Number rings are Dedekind domains (Theorem 1.4.5) and it is not too difficult to show that a Dedekind domain has unique factorization if and only if every ideal is principal (Theorem 1.4.6). This gives us a relatively straightforward way to check whether a number ring has unique factorization: we simply need to check if it is a principal ideal domain! Once we have established the required language and tools, it is not too difficult to construct an object that allows us to do this. To this end, we will define the ideal class group of a number ring, which 'measures' how far a number ring is from being a principal ideal domain in the following sense: if the ideal class group of a number ring is trivial, then that ring is a principal ideal domain, otherwise not. Section 1.5 discusses how prime ideals of $\mathcal{O}_K$ can factor in finite extensions L/K. In section 1.6, we show that the ideal class group is a finite abelian group and in the final section 1.7, we use the established tools to compute class groups explicitly.

Sections 1.1 through 1.3 and 1.6 are adapted from the material of Marcus' classic text 'Number Fields' [33]. Section 1.5 is adapted from the material of Milne's notes [37]. For a more thorough treatment of algebraic number theory, the reader is encouraged to look at these two sources.

1.1 Basic definitions

A field K is said to be a *number field* if it is a finite field extension of the rationals $\mathbb{Q}$. A number field is said to be of *degree* n if its degree over $\mathbb{Q}$ as a field extension is n.

Note any number field K has the form $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$: since $\mathbb{Q} \subseteq K$, K has characteristic 0, whence the extension $K/\mathbb{Q}$ is separable, so the primitive element theorem applies.

Example 1.1.1. (a) The trivial example: $\mathbb{Q}$ is the only number field with degree 1. We typically assume number fields have degree $n > 1$.

(b) Let $d \in \mathbb{Z}$ be squarefree. Then $K = \mathbb{Q}(\sqrt{d})$ is a number field of degree 2. Number fields of degree 2 are called *quadratic*, and in fact all of them are of this form, but see Proposition 1.1.6.

(c) Let $m \in \mathbb{Z}$ be cubefree. Then, $\mathbb{Q}[X]/(X^3 - m)$ is a number field with degree 3. Number fields of degree 3 are called *cubic*.

(d) Let ζ_m be a primitive m-th root of unity. Then, $K = \mathbb{Q}(\zeta_m)$ is a number field of degree $\varphi(m)$, where φ is Euler's totient function.

The goal of this section is to define and study a subring $\mathcal{O}_K \subset K$ containing the 'integers' of the number field, analogous to how $\mathbb{Z}$ sits inside $\mathbb{Q}$. We would like to do arithmetic with these 'integers' in a similar manner as we are used to with $\mathbb{Z}$. To accomplish this, we define the notion of integrality.

Let $A \subseteq B$ denote commutative rings with 1. An element $x \in B$ is said to be *integral* over A if it satisfies a monic polynomial relation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with coefficients $a_i \in A$. Equivalently, x is a root of some monic polynomial $f \in \mathbb{Z}[X]$.

Notation: We will often drop the 'over A' specification when it is clear what the base ring is. The set of all integral elements over A in B is called the *integral closure* of A in B. We say a ring A is *integrally closed* in B if A equals its integral closure in B. We will only talk about integral closures of A in its field of fractions $\mathrm{Frac}(A)$, so from now on, we refer to this simply as the integral closure of A without specifying the second ring.

Example 1.1.2. (a) $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, its field of fractions. Let $a/b \in \mathbb{Q}$ integral over $\mathbb{Z}$ with $a, b \in \mathbb{Z}$. If $b = \pm 1$, then $a/b \in \mathbb{Z}$ so suppose this is not the case. Then, there must exist a prime divisor $p \mid b$ such that $p \nmid a$. Since a/b is integral over $\mathbb{Z}$, it satisfies an equation

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0.$$

Multiplying this through by b^n, we obtain the equation

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0.$$

Here, p divides every element on the left-hand side except a^n, but hence $p \mid a^n$. Since $p \nmid a$, this is a contradiction. Thus, $\mathbb{Z}$ is integrally closed.

(b) In the same manner as (a), any UFD R is integrally closed in its field of fractions. Take $a, b \in R$ and repeat the same argument with $p \in R$ an irreducible element. Being integrally closed is thus a weaker condition than being a UFD (with some extra assumptions, we can salvage some kind of unique factorization, see Theorem 1.4.3).

For a number field K, we call the integral closure of $\mathbb{Z}$ in K the *ring of integers* (or *number ring*) and denote it $\mathcal{O}_K$. This is the generalization of the integers we were searching for inside K. We will show $\mathcal{O}_K$ is indeed a ring, by means of the following general characterization of integrality.

Proposition 1.1.3. Let $A \subseteq B$ be commutative rings with 1. Then, $x \in B$ is integral over A if and only if $A[x]$ is finitely generated as an A-module. More generally, finitely many $x_1, \ldots, x_n \in B$ are integral over A if and only if $A[x_1, \ldots, x_n]$ is finitely generated as an A-module.

Proof. See [2, Proposition 5.1]. □

As a consequence of the above result, we have that if $b_1, \ldots, b_n \in B$ are integral over A, then any $b \in A[b_1, \ldots, b_n]$ is integral over A as well, because $A[b_1, \ldots, b_n, b] = A[b_1, \ldots, b_n]$ is finitely generated as an A-module. In particular, sums and products of integral elements are integral themselves. As a result of this reasoning, we obtain the desired result:

Corollary 1.1.4. For any number field K, $\mathcal{O}_K$ is a ring.

Proof. Let $A = \mathbb{Z}$ and $B = \mathcal{O}_K$ for a number field K. Any $a, b \in B$ are integral over $\mathbb{Z}$ by definition, and so Proposition 1.1.3 implies that $A[a, b]$ is finitely generated as an A-module. From the above reasoning, $a + b$ and ab are also elements of $\mathcal{O}_K$, so that $\mathcal{O}_K$ is a ring. □

Example 1.1.5. (a) We have shown in Example 1.1.2 that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

(b) Let $K = \mathbb{Q}(\sqrt{2})$. This has ring of integers $\mathbb{Z}[\sqrt{2}]$ (see Theorem 1.2.7).

(c) A number field $\mathbb{Q}(\alpha)$ does not necessarily have ring of integers $\mathbb{Z}[\alpha]$! Let $K = \mathbb{Q}(\sqrt{5})$. Then $\mathcal{O}_K \neq \mathbb{Z}[\sqrt{5}]$, because $\mathbb{Z}[\sqrt{5}]$ is not integrally closed: $x = \frac{1}{2} + \frac{\sqrt{5}}{2}$ has minimal polynomial $x^2 - x - 1$ over $\mathbb{Q}$, so x must be integral over $\mathbb{Z}$, but $x \notin \mathbb{Z}[\sqrt{5}]$.

In this thesis, we shall be mainly interested in *quadratic* number fields: these are number fields K such that $[K : \mathbb{Q}] = 2$. We end this section with a result characterizing such fields.

Proposition 1.1.6. All quadratic number fields K are of the form $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is squarefree.

Proof. We know $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$. Denote the minimal polynomial of α as f_α and let $f_\alpha(X) = X^2 + pX + q$ for some $p, q \in \mathbb{Q}$. We then have $\alpha = -p/2 \pm \sqrt{D}$, where $D = p^2/4 - q$. Observe that $D \neq 0$, else $\alpha = -p/2$ and $K = \mathbb{Q}$. But then, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(-p/2 \pm \sqrt{D}) = \mathbb{Q}(\sqrt{D})$. It remains to show that we can choose D to be a squarefree integer. Since $D \in \mathbb{Q}$, we can write $D = a/b$ with $a, b \in \mathbb{Z}$. Then, we can write $b^2 D = ab$, and collecting maximal even powers of primes in the prime factorization of ab, we can write $ab = c^2 d$ where d is squarefree. Hence, $D = (c/b)^2 d$, so that $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(c/b\sqrt{d}) = \mathbb{Q}(\sqrt{d})$. □

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. If $d < 0$, we say K is an *imaginary* quadratic field, a *real* quadratic field if $d > 0$.

1.2 Linear algebra in number fields

1.2.1 Norms and traces

One can associate two functions to a number field K called the trace and the norm. These functions turn out to be quite useful in the study of the integral elements $\mathcal{O}_K$.

Let K be a number field of degree n. We associate to each element $\alpha \in K$ the $\mathbb{Q}$-linear transformation $m_\alpha : K \to K$ where m_α is multiplication by α, i.e. $m_\alpha(\beta) = \alpha\beta$. We can view K as a $\mathbb{Q}$-vector space with dimension n, and thereby pick a $\mathbb{Q}$-basis $\{e_1, \ldots, e_n\}$ for K. With a choice of basis, we can create a matrix representation for m_α.

We define the *trace* and the *norm* for $\alpha \in K$ to be the trace and determinant of a matrix representation for m_α viewed as a $\mathbb{Q}$-linear map:

$$\mathrm{Tr}_K(\alpha) = \mathrm{Tr}[m_\alpha] \in \mathbb{Q}, \qquad N_K(\alpha) = \det[m_\alpha] \in \mathbb{Q}.$$

When it is clear what K is, we will drop the subscript.

Remark 1.2.1. While we do not use this notion, note that one can define the *relative norm* on an extension L/K of number fields in much the same way by treating L as a vector space over K.

Example 1.2.2. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree and let $\alpha \in K$ be given as $a + b\sqrt{d}$. Choosing the $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$, we compute the matrix of m_α:

$$[m_\alpha] = \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Hence, $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})}(\alpha) = 2a$ and $N_{\mathbb{Q}(\sqrt{d})}(\alpha) = a^2 - db^2$.

An *embedding* of a number field K in $\mathbb{C}$ is an field homomorphism $K \to \mathbb{C}$. For example, $K = \mathbb{Q}(i)$ has two embeddings in $\mathbb{C}$, one sends $i \mapsto i$ and the other sends $i \mapsto -i$. A number field K of degree n has precisely n embeddings into $\mathbb{C}$, because there is only one way to embed $\mathbb{Q} \to \mathbb{C}$, and by standard field theory there are precisely $n = [K : \mathbb{Q}]$ ways to extend this to a field homomorphism $K \to \mathbb{C}$. We show this in the following proposition:

Proposition 1.2.3. The number of distinct embeddings $K \to \mathbb{C}$ is $[K : \mathbb{Q}]$.

Proof. We know $K = \mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$. Let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α over $\mathbb{Q}$; thus, $K \cong \mathbb{Q}[X]/(f(X))$. Denote $n = [K : \mathbb{Q}] = \deg f$ and note that any embedding $\sigma : K \to \mathbb{C}$ restricts to the identity on $\mathbb{Q}$, but $f(X)$ has n distinct roots in $\mathbb{C}$ (f is separable and irreducible). Thus there are n distinct choices for α under any embedding $K \to \mathbb{C}$, so we can extend the identity map $\mathbb{Q} \to \mathbb{C}$ in n distinct ways. □

We say an embedding $\sigma : K \to \mathbb{C}$ is a *real* embedding if $\overline{\sigma(\alpha)} = \sigma(\alpha)$ for all $\alpha \in K$ (that is, it has image contained in $\mathbb{R}$), and *complex* otherwise. Note that complex embeddings always come in conjugate pairs. We denote the number of real embeddings by r and the number of pairs of complex conjugate embeddings as s.

Example 1.2.4. (a) As we have mentioned, the only embedding $\mathbb{Q} \to \mathbb{C}$ is the identity.

(b) Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. We have two embeddings, the identity and $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. If K is real quadratic, then both of these embeddings have image contained entirely in $\mathbb{R}$ so $r = 2, s = 0$. If K is imaginary quadratic, then $r = 0, s = 1$.

(c) Let $K = \mathbb{Q}[X]/(X^3 - m)$ with m a cubefree integer $\neq 0$. Then, m has one real cube root and two complex cube roots, hence $r = 1, s = 1$.

We can alternatively define the norm and trace in terms of embeddings, as follows:

Proposition 1.2.5. Let K be a number field of degree n and $\sigma_1, \ldots, \sigma_n$ be its n embeddings into $\mathbb{C}$. Then, the trace and the norm of K are given by

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Tr}_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Proof. This is a special case of [37, Proposition 2.19], by setting $K = \mathbb{Q}$. □

Any embedding $\sigma : K \to \mathbb{C}$ permutes the roots of the minimal polynomial of an element $\alpha \in K$ – this proposition is essentially saying that the trace of $\alpha \in K$ is the sum of the roots of its minimal polynomial, and the norm is the product of the roots.

Note that if $\alpha \in \mathcal{O}_K$, then its minimal polynomial over $\mathbb{Q}$ has integer coefficients: we have $f(\alpha) = 0$ for some $f \in \mathbb{Z}[T]$, so the minimal polynomial p_α over $\mathbb{Q}$ must divide f in $\mathbb{Q}[T]$. Applying Gauss' lemma implies that $p_\alpha \in \mathbb{Z}[T]$. In fact, the converse is also true:

Proposition 1.2.6. Let K be a number field. Then, $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Proof. We have already shown the forward direction above. Conversely, let $\alpha \in \mathcal{O}_K$, so that

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0,$$

with the $a_i \in \mathbb{Z}$. Let $p_\alpha(T)$ be the minimal polynomial of α over $\mathbb{Q}$. For any other root α' of $p_\alpha(T)$, there exists a $\mathbb{Q}$-isomorphism $\mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha']$ given by $\alpha \mapsto \alpha'$. Applying this isomorphism to the above equation, we obtain

$$\alpha'^m + a_1\alpha'^{m-1} + \cdots + a_m = 0$$

so that also $\alpha' \in \mathcal{O}_K$. By the same reasoning, all the roots of $p_\alpha(T)$ are in $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a ring, it follows that the coefficients of $p_\alpha(T)$ are also in $\mathcal{O}_K$; these coefficients are in $\mathbb{Q}$, and since $\mathbb{Z}$ is integrally closed, it follows that $p_\alpha(T) \in \mathbb{Z}[T]$. □

In particular, the above implies that if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

Recall from Example 1.1.5(c) that $\mathbb{Z}[\sqrt{5}]$ is not the ring of integers of $\mathbb{Q}(\sqrt{5})$ – this highlights even for the simple case of a quadratic number field, the ring of integers is not straightforward to compute. However, norms and traces allow to compute rings of integers (in some cases). For example, we have the following result:

Theorem 1.2.7. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right] & d \equiv 1 \pmod 4 \end{cases}$$

Proof. From Example 1.2.2 and Proposition 1.2.6, we know $\alpha = x + y\sqrt{d} \in \mathcal{O}_K$ implies $2x, x^2 - dy^2 \in \mathbb{Z}$. Together, these mean that $4dy^2 \in \mathbb{Z}$. Let $y = r/s$ with $r, s \in \mathbb{Z}$ coprime. Then, $s^2 \mid 4d$, but d is squarefree: so $s^2 \mid 4$ and $s = 1$ or 2. If $s = 1$, then $y \in \mathbb{Z}$ already, whence $x \in \mathbb{Z}$ and we are done. Suppose $s = 2$, then letting $x = u/2$ and $y = v/2$ for $u, v \in \mathbb{Z}$, we obtain that $u^2 \equiv dv^2 \bmod 4$. The squares modulo 4 are just 0 and 1, so if $d \not\equiv 1 \bmod 4$, then $u^2 \equiv v^2 \equiv 0 \bmod 4$, so that u, v are even. Thus, in this case $x, y \in \mathbb{Z}$, giving $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Otherwise, $d \equiv 1 \bmod 4$ and so $u^2 \equiv v^2 \bmod 4$. Thus, $u \equiv v \bmod 2$, which means we can always write $x + y\sqrt{d} = u/2 + v/2\sqrt{d}$ in the form $a + b/2(1 + \sqrt{d})$ for $a, b \in \mathbb{Z}$. Hence, $\alpha \in \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$. □

1.2.2 The discriminant

Let K be a number field of degree n and let $\sigma_1, \ldots, \sigma_n$ be its n complex embeddings. For any $\alpha_1, \ldots, \alpha_n \in K$, define their *discriminant* as

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det \left| \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ldots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \right|^2$$

The discriminant is related to the trace from the previous subsection. Letting

$$D = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ldots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix},$$

we have the matrix equality

$$\begin{aligned} D^T D &= \begin{pmatrix} \sigma_1(\alpha_1^2) + \cdots + \sigma_n(\alpha_1^2) & \ldots & \sigma_1(\alpha_1\alpha_n) + \cdots + \sigma_n(\alpha_1\alpha_n) \\ \vdots & \ldots & \vdots \\ \sigma_1(\alpha_n\alpha_1) + \cdots + \sigma_n(\alpha_n\alpha_1) & \ldots & \sigma_1(\alpha_n^2) + \cdots + \sigma_n(\alpha_n^2) \end{pmatrix} \\ &= \begin{pmatrix} \operatorname{Tr}(\alpha_1^2) & \ldots & \operatorname{Tr}(\alpha_1\alpha_n) \\ \vdots & \ldots & \vdots \\ \operatorname{Tr}(\alpha_n\alpha_1) & \ldots & \operatorname{Tr}(\alpha_n^2) \end{pmatrix} \end{aligned}$$

so that

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(D^2) = \det(D^T D) = \det \begin{pmatrix} \operatorname{Tr}(\alpha_1^2) & \ldots & \operatorname{Tr}(\alpha_1\alpha_n) \\ \vdots & \ldots & \vdots \\ \operatorname{Tr}(\alpha_n\alpha_1) & \ldots & \operatorname{Tr}(\alpha_n^2) \end{pmatrix}$$

It follows from the above that the discriminant of any $\alpha_1, \ldots, \alpha_n \in K$ is a rational number: each element of the matrix on the right is the trace of an element of K, so must be a rational number. The determinant of a matrix with rational entries is rational, hence so is the discriminant $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. In particular, note that if the $\alpha_1, \ldots, \alpha_n$ are elements of $\mathcal{O}_K$, their discriminant $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ by Proposition 1.2.6.

In this subsection, we will utilize the discriminant to show that $\mathcal{O}_K$ is a free abelian group of rank n. The idea of the proof is to 'sandwich' $\mathcal{O}_K$ between two free abelian groups $A \subset \mathcal{O}_K \subset A'$, where A, A' are both of rank n. It follows by [50, Theorem IX.2.1] that $\mathcal{O}_K$ is a free abelian group of rank n.

First, we construct A. This is relatively straightforward, once we prove the following claim: for any $\alpha \in K$, there exists an integer m such that $m\alpha \in \mathcal{O}_K$. Let $g(X)$ be the minimal polynomial of α over $\mathbb{Q}$. By multiplying the coefficients by a common multiple of their denominators, we obtain a polynomial $f(X) \in \mathbb{Z}[X]$ with $f(\alpha) = 0$. Write

$$f(X) = a_n X^n + \cdots + a_1 X + a_0.$$

Then, one has

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$$

Multiplying through by a_n^{n-1},

$$\begin{aligned} a_n^n \alpha^n + \cdots + a_1 a_n^{n-1} \alpha + a_0 a_n^{n-1} &= 0 \\ (a_n \alpha)^n + a_{n-1}(a_n \alpha)^{n-1} + \cdots + a_1 a_n^{n-2}(a_n \alpha) + a_0 a_n^{n-1} &= 0 \end{aligned}$$

and setting $m = a_n$, we obtain an integer m so that $m\alpha$ satisfies an integral equation, i.e. $m\alpha \in \mathcal{O}_K$. In order to construct A, let us pick a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K. Using the claim we have just proven, we can always choose this basis to consist entirely of elements of $\mathcal{O}_K$. This is seen as follows: for each α_i, we obtain a m_i so that $m_i \alpha_i \in \mathcal{O}_K$ via the claim. Now, let m be any nonzero common multiple of the m_i, so the $m\alpha_1, \ldots, m\alpha_n$ form a $\mathbb{Q}$-basis of K consisting entirely of elements of $\mathcal{O}_K$. Let A be the free abelian group generated by the α_i. This is a subgroup of $\mathcal{O}_K$, as desired.

Second, we shall construct A'. This is done using the discriminant, by way of the following proposition.

Proposition 1.2.8. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K consisting entirely of elements of $\mathcal{O}_K$, and set $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. Then, every $\alpha \in \mathcal{O}_K$ may be written as

$$\alpha = \frac{m_1 \alpha_1 + \ldots m_n \alpha_n}{d}$$

for some integers $m_1, \ldots, m_n$ with $d \mid m_i^2$.

Proof. See [33, Theorem 2.9]. □

The above proposition indicates how to define A'. Let

$$A' = \frac{\alpha_1}{d}\mathbb{Z} \oplus \cdots \oplus \frac{\alpha_n}{d}\mathbb{Z}$$

then by the proposition, $\mathcal{O}_K \subset A'$. By [50, Theorem IX.2.1] we have that $\mathcal{O}_K$ is a free abelian group of rank n. For future reference, we establish this as the following theorem.

Theorem 1.2.9. For a number field K of degree n, the corresponding number ring $\mathcal{O}_K$ is a free abelian group of rank n.

After this discussion, we can define an invariant associated to the number ring $\mathcal{O}_K$: the *discriminant* of $\mathcal{O}_K$. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and denote the discriminant $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ as $\mathrm{disc}(\mathcal{O}_K)$. Of course this is not a priori well-defined, because we have not shown the discriminant is independent of the $\mathbb{Z}$-basis chosen. The following proposition remedies this:

Proposition 1.2.10. Take any two $\mathbb{Z}$-bases $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ of $\mathcal{O}_K$. Then, $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\beta_1, \ldots, \beta_n)$.

Proof. See [33, Theorem 2.11]. □

Note that the discriminant of a number ring is always is an integer, by Proposition 1.2.6. It is also possible to define the discriminant starting from just the trace, see [37, p. 33] for details.

Notation. Instead of writing $\mathrm{disc}(\mathcal{O}_K)$, we will abuse notation and write $\mathrm{disc}(K)$ instead, and say 'discriminant of K' instead of 'discriminant of $\mathcal{O}_K$'.

In view of our main topic of interest in this thesis, we compute the discriminant of a general quadratic number field.

Example 1.2.11. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. By Theorem 1.2.7, $\mathcal{O}_K$ is either $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \bmod 4$ or $\mathbb{Z}[(1+\sqrt{d})/2]$ if $d \equiv 1 \bmod 4$. Thus, a $\mathbb{Z}$-basis for $\mathcal{O}_K$ is given by $\{1, \sqrt{d}\}$ in the first case, and by $\{1, (1+\sqrt{d})/2\}$ in the second. We compute the discriminant in each case:

$$\mathrm{disc}(K) = \mathrm{disc}(1, \sqrt{d}) = \det \left| \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \right|^2 = 4d \qquad (d \equiv 2, 3 \bmod 4)$$

$$\mathrm{disc}(K) = \mathrm{disc}(1, (1+\sqrt{d})/2) = \det \left| \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix} \right|^2 = d \qquad (d \equiv 1 \bmod 4)$$

Remark 1.2.12. It is possible, as for norms and traces, to define the notion of a *relative* discriminant for a finite number field extension L/K. This is more involved, see [37, p. 33] for details. Briefly, one can directly define the discriminant $\mathrm{disc}(\beta_1, \ldots, \beta_m)$ as the determinant of the matrix $[\mathrm{Tr}(\beta_i \beta_j)]$. If the β_i form an A-basis for B, then the discriminant $\mathrm{disc}(\beta_1, \ldots, \beta_m)$ is well-defined upto the square of a unit in A. In particular, the ideal generated by $\mathrm{disc}(\beta_1, \ldots, \beta_m)$ is independent of the A-basis picked and thus we denote this ideal as $\mathrm{disc}(B/A)$ or $\mathrm{disc}(L/K)$. This construction requires $\mathcal{O}_L$ to be a free $\mathcal{O}_K$-module, otherwise the trace form is degenerate.

1.3 The unit group

In this section, we briefly discuss the structure of the group of units $U_K := \mathcal{O}_K^\times$ of the ring of integers $\mathcal{O}_K$ of a number field K. We can make a first characterization of units of a number ring by their norm:

Lemma 1.3.1. For a number field K, $\alpha \in K$ is a unit if and only if $\alpha \in \mathcal{O}_K$ and $N(\alpha) = \pm 1$.

Proof. If α is a unit, there is some $\beta \in \mathcal{O}_K$ with $\alpha\beta = 1$. By Proposition 1.2.6, we know $N(\alpha), N(\beta) \in \mathbb{Z}$; moreover $1 = N(\alpha\beta) = N(\alpha) \cdot N(\beta)$, so that $N(\alpha) = \pm 1$. Conversely, fix an embedding $\sigma : K \to \mathbb{C}$. Using this embedding, we can identify K with a subfield of $\mathbb{C}$. Using the definition of the norm in Proposition 1.2.5, we have

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \prod_{\sigma_i \neq \sigma} \sigma_i(\alpha).$$

Let $\beta = \prod_{\sigma_i \neq \sigma} \sigma_i(\alpha)$. If $\alpha \in \mathcal{O}_K$, then each $\sigma_i(\alpha)$ is also integral over $\mathbb{Z}$ (but not necessarily in $\mathcal{O}_K$), by Proposition 1.2.6, and so β is integral over $\mathbb{Z}$ itself. If $N(\alpha) = \pm 1$, then $\alpha\beta = \pm 1$ and so $\beta = \pm 1/\alpha \in K$. Therefore, if $\alpha \in \mathcal{O}_K$ and $N(\alpha) = \pm 1$, then α is a unit as required. □

The unit group U_K is a free abelian group of rank $\leq n$ as a subgroup of $\mathcal{O}_K$. One of the basic theorems of algebraic number theory is Dirichlet's unit theorem, which explicitly relates the rank of U_K to the number of real and complex embeddings of K into $\mathbb{C}$.

Theorem 1.3.2 (Dirichlet's unit theorem)**.** Let K be a number field with r real embeddings and s pairs of complex conjugate embeddings. Then, the unit group U_K is finitely generated and abelian with rank equal to $r + s - 1$.

Proof. See [37, Chapter 5] or [33, Chapter 5]. □

Example 1.3.3. (a) Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. If $d < 0$, that is, K is imaginary, we have a pair of complex conjugate embeddings (the identity and complex conjugation) so $r = 0$, $s = 1$. Dirichlet's unit theorem implies U_K is finite.

(b) If $d > 0$, we have $r = 2$, $s = 0$, so the theorem implies that the unit group has rank 1. Hence $U_K = \pm\varepsilon^{\mathbb{Z}}$ for some ε. We call this ε the *fundamental unit*. The fundamental unit is commonly *normalised*: this means that we pick ε so that it is the minimal generator of U_K with $\varepsilon > 1$ (as a real number).

(c) Let $K = \mathbb{Q}[X]/(X^3 - m)$ with $m \neq 0$ a cubefree integer. We know from Example 1.2.4 that $r = 1 = s$, so U_K has rank 1.

1.4 Unique factorization and the ideal class group

The fundamental theorem of arithmetic says that any integer n has a unique factorization as a product of primes (alternatively, this says that $\mathbb{Z}$ is a UFD). In an arbitrary number ring $\mathcal{O}_K$, we often do not get unique factorization. For example, consider $K = \mathbb{Q}(\sqrt{-5})$. We have the factorization

$$6 = 3 \cdot 2 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ (see Proposition 1.1.6). Note that in $\mathbb{Z}[\sqrt{-5}]$, no element can have norm 2 or 3: an element $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ has norm 2 or 3 when $a^2 + 5b^2 = 2$ or 3, but this is impossible. The elements 2, 3, $1 - \sqrt{-5}$, $1 + \sqrt{-5}$ have norms 4, 9, 6 and 6 respectively. If any of them were reducible, the factors would have norm either 2 or 3, but this is not possible. The above is hence an example of the failure of unique factorization in $\mathcal{O}_K$.

This failure of unique factorization presents a challenge. The idea of this section is that we would like some sort of 'unique factorization' in the ring of integers $\mathcal{O}_K$: since we do not necessarily have unique factorization for elements in an arbitrary $\mathcal{O}_K$, we settle for unique factorization of ideals. Given a ring of integers $\mathcal{O}_K$, we can use unique factorization of ideals to define the *ideal class group*, which measures 'how far' a number ring is from being a UFD (see Theorem 1.4.6). To establish the machinery for this, we estiablish the notion of a Dedekind domain in the first subsection. The following subsection introduces the notion of a fractional ideal, which generalise the usual ideals. Armed with these definitions, we can finally define the ideal class group of a number field.

1.4.1 Factorization and Dedekind domains

A *Dedekind domain* is an integral domain R such that

(i) Every ideal of R is finitely generated,

(ii) Every nonzero prime ideal is maximal,

(iii) R is integrally closed (in its field of fractions).

In this section, we will work in the general setting where A is a Dedekind domain, note that all our results specialize to the case where $A = \mathcal{O}_K$ for some K (see Theorem 1.4.5).

Example 1.4.1. (a) Any field K is a Dedekind domain: the only ideals of K are (0) and (1), and $\operatorname{Frac} K = K$ so of course K is integrally closed in its field of fractions.

(b) Any principal ideal domain is a Dedekind domain. Every ideal is principal, therefore finitely generated; in particular prime ideals are principal therefore maximal. A principal ideal domain is a UFD, so also integrally closed, see Example 1.1.2.

(c) Not all Dedekind domains are PIDs, or even UFDs. As an example, take $\mathbb{Z}[\sqrt{-5}]$ from the beginning of this section. In fact, for a Dedekind domain, being a UFD is equivalent to being a PID: see Theorem 1.4.6.

Remark 1.4.2. Rings satisfying condition (i) in the definition above are called *Noetherian*. One of the main useful results about Noetherian rings is that any ideal has a primary decomposition, that is, every ideal can be decomposed as the intersection of finitely many primary ideals. This is a much more general version of Theorem 1.4.3, see [2, Chapter 4] for details.

As mentioned at the beginning of this section, the motivation for studying Dedekind domains in our context comes from the following result:

Theorem 1.4.3. Every ideal in a Dedekind domain can be uniquely represented as a product of prime ideals.

Proof. See [33, Theorem 3.16] or [37, Theorem 3.7]. □

Corollary 1.4.4. Let I be an ideal in a Dedekind domain. Then, there is an ideal J such that IJ is principal.

Proof. Suppose I factors into prime ideals as $I = \prod_i \mathfrak{p}_i^{r_i}$. Pick $a \in I$ with $a \neq 0$ and let (a) factor into prime ideals as $(a) = \prod_i \mathfrak{p}_i^{s_i}$ with $s_i \geq r_i$, where the prime ideals in the factorization must be the same since $(a) \subset I$. Define $J = \prod_i \mathfrak{p}_i^{s_i - r_i}$, then $IJ = (a)$ by commutativity. □

This result will allow us to recover some notion of unique factorization in an arbitrary number ring $\mathcal{O}_K$. Of course, to use this result, it remains to show rings of integers are in fact Dedekind domains.

Theorem 1.4.5. For a number field K of degree n, $\mathcal{O}_K$ is a Dedekind domain.

Proof. From Theorem 1.2.9, we know $\mathcal{O}_K$ is a free abelian group with rank n; any ideal of $\mathcal{O}_K$ is an additive subgroup, therefore finitely generated. We need to show every nonzero prime ideal is maximal. It suffices to show that for any prime ideal $\mathfrak{p}$, $\mathcal{O}_K/\mathfrak{p}$ is finite, since any finite integral domain is a field. We show the more general fact: that $\mathcal{O}_K/I$ is finite for any nonzero ideal $I \subset \mathcal{O}_K$. Let $I \subset \mathcal{O}_K$ be a nonzero ideal, and pick $0 \neq \alpha \in I$. From Proposition 1.2.6, $m := N(\alpha) \in \mathbb{Z}$, and from the definition of the norm $m \neq 0$. Using the alternative definition of the norm in Proposition 1.2.5, we can write $m = \alpha\beta$, where β is a product of conjugates of α. Moreover, $\beta \in \mathcal{O}_K$, since $\beta = m/\alpha \in K$ and β is integral over $\mathbb{Z}$ as the product of integral elements. Hence, $m \in I$. Since $\mathcal{O}_K$ is a free abelian group with rank n, we have

$$\mathcal{O}_K/(m) \cong \mathbb{Z}^n/(m) \cong \mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$$

and since $(m) \subset I$, we have $\mathcal{O}_K/I \subset \mathcal{O}_K/(m)$, so $\mathcal{O}_K/I$ is finite as required. Finally, we have defined $\mathcal{O}_K$ to be integrally closed, so we are done. □

We know that every PID is also a UFD. The converse is false in general: take for example $R = K[X, Y]$ with K a field, then the ideal (X, Y) is not principal. However, for Dedekind domains the converse does hold:

Theorem 1.4.6. A Dedekind domain is a UFD if and only if it is a PID.

Proof. We only need to prove the forward direction. Let A be a Dedekind domain. It suffices to show that every prime ideal is principal by Theorem 1.4.3, since the product of principal ideals is principal. To this end, suppose $\mathfrak{p} \subset A$ is a nonzero prime ideal and pick any $a \in \mathfrak{p}$. Since A is a UFD, a factors uniquely into irreducibles, let one of these irreducibles be denoted π. Irreducible elements generate prime ideals in UFDs: since we have $\mathfrak{p} \supset (\pi) \neq 0$ and prime ideals are maximal in Dedekind domains, it follows $\mathfrak{p}$ is principal. □

1.4.2 Fractional ideals, the ideal class group

Let A be a Dedekind domain and K its field of fractions. A *fractional ideal* of A is a nonzero A-submodule M of K, such that there exists an $x \neq 0$ in A so that xM is an ideal of A. In particular, the 'ordinary' ideals of A are fractional ideals by taking $x = 1$. To avoid confusion, henceforth we refer to the ideals of A as *integral ideals*. Intuitively, one can think of fractional ideals as defining the 'negative powers' in the factorization of an ideal into prime powers.

Every element $b \in K^\times$ defines a fractional ideal as

$$(b) := \{ba \mid a \in A\}$$

A fractional ideal of this form is said to be *principal*.

Example 1.4.7. Let $M \subset \mathbb{Q}$ be the set of all integer multiples of $2/3$. Then, M is a fractional ideal of $\mathbb{Z}$ (because eg. $3M \subset \mathbb{Z}$).

Products of fractional ideals are defined the same way as for integral ideals: let M and N be fractional ideals of A, then

$$MN := \left\{ \sum_i m_i n_i \mid m_i \in M, n_i \in N \right\}$$

This is still an A-module; moreover if $xM \subset A$ and $yN \subset A$ then $xyMN \subset A$, so MN is also a fractional ideal of A. Note in particular that the product of principal fractional ideals is also principal. This motivates the following theorem:

Theorem 1.4.8. Let A be a Dedekind domain. The set of fractional ideals I_A of A forms a group under multiplication. In particular, it is the free abelian group generated by prime ideals of A.

Proof. We have seen fractional ideals are closed under multiplication. Clearly A itself is a fractional ideal, so we have an identity element. We are working with commutative rings, so commutativity of the operation follows; we do not show associativity as it is a bit tedious. We need only show the existence of inverses. Let $\mathfrak{a}$ be an integral ideal of A. Then, Corollary 1.4.4 implies there is an $\mathfrak{a}^*$ such that $\mathfrak{a}\mathfrak{a}^* = (a)$ is principal. Then of course $\mathfrak{a}(a^{-1}\mathfrak{a}^*) = (1) = A$, so an inverse for $\mathfrak{a}$ is given by $\mathfrak{a}^{-1} = a^{-1}\mathfrak{a}^*$. If we let $\mathfrak{a}$ be a fractional ideal instead, there exists a nonzero $x \in A$ such that $x\mathfrak{a}$ is an integral ideal. Then, there is an integral ideal $(x\mathfrak{a})^*$ so that $(x\mathfrak{a})(x\mathfrak{a})^*$ is principal. An inverse for $\mathfrak{a}$ is thus given by $\mathfrak{a}^{-1} = x \cdot (x\mathfrak{a})^{-1}$, where $(x\mathfrak{a})^{-1}$ is the inverse for an integral ideal just defined.
It remains to show that I_A is in fact generated by the prime ideals of A. This essentially follows from Theorem 1.4.3: for any fractional ideal $\mathfrak{a}$, there is a nonzero $x \in A$ such that $x\mathfrak{a}$ is an integral ideal. By Theorem 1.4.3, one can write

$$x\mathfrak{a} = \mathfrak{p}_1^{r_1} \dots \mathfrak{p}_m^{r_m}, \quad (x) = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m}$$

Thus, by the same argument as Corollary 1.4.4, we have $\mathfrak{a} = \mathfrak{p}_1^{r_1 - s_1} \dots \mathfrak{p}_m^{r_m - s_m}$, and the uniqueness of the representation follows via the uniqueness asserted for integral ideals in Theorem 1.4.3. □

We define the *ideal class group* $\mathrm{Cl}(A)$ of a Dedekind domain A as the quotient $\mathrm{Cl}(A) = I_A/P_A$ of the group of fractional ideals by its subgroup of principal fractional ideals. The *class number* of A is the order of the class group $h(A) = |\mathrm{Cl}(A)|$. When $A = \mathcal{O}_K$ for a number field K, we will refer to $\mathrm{Cl}(\mathcal{O}_K)$ as the ideal class group of K and its order as the class number K. We will also be a bit careless and denote $\mathrm{Cl}(\mathcal{O}_K)$ as $\mathrm{Cl}(K)$, $h(\mathcal{O}_K)$ as $h(K)$, $I_{\mathcal{O}_K}$ and $P_{\mathcal{O}_K}$ as I_K and P_K respectively.

Let K be a number field. We have seen that $\mathcal{O}_K$ does not have to be a UFD. Indeed, the ideal class group provides us with a way to check whether a given number ring is a UFD: via Theorem 1.4.6, if the ideal class group $\mathrm{Cl}(K)$ is trivial, then every fractional ideal is principal, which implies $\mathcal{O}_K$ is a UFD. Since we would prefer our number rings to have unique factorization, a question arises: which number fields have class number 1? This is the **class number problem**, first posed by Gauss in 1801. So far, it is known there are only 9(!) imaginary quadratic fields with class number one; in the real quadratic case the answer is still not known. Part of the difficulty of the class number problem in the real case is that the unit group is no longer finite (see Dirichlet's unit theorem).

To end this section, we will make a final note. There is a homomorphism from $K^\times$ to I_K given by $\alpha \mapsto (\alpha)$ the fractional ideal generated by α. The kernel of this homomorphism is U_K, as the units of $\mathcal{O}_K$ generate the ideal (1) in $\mathcal{O}_K$. This yields the following exact sequence, sometimes called the fundamental exact sequence of algebraic number theory:

$$1 \to U_K \to K^\times \to I_K \to \mathrm{Cl}(K) \to 1 \tag{1.1}$$

1.5 Prime decomposition in number rings

Let K be a number field. A prime ideal (p) of $\mathbb{Z}$ does not necessarily have to be prime when viewed as an ideal in $\mathcal{O}_K$. From Theorem 1.4.3, we know that $p\mathcal{O}_K$ can be factored uniquely as a product of prime ideals

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$$

where the $\mathfrak{p}_i \subset \mathbb{Z}$ are prime ideals with $e_i \geq 1$ for every i. In this section, we discuss this phenomenon in the more general setting where we replace $\mathbb{Z} \subseteq \mathcal{O}_K$ with $\mathcal{O}_K \subset \mathcal{O}_L$, where $K \subseteq L$ are number fields. That is, we study the factorization of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ when viewed as an ideal $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$ into

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_k^{e_k} \tag{1}$$

where the $\mathfrak{P}_i$ are prime ideals of $\mathcal{O}_L$. The material in this section is adapted from Milne's notes [37, p. 59-65].

We have the following lemma about divisibility of ideals $\mathfrak{p} \subset \mathcal{O}_K$ by prime ideals of $\mathcal{O}_L$:

Lemma 1.5.1. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime ideal. Then, $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}_L$ if and only if $\mathfrak{p} = \mathfrak{P} \cap K$.

Proof. If a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ divides $\mathfrak{p}\mathcal{O}_L$, then $(p) \subset \mathfrak{p} \cap K$ by definition. Moreover, $\mathfrak{p}$ is maximal since $\mathcal{O}_K$ is Dedekind, so $\mathfrak{p} = \mathfrak{P} \cap K$. Conversely, If $\mathfrak{p} = \mathfrak{P} \cap K$, then $\mathfrak{P} \subset \mathfrak{p}\mathcal{O}_L$, and Theorem 1.4.3 implies that $\mathfrak{P}$ must appear in the factorization of $\mathfrak{p}\mathcal{O}_L$, hence $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}_L$. □

If $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_L$, it lies over a unique prime ideal $\mathfrak{p} = \mathfrak{P} \cap K$ by Lemma 1.5.1.

Notation. If a prime ideal $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}_L$, we say $\mathfrak{P}$ is *lying over* $\mathfrak{p}$. If $\mathfrak{P}$ is lying over $\mathfrak{p}$, it must be one of the $\mathfrak{P}_i$ in (1). The corresponding e_i is called the ramification index and written $e_{\mathfrak{P}|\mathfrak{p}} = e_i$. Each prime ideal $\mathfrak{P}$ dividing $\mathfrak{p}$ also yields an extension of residue fields $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$ (recall $\mathcal{O}_K$ and $\mathcal{O}_L$ are Dedekind domains, so nonzero prime ideals are maximal). By the proof of Theorem 1.4.5, this is an extension of finite fields. We call the degree of this extension the *inertial degree*, denoted by $f_{\mathfrak{P}|\mathfrak{p}} = f_i$.

If any of the $e_i > 1$, we say that $\mathfrak{p}$ *ramifies* in $\mathcal{O}_L$ (or L). If all of the $e_i = 1$, then we say $\mathfrak{p}$ is *unramified* in L. Finally, if $\mathfrak{p}$ satisfies the stronger condition that all e_i and f_i are 1, then we say $\mathfrak{p}$ *splits completely* in L. If $\mathfrak{p}$ stays prime in $\mathcal{O}_L$, then we will say $\mathfrak{p}$ is *inert*.

Example 1.5.2. We work in the extension $\mathbb{Q}(i)/\mathbb{Q}$.

- Consider the prime ideal $(2) \subset \mathbb{Z}$. We can factor $2 = (1+i)(1-i)$, so we can write

$$2\mathbb{Z}[i] = (1+i)(1-i)$$

Recall that prime elements generate prime ideals, so we need to show that both $1+i$ and $1-i$ are prime. We can see this by computing norms: $N(1+i) = 2 = N(1-i)$, so if either was not prime, there would exist nonunit $x, y \in \mathbb{Z}[i]$ with $N(x)N(y) = N(xy) = N(1 \pm i) = 2$ which is a contradiction. Moreover, $(1-i) = -i(1+i)$ so $2\mathbb{Z}[i] = (1+i)^2$. Thus, here we have $e = 2$. Since $ef = 2$ by the theorem, we have $f = 1$.

- Consider the prime ideal $(7) \subset \mathbb{Z}$. This prime stays inert in L, which can be seen once again by computing norms. Recall that $\mathbb{Z}[i]$ is Euclidean, so in particular a UFD. Hence, if 7 is not prime in $\mathbb{Z}[i]$, it must factor as the product of nonunit irreducibles $7 = ab$. By Lemma 1.3.1, a cannot have norm ± 1, so $N(a) = \pm 7$. But letting $a = x + iy$, this means $x^2 + y^2 = 7$ for $x, y \in \mathbb{Z}$, which is impossible. Hence, here $e = 1$ and $f = 2$. The residue field is thus $\mathbb{Z}[i]/7\mathbb{Z}[i] \cong \mathbb{F}_{49}$.

Notation: When talking about ramification, if we are working with $K = \mathbb{Q}$, we will often drop the brackets around prime ideals (p) and just write p.

Ramification indices and inertial degrees are multiplicative over finite extensions:

Proposition 1.5.3. Let $K \subset L \subset M$ be an extension of number fields with corresponding rings of integers $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$. Take a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathfrak{P}$ lying over $\mathfrak{p}$ in $\mathcal{O}_L$ and $\mathfrak{Q}$ lying over $\mathfrak{P}$ in $\mathcal{O}_M$. Then, the ramification indices and inertial degrees satisfy:

$$e_{\mathfrak{Q}|\mathfrak{p}} = e_{\mathfrak{Q}|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}}, \text{and} \quad f_{\mathfrak{Q}|\mathfrak{p}} = f_{\mathfrak{Q}|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathfrak{p}}$$

Proof. The multiplicativity of the inertial degrees follows from the definitions: we have

$$f_{\mathfrak{Q}|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathfrak{p}} = [\mathcal{O}_M/\mathfrak{Q} : \mathcal{O}_L/\mathfrak{P}] \cdot [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_M/\mathfrak{Q} : \mathcal{O}_K/\mathfrak{p}] = f_{\mathfrak{Q}|\mathfrak{p}}$$

by the multiplicativity of field extension degrees. To show this for the ramification indices, let e denote $e_{\mathfrak{Q}|\mathfrak{P}}$ and e' denote $e_{\mathfrak{P}|\mathfrak{p}}$. Then, by factoring in $\mathcal{O}_L$ then $\mathcal{O}_M$, we have

$$\mathfrak{p}\mathcal{O}_M = (\mathfrak{p}\mathcal{O}_L)\mathcal{O}_M = \left(\prod \ldots \mathfrak{P}^{e'} \ldots\right)\mathcal{O}_M = \prod \ldots (\mathfrak{P}\mathcal{O}_M)^{e'} \cdots = \prod \ldots \mathfrak{Q}^{ee'} \ldots$$

where we have ignored all the primes in the respective factorizations except the relevant ones. This completes the proof. □

This proposition means that if we have a prime $\mathfrak{p}$ of K unramified in M, then $\mathfrak{p}$ is also unramified in L. Conversely, if $\mathfrak{p}$ ramifies in L, then it also ramifies in M.

Suppose now the extension L/K is Galois. Any $\sigma \in \mathrm{Gal}(L/K)$ restricts to a ring automorphism of $\mathcal{O}_L$, thus must take prime ideals to prime ideals. By Lemma 1.5.1, we know that $\mathfrak{p} = \mathfrak{P} \cap K = \mathfrak{P}' \cap K$. Since σ fixes K, it follows that $\sigma(\mathfrak{P})$ must be another prime ideal $\mathfrak{P}'$ lying over $\mathfrak{p}$. Together, all this means that the Galois group G acts on the set of prime ideals lying over $\mathfrak{p}$. Clearly $\mathrm{id}(\mathfrak{P}) = \mathfrak{P}$, and if $\sigma_1, \sigma_2 \in G$ then $(\sigma_1 \circ \sigma_2)(\mathfrak{P}) = \sigma_1(\sigma_2(\mathfrak{P}))$, and we have already argued that $\sigma_2(\mathfrak{P})$ is a prime ideal lying over $\mathfrak{p}$. In fact, this action is transitive:

Lemma 1.5.4. The action of the Galois group L/K on the set of prime ideals lying over $\mathfrak{p}$ is transitive.

Proof. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be distinct prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Suppose there is no automorphism $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Since $\mathcal{O}_L$ is a Dedekind domain, any two prime ideals of $\mathcal{O}_L$ are maximal and consequently coprime. The Chinese remainder theorem then yields the existence of an $\beta \in \mathcal{O}_K$ such that $\beta \equiv 0 \bmod \mathfrak{P}'$ and $\beta \equiv 1 \bmod \sigma(\mathfrak{P})$ for any $\sigma \in \mathrm{Gal}(L/K)$ (that is, $\beta \in \mathfrak{P}'$ but $\beta \notin \sigma(\mathfrak{P})$). Then, the norm $b = N(\beta) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta)$ is an element of $\mathbb{Z}$ since $\beta \in \mathcal{O}_L$, and also an element of $\mathfrak{P}'$ since $b = \beta \cdot \prod_{\sigma \neq \mathrm{id}} \sigma(\beta)$. Hence, $b \in \mathfrak{P}' \cap \mathbb{Z} = \mathfrak{p}$. By construction of β, $\beta \notin \sigma(\mathfrak{P})$ for any $\sigma \in \mathrm{Gal}(L/K)$, and thus $\sigma(\beta) \notin \mathfrak{P}$. But $b \in \mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}$ which contradicts the primality of $\mathfrak{P}$. □

We obtain as a corollary that the ramification indices and inertial degrees are equal for two distinct primes lying over $\mathfrak{p}$, if L/K is Galois. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$. There exists a $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{P}_1) = \mathfrak{P}_j$ for any j, thus $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{P}_j^{e_1} \sigma(\mathfrak{P}_2)^{e_2} \dots \sigma(\mathfrak{P}_r)^{e_r}$. By unique factorization of ideals, we must then have $e_1 = e_j$. This also yields, an isomorphism $\mathcal{O}_L/\mathfrak{P}_1 \to \mathcal{O}_L/\mathfrak{P}_j$, so the corresponding inertial degrees are equal. In fact, we can say more even when L/K is not Galois; the relation between the e_i and the f_i is as follows:

Theorem 1.5.5. If e_i (resp. f_i), $i = 1, \dots, k$ are the ramification indices (resp. inertial degrees) of $\mathfrak{p}\mathcal{O}_L$ defined in (1), then

$$\sum_{i=1}^{k} e_i f_i = n.$$

If the extension L/K is Galois, one has $e := e_1 = \dots = e_k$ and $f := f_1 = \dots = f_k$.

Proof. For the first part, see [33, Theorem 3.21]. The second assertion we have shown above. □

Notation: If the extension L/K is Galois, we denote the corresponding Galois group $\mathrm{Gal}(L/K)$ as $G_{L/K}$ or G where the context is clear. The induced extension of residue fields $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$ is also Galois because it is an extension of finite fields (see the proof of Theorem 1.4.5), and we denote the corresponding Galois group as $\overline{G}_{\mathfrak{P}|\mathfrak{p}}$ or simply $\overline{G}$.

Given number fields $K \subset L$, it is useful to be able to compute the factorization of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ in $\mathcal{O}_L$. This is usually achieved via the following theorem.

Theorem 1.5.6 (Dedekind-Kummer)**.** Suppose $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and let $f(X)$ be the minimal polynomial of α over K. If $\mathfrak{p} \subset \mathcal{O}_K$ is prime and f factors into distinct irreducible polynomials modulo $\mathfrak{p}$ as

$$f(X) = \prod_{i=1}^{r} g_i(X)^{e_i} \pmod{\mathfrak{p}}$$

then $\mathfrak{p}\mathcal{O}_L$ factors into prime ideals as

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} (\mathfrak{p}, g_i(\alpha))^{e_i}.$$

Moreover, also $\mathcal{O}_L/(\mathfrak{p}, g_i(\alpha))^{e_i} \cong (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{g}_i)$, so that $f_i = \deg g_i$.

Proof. See [37, Theorem 3.41]. □

Example 1.5.7. Take $K = \mathbb{Q}(\alpha)$ with α a root of $f(X) = X^3 + X + 1$. Using Dedekind-Kummer, we look at how the primes 2 and 3 factorize in $\mathcal{O}_K$. Reducing f modulo 2 and 3 yields

$$\begin{aligned} f(X) &\equiv X^3 + X + 1 \pmod 2 \\ &\equiv (X-1)(X^2 + X - 1) \pmod 3 \end{aligned}$$

Hence 2 is inert in $\mathcal{O}_K$, while 3 splits into the prime ideals $(3, \alpha - 1)$ and $(3, \alpha^2 + \alpha - 1)$.

After studying the theory of ramification, a natural question that arises is: what are the primes that ramify? We would like to obtain a description of the primes that ramify in an extension of number fields $L \supset K$. This turns out to be a very nice description:

Theorem 1.5.8. Suppose $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module. Then, a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in L if and only if $\mathfrak{p} \mid \operatorname{disc}(L/K)$ in $\mathcal{O}_K$. In particular, only finitely many primes of $\mathcal{O}_K$ ramify in L.

Proof. See [37, Theorem 3.35] for a full proof. □

We end this section by stating some corollaries of the above theorem. In the trivial case where $L = K = \mathbb{Q}$, we obtain the following result, due to Minkowski:

Corollary 1.5.9. There are no nontrivial extensions $K/\mathbb{Q}$ such that every prime ideal $(p) \subset \mathbb{Z}$ is unramified in $\mathcal{O}_K$.

Proof. Any nontrivial finite extension $K/\mathbb{Q}$ has discriminant $|\operatorname{disc}(K)| > 1$; this is a consequence of Minkowski's bound (Theorem 1.6.4), since any nontrivial extension must have $n \geq 2$, we deduce that $\operatorname{disc}(K) \geq 4$. Thus, it follows from the previous theorem that there is always a prime of $\mathbb{Q}$ that ramifies in K. □

In the case where K is a quadratic number field, Theorem 1.5.5 gives 3 possibilities for the factorization of $\mathfrak{p}\mathcal{O}_K$, which we summarize in the following corollary.

Corollary 1.5.10. Let K be a quadratic number field. If $p \in \mathbb{Z}$ is prime, then

$$p\mathcal{O}_K \text{ is } \begin{cases} \text{ramified, } p\mathcal{O}_K = \mathfrak{p}^2, & \text{if } p \mid \operatorname{disc}(K) \\ \text{splits, } p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}', & \text{if } p \nmid \operatorname{disc}(K) \text{ and } \operatorname{disc}(K) \text{ is a quadratic residue mod } p \\ \text{inert, i.e. } p\mathcal{O}_K \text{ remains prime,} & \text{if } p \nmid \operatorname{disc}(K) \text{ and } \operatorname{disc}(K) \text{ is not a quadratic residue mod } p \end{cases}$$

Remark 1.5.11. The conditions above are precisely the conditions that define the Legendre symbol: for a prime p, one defines the *Legendre symbol* as

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ and } a \text{ is a quadratic residue} \pmod p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a quadratic residue} \pmod p \end{cases}$$

The law of quadratic reciprocity, proven by Gauss, says that for distinct odd primes p, q, one has

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

1.6 Finiteness of the class group

In this section, we will show the ideal class group of a number ring is in fact finite.

Let $\mathfrak{a}$ be a nonzero ideal of a number ring $\mathcal{O}_K$. We define the norm of $\mathfrak{a}$ to be the size of the corresponding quotient ring, i.e. $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$. Here, we use the same notation as the usual element norm because these two notions coincide in the following sense: if $\mathfrak{a}$ is principal with $\mathfrak{a} = (a)$, then the element and the ideal norm are related as $N(\mathfrak{a}) = |N(a)|$ [37, p. 68].

Establishing the finiteness of the class group is done via the following result:

Theorem 1.6.1. Every nonzero ideal I of $\mathcal{O}_K$ contains a nonzero element α such that

$$|N(\alpha)| \leq \lambda N(I)$$

where λ is a positive constant depending on K.

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K into $\mathbb{C}$ and let $\alpha_1, \ldots, \alpha_n$ be an $\mathbb{Z}$-basis for $\mathcal{O}_K$. We claim that we can pick

$$\lambda = \prod_i \sum_j |\sigma_i(\alpha_j)|.$$

Pick an ideal $I \subset \mathcal{O}_K$ and set m to be the unique integer such that $m^n \leq N(I) < (m+1)^n$. Consider the elements of $\mathcal{O}_K$ of the form

$$\sum_{j=1}^{n} m_j \alpha_j, \qquad 0 \leq m_j \leq m$$

There are $(m+1)^n$ of these elements by counting the possibilities for m_j, and thus at least two of these elements must be congruent modulo I. Take the difference of these two elements, then we have an element of I of the form

$$\sum_{j=1}^{n} m_j \alpha_j, \qquad |m_j| \leq m$$

Denote this element as α. Then,

$$|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \prod_i \sum_j |m_j| \cdot |\sigma_i(\alpha_j)| \leq m^n \lambda \leq \lambda N(I)$$

which completes the proof. □

The point of the above theorem is that now we will be able to pick an ideal in every ideal class of $\mathrm{Cl}(K)$ such that its norm is bounded above. Let us formalize this in the following:

Corollary 1.6.2. The number of ideal classes in $\mathrm{Cl}(K) = I_K/P_K$ is finite.

Proof. First, we show every ideal class contains an ideal J such that $N(J) \leq \lambda$, where λ is as in the proof of the above theorem. Given an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(K)$, fix any ideal $I \in [\mathfrak{a}]^{-1}$. By the theorem, there exists an $\alpha \in I$ such that $|N(\alpha)| \leq \lambda N(I)$; by Corollary 1.4.4 there must exist an ideal J with $IJ = (\alpha)$.

Since IJ is principal, we have $J \in [\mathfrak{a}]$. Thus,

$$|N(\alpha)| = N((\alpha)) = N(IJ) = N(I)N(J)$$

so that $N(J) \leq \lambda$. It suffices now to show there are finitely many ideals $\mathfrak{a}$ in $\mathcal{O}_K$ such that $N(\mathfrak{a}) \leq \lambda$. Suppose $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ with $N(\mathfrak{a}) \leq \lambda$ and suppose the prime factorization of $\mathfrak{a}$ is given by $\prod_i \mathfrak{p}_i^{e_i}$. Then, $N(\mathfrak{a}) = \prod_i N(\mathfrak{p}_i)^{e_i} = \prod_i p_i^{e_i f_i}$ where $p_i = \mathfrak{p}_i \cap \mathbb{Z}$. Since $N(\mathfrak{a}) \leq \lambda$ by assumption, this allows finitely many possibilities for the primes p_i and their exponents e_i and f_i, so there are finitely many possible $\mathfrak{a}$. □

We can use Theorem 1.6.1 to compute class groups explicitly in the following manner. Note that every ideal class of the class group contains an ideal J with $|N(J)| \leq \lambda$. We can compute λ, and the prime ideals of $\mathcal{O}_K$ that can divide J must be the ones lying over the primes $p \in \mathbb{Z}$ with $p \leq m$. Suppose J factors into prime ideals as $J = \prod_i \mathfrak{p}_i^{e_i}$. Taking norms, we have $N(J) = \prod_i p_i^{e_i f_i} \leq \lambda$ where the $p_i = \mathfrak{p}_i \cap \mathbb{Z}$. Each of these primes p_i must therefore satisfy $p_i \leq \lambda$. Via Theorem 1.5.6, we can compute the factorizations of $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ for each p. Finally, we must check whether any of the $\mathfrak{P}_i$ are themselves principal for a given p, and compute the relations between ideal classes so we can obtain the group structure of the class group. Let us provide an example to illustrate this procedure:

Example 1.6.3. Let $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$. Taking $\mathbb{Z}$-basis $\{1, i\}$, we obtain $\lambda = 2$ as in the proof of Theorem 1.6.2. Thus, we only need to check the primes lying over 2. Note that $2\mathcal{O}_K$ factors into the prime ideals $(1+i)^2$ from Example 1.5.2. Thus, every ideal is principal and $\mathbb{Q}(i)$ has class number 1.

Computing class groups using the bound of Theorem 1.6.1 can become quite cumbersome. This is because the present value of λ gets large quite quickly, so the bound itself is not very useful. The finiteness of the class group is not a property of an arbitrary Dedekind domain, and the proof of Theorem 1.6.1 relies (in some sense) on the fact that number rings can be embedded as a lattice into some finite dimensional real vector space. This idea can be used to prove the following improved bound, due to Minkowski:

Theorem 1.6.4 (Minkowski's bound)**.** Let K be a number field of degree n with discriminant $\mathrm{disc}(K)$. Let s denote the number of pairs of complex embeddings of K. Then, each ideal class of $\mathrm{Cl}(K)$ contains an ideal J such that

$$|N(J)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |\mathrm{disc}(K)|^{\frac{1}{2}}$$

Proof. See [37, Chapter 4] or [33, Chapter 5]. □

This bound grows much slower with n than Theorem 1.6.1. We can use the bound of Theorem 1.6.4 in the same way as Theorem 1.6.1 to compute class groups (more efficiently), which we provide examples of in the following section.

1.7 Examples of computing class groups

In this section, we use Minkowski's bound and the Dedekind-Kummer theorem (Theorem 1.5.6) to compute class groups explicitly in some small examples.

Example 1.7.1. When the Minkowski bound is less than 2, the class group is trivial. When K is real quadratic, one has $s = 0$, so the class group is trivial when $|\text{disc}(K)| < 16$. For imaginary quadratic fields, $s = 1$, so the bound is less than 2 when $|\text{disc}(K)| < \pi^2$. This tells us immediately that the following fields have $h_K = 1$: $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{13}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$ by computing discriminants via Example 1.2.11. Of course, there are other quadratic fields with class number 1, see the subsequent example.

Example 1.7.2. Let $K = \mathbb{Q}(\sqrt{-19})$. Here, $n = 2$, $s = 1$ and since $-19 \equiv 1 \bmod 4$, we have $\mathcal{O}_K = (1 + \sqrt{-19})/2$ and $\text{disc}(K) = -19$. Thus, the Minkowski bound is ≈ 2.77, so we only need to check how (2) factors in $\mathcal{O}_K$. For this, we use Dedekind-Kummer: the minimal polynomial of $(1 + \sqrt{-19})/2$ is $T^2 - T + 5$ and reducing this mod 2 gives $T^2 - T + 1$ which is irreducible over $\mathbb{Z}/2\mathbb{Z}$. Hence, (2) remains prime in $\mathcal{O}_K$, so the class group $\text{Cl}(K)$ is trivial.

Example 1.7.3. Let $K = \mathbb{Q}(\sqrt{10})$. Here, $n = 2, s = 0$ and $\text{disc}(K) = 40$, so that the Minkowski bound is ≈ 4.16. Using Dedekind-Kummer, we study the primes lying over 2 and 3:

p	$T^2 + 10 \pmod p$	$p\mathcal{O}_K$
2	T^2	$\mathfrak{p}_2^2$
3	$T^2 + 1$ irred.	prime

Thus, the class group of K is generated by $[\mathfrak{p}_2]$. We check if $\mathfrak{p}_2$ is principal: suppose $\mathfrak{p}_2 = (a + b\sqrt{10})$ for some $a, b \in \mathbb{Z}$. Then we would have $a^2 - 10b^2 = \pm 2$ (since $N(\mathfrak{p}_2^2) = N(2) = 4$). Reducing both sides of this modulo 5, we obtain $a^2 = \pm 2 \bmod 5$, contradiction. Hence, $\text{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Example 1.7.4. Let $K = \mathbb{Q}(\sqrt{-21})$. We will show that $\text{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Here, $n = 2$, $s = 1$ and $\text{disc}(K) = -84$. Hence, the Minkowski bound is ≈ 5.83 so we only need to check the primes lying over 2, 3 and 5. Again, using Dedekind-Kummer, we make the following table:

p	$T^2 + 21 \pmod p$	$p\mathcal{O}_K$
2	$(T-1)(T+1)$	$\mathfrak{p}_2\mathfrak{p}_2'$
3	T^2	$\mathfrak{p}_3^2$
5	$(T-2)(T-3)$	$\mathfrak{p}_5\mathfrak{p}_5'$

Note that in the table, the factorization of $p\mathcal{O}_K$ corresponds to the factorization of $T^2 + 21$ mod p left-to-right, i.e. $\mathfrak{p}_2$ is the ideal $(3, \sqrt{-21} - 1)$. All three of $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$ are nonprincipal, since for $a, b \in \mathbb{Z}$, $N(a + b\sqrt{-21}) = a^2 + 21b^2$ cannot be equal to 2, 3 or 5. Moreover, since $N(3 + \sqrt{-21}) = 30 = 2 \cdot 3 \cdot 5$, $(3 + \sqrt{-21}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Thus, in the class group $[\mathfrak{p}_2][\mathfrak{p}_5] = [\mathfrak{p}_3]^{-1}$, so that $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$ generate the class group. Since $\mathfrak{p}_3^2 = (3)$ is principal, we have $[\mathfrak{p}_3] = [\mathfrak{p}_3]^{-1}$. Consequently, the relation $[\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5] = 1$ can be rewritten as $[\mathfrak{p}_2\mathfrak{p}_5] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3]$. As we have seen already, $\mathfrak{p}_3$ is not principal, so this implies $[\mathfrak{p}_2] \neq [\mathfrak{p}_5]$. Finally, we want to show both $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$ have order 2. Note that $N(2 + \sqrt{-21}) = 25$ and 5 does not divide $2 + \sqrt{-21}$, so $(2 + \sqrt{-21})$ must be divisible by one of either $\mathfrak{p}_5$ or $\mathfrak{p}_5'$ (since they are conjugate ideals). Let $\mathfrak{p}_5$ be that prime, so that $(2 + \sqrt{-21}) = \mathfrak{p}_5^2$. Thus, the ideal class $[\mathfrak{p}_5]$ has order 2, but since both $[\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$ have order 2, it follows that that $[\mathfrak{p}_2]$ also has order 2. Hence, $\text{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remark 1.7.5. The first two examples above yield 5 imaginary quadratic fields with class number 1. As we have

said, there are in fact only 9 such fields; the other 4 are $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67}$, $\mathbb{Q}(\sqrt{-163})$. It is easy to show these 9 fields have class number 1, but it is quite hard to show these are all such imaginary fields. Baker and Stark independently proved this fact in 1967. See [17, Chapter 12E] for a proof along Stark's lines using modular forms.

Chapter 2

Class field theory lite

In this chapter, we give a short introduction to class field theory. The main theme of class field theory is that abelian extensions L/K of a number field K can be characterized via the arithmetic of K. In our context, the 'arithmetic of K' shall loosely be defined as the study of the objects that arise from the free abelian group I_K generated by the prime ideals of $\mathcal{O}_K$, such as its subgroups and factor groups (eg. P_K, $\mathrm{Cl}(K)$, U_K).

Section 2.1 can be thought of as a continuation of section 1.6 – here we study ramification further in the situation where L/K is a Galois extension of number fields, defining two objects, the decomposition and inertia groups. Essentially this section can be thought of as the Galois theory of prime decomposition (cf. Theorem 2.1.4).

In section 2.2, we provide some motivation for the themes of class field theory by introducing the Kronecker-Weber theorem (Theorem 2.2.1) that says every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension field $\mathbb{Q}(\zeta_n)$, and using it to study the abelian extensions of $\mathbb{Q}$.

Section 2.3 generalises the setup of section 2.2 by defining the Artin map, which is a homomorphism from the ideal group I_K to the Galois group of a finite abelian extension of number fields L/K. To each prime ideal, it assigns the corresponding Artin symbol, which describes (in a way that we will make explicit later) how that prime ideal factors in L. Later, we define the Hilbert class field $\mathbb{H}(K)$ of a number field K, and establish an isomorphism between the Galois group of the Hilbert class field $\mathrm{Gal}(\mathbb{H}(K)/K)$ and the class group $\mathrm{Cl}(K)$. Finally, in section 2.4, we discuss the Chebotarev density theorem, an application of the theorems of class field theory that describes the density of the primes that split in a given extension of number fields L/K.

Section 2.1 is adapted from the material of Marcus [33, Chapter 4] and Neukirch [42, Chapter I, §9], the remaining sections are loosely based on these notes by Kedlaya [29, Chapter 1] and Cox's 'Primes of the form $x^2 + ny^2$' [17, Chapter 8]. For historical context on the development of class field theory and a more detailed summary (than we present here), we encourage the reader to look at 'Class field theory summarized' by Garbanati [22]. Alternatively, this excellent article [32] by Stevenhagen and Lenstra provides an elementary introduction to the contents of sections 2.2 and 2.3.

Class field theory is a (notoriously) difficult subject, and establishing even the basic theorems in detail

would take up much space, so by necessity we are quite brief[1]. Throughout this chapter, the focus is on explaining through examples, so we often provide only sketches of proofs or omit them entirely.

2.1 The decomposition and inertia groups

Notation. Let L/K be a Galois extension of number fields with $[L:K] = n$. Denote the Galois group of the number field extension $\mathrm{Gal}(L/K)$ as G. As in section 1.6, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then when viewed as an ideal in $\mathcal{O}_L$, $\mathfrak{p}\mathcal{O}_L$ factors uniquely into prime ideals as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

In what follows, we fix $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal and $\mathfrak{P} \subset \mathcal{O}_L$ a prime ideal lying over $\mathfrak{p}$. Finally, we let $\overline{G}$ denote the Galois group of the residue field extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$.

Recall from section 1.6 and in particular Lemma 1.5.4 that G acts transitively on the set of primes lying over $\mathfrak{p}$. For each prime $\mathfrak{P} \subset \mathcal{O}_L$ lying over $\mathfrak{p}$, we define the *decomposition group* $D_{\mathfrak{P}|\mathfrak{p}}$ as the stabilizer of this action with respect to $\mathfrak{P}$. Explicitly, this is the subgroup of G given by

$$D_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

When the ideals $\mathfrak{P} \mid \mathfrak{p}$ are clear from context, we will omit the subscript. The decomposition group describes how $\mathfrak{p}$ 'decomposes' (that is, factors) in $\mathcal{O}_L$: note by the orbit-stabilizer formula, we can compute the number of prime ideals lying over $\mathfrak{p}$ from the size of the decomposition group, because $r = |G|/|D_{\mathfrak{P}|\mathfrak{p}}| = [L:K]/|D_{\mathfrak{P}|\mathfrak{p}}|$.

Example 2.1.1. Let $f(X) = X^3 + 3X + 1$. Note that $f(X)$ is irreducible over $\mathbb{Q}$ (eg. because it is irreducible modulo 3), and denote the splitting field of f over $\mathbb{Q}$ by K. Let $K = \mathbb{Q}(\alpha)$, then α has minimal polynomial $X^6 + 18X^4 + 81X^2 + 135$ using PARI's `nfsplitting`. The discriminant of f is -135, so the Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ (see [38, p. 49]).

- Consider $p = 5$. The minimal polynomial of α factors modulo 5 as $X^6 + 18X^4 + 81X^2 + 135 \equiv X^2(X-1)^2(X+1)^2$, so Dedekind-Kummer implies that $5\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$. In particular, we have $r = 3$, which implies D has order $6/3 = 2$, whence $D \cong \mathbb{Z}/2\mathbb{Z}$.
- Consider $p = 3$. Here, $X^6 + 18X^4 + 81X^2 + 135 \equiv X^6 \bmod 3$, so $e = 6$ and $f = 1$. Since $r = 1$, the decomposition group must have size $[K:\mathbb{Q}]$, so $D = \mathrm{Gal}(K/\mathbb{Q})$.

The following proposition relates the decomposition groups of different prime ideals $\mathfrak{P}, \mathfrak{P}'$ lying over the same $\mathfrak{p}$.

Proposition 2.1.2. Let $\mathfrak{P}, \mathfrak{P}' \subset \mathcal{O}_L$ be two distinct prime ideals lying over $\mathfrak{p} \subset \mathcal{O}_K$. Then, the groups $D_{\mathfrak{P}|\mathfrak{p}}$ and $D_{\mathfrak{P}'|\mathfrak{p}}$ are conjugate by some element $\sigma \in \mathrm{Gal}(L/K)$.

Proof. By Lemma 1.5.4, there is a $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Let $\tau \in D_{\mathfrak{P}'|\mathfrak{p}}$, then we have the equalities

$$\sigma(\mathfrak{P}) = \mathfrak{P}' = \tau(\mathfrak{P}') = (\tau \circ \sigma)(\mathfrak{P})$$

[1] We also keep the language simple by ignoring ideles and adeles.

which shows that $\sigma^{-1}\tau\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$, so that $\sigma^{-1}D_{\mathfrak{P}'|\mathfrak{p}}\sigma \subseteq D_{\mathfrak{P}|\mathfrak{p}}$. The reverse inclusion follows similarly. $\square$

Proposition 2.1.2 implies for instance that if the Galois group $\mathrm{Gal}(L/K)$ is abelian, then we have equality $D_{\mathfrak{P}|\mathfrak{p}} = D_{\mathfrak{P}'|\mathfrak{p}}$. Note that in this case, the decomposition group depends entirely on $\mathfrak{p}$ and not the ideal(s) lying over it.

The automorphisms in the decomposition group $D_{\mathfrak{P}|\mathfrak{p}}$ induce automorphisms of the residue field $\mathcal{O}_L/\mathfrak{P}$. Any $\sigma \in G$ fixes K, and so must fix $\mathcal{O}_K$ and consequently $\mathcal{O}_K/\mathfrak{p}$. Moreover, we have seen already that σ restricts to a ring automorphism of $\mathcal{O}_L$, therefore also $\mathcal{O}_L/\mathfrak{P}$. The projection map $\pi : \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$ has kernel $\mathfrak{P}$, thus any $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$ induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}$, in such a way that the following diagram commutes

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \mathcal{O}_L/\mathfrak{P} & \xrightarrow[\overline{\sigma}]{} & \mathcal{O}_L/\mathfrak{P} \end{array}$$

Here, the vertical arrows represent projection maps. This means the elements of D (naturally) induce automorphisms of the residue field $\mathcal{O}_L/\mathfrak{P}$. Hence, this reduced homomorphism $\overline{\sigma}$ is an element of $\overline{G}$. We therefore obtain a map $D \to \overline{G}$ given by $\sigma \mapsto \overline{\sigma}$. This map is in fact a homomorphism, since the diagram above commutes.

We define a second group: the *inertia group* $E_{\mathfrak{P}|\mathfrak{p}}$, as the kernel of this homomorphism. This is the subgroup of D given by

$$E_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\}$$

By the first isomorphism theorem, we have an injective homomorphism of groups $D/E \to \overline{G}$. At the beginning of this chapter, we have said that this section can be thought of as the Galois theory of prime decomposition – concretely, this is because the homomorphism $D/E \to \overline{G}$ is in fact surjective, as we will see shortly.

Example 2.1.3. Let $f(X) = X^4 - X^3 + 2X + 1$. As in the previous example, we let K be the splitting field of f over $\mathbb{Q}$, and we write $K = \mathbb{Q}(\alpha)$, where α has minimal polynomial $X^8 - 6X^4 + 63X^2 + 9$. The Galois group of K is D_4 and its discriminant is $\mathrm{disc}(K) = 3^6 \cdot 7^4$.

- Consider $p = 3$. We have $X^8 - 6X^4 + 63X^2 + 9 \equiv X^4 \bmod 3$, so by Dedekind-Kummer, $3\mathcal{O}_K = \mathfrak{p}^4$ for a prime ideal $\mathfrak{p}$. We thus have $e = 4$ and $f = 2$. Thus, $D = \mathrm{Gal}(K/\mathbb{Q})$; since $D/E \cong \overline{G}$, we deduce that $E \cong \mathbb{Z}/2\mathbb{Z}$.
- Consider $p = 7$. We have $X^8 - 6X^4 + 63X^2 + 9 \equiv (X^2 + 2X + 2)^2(X^2 + 5X + 2)^2 \bmod 7$, so $e = 2$ and $f = 2$. Thus, $|D| = 4$ and $|E| = 2$. We deduce that $E \cong \mathbb{Z}/2\mathbb{Z}$, and since S_3 has no elements of order 4, $D \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since $E \subset D \subset G$, by Galois theory we have the field extensions $K \subset L^D \subset L^E \subset L$, where L^D, L^E are the fixed fields of D and E. Clearly, these are also number fields. To simplify the notation of the following theorem, we shall define the (unique) prime of L^E lying under $\mathfrak{P}$ by $\mathfrak{P}^E$ and similarly, the prime of L^D lying under $\mathfrak{P}^E$ is denoted $\mathfrak{P}^D$. Finally, let r be the number of primes lying over $\mathfrak{p}$ in L, $e = e_{\mathfrak{P}|\mathfrak{p}}$ and $f = f_{\mathfrak{P}|\mathfrak{p}}$. We can now state the main theorem of this section:

Theorem 2.1.4. The degrees of the Galois extensions L^D/K, L^E/L^D and L/L^E are r, f and e respectively. Moreover, we have the following ramification indices and inertial degrees:

	ramification index	inertial degree
$\mathfrak{P} \mid \mathfrak{P}^E$	e	1
$\mathfrak{P}^E \mid \mathfrak{P}^D$	1	f
$\mathfrak{P}^D \mid \mathfrak{p}$	1	1

Proof. See [33, Theorem 4.28]. □

Essentially, what the above is saying is that we can split up any extension of number fields into an unramified and a completely ramified part. We note some consequences of this theorem:

(1) We have the Galois groups $\mathrm{Gal}(L^E/L^D) \cong D/E$ and $\mathrm{Gal}(L/L^E) \cong E$.

(2) If $\mathfrak{p}$ is unramified, then $e = 1$ so $L^E = L$, and consequently E is trivial.

We illustrate the theorem with an example:

Example 2.1.5. We take K as in the previous example, that is K is the splitting field of $f(X) = X^4 - X^3 + 2X + 1$ over $\mathbb{Q}$. We have computed that $K = \mathbb{Q}(\alpha)$ with α a root of the irreducible polynomial $X^8 - 6X^4 + 63X^2 + 9$.

- For $p = 3$, $3\mathcal{O}_K = \mathfrak{p}^4$, so K^D has degree 1 over $\mathbb{Q}$, i.e. $K^D = \mathbb{Q}$. The extension K^E/K^D has degree $f = 2$, and PARI computes (using `galoisfixedfield`) $K^E = \mathbb{Q}(\sqrt{-7})$. Hence, we have the extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-7}) \subset K$, such that 3 is unramified in the first extension $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$ (as $3 \nmid 7 = \mathrm{disc}(K^E)$), and ramifies with $e = 4$ in the second extension $K/\mathbb{Q}(\sqrt{-7})$.
- For $p = 7$, we know $e = f = 2$ and the degree $[K : \mathbb{Q}] = 8$, so each extension $K^D/\mathbb{Q}$, K^E/K^D and K/K^E is quadratic. PARI computes $K^D = \mathbb{Q}(\sqrt{-3})$ and $K^E = \mathbb{Q}(\beta)$, where β is a root of the original polynomial $f(X) = X^4 - X^3 + 2X + 1$. Consequently, we have the tower of extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-3}) \subset \mathbb{Q}(\beta) \subset K$. The ring of integers of $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[(1 + \sqrt{-3})/2]$, and the minimal polynomial of $(1 + \sqrt{-3})/2$ is $X^2 - X + 1$, which factors as $X^2 - X + 1 \equiv (X + 2)(X + 4) \bmod 7$, so 7 indeed splits completely in $K^D/\mathbb{Q}$.

As a corollary to Theorem 2.1.4, we obtain the desired isomorphism $D/E \cong \overline{G}$.

Corollary 2.1.6. The homomorphism $D \to \overline{G}$ described above is surjective. Thus, $D/E \cong \overline{G}$.

Proof. Note that $|D/E| = [L^E : L^D] = f = |\overline{G}|$ by Galois theory, so indeed $D/E \cong \overline{G}$. □

In particular, $\overline{G}$ being an extension of finite fields is cyclic with order $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f$, hence D/E is cyclic of order f as well. When $\mathfrak{p}$ is unramified in L then $D \cong \overline{G}$, so D itself is cyclic of order f.

2.2 Abelian extensions of $\mathbb{Q}$

We say an *abelian extension* of a field is a Galois extension with abelian Galois group. One of the remarkable applications of class field theory is the Kronecker-Weber theorem, that characterizes the abelian extensions of $\mathbb{Q}$:

Theorem 2.2.1 (Kronecker-Weber)**.** Every abelian extension $K/\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$ for some n.

The smallest n such that $K \subset \mathbb{Q}(\zeta_n)$ is called the *conductor* of K.

Cyclotomic extensions. We briefly review the theory of the cyclotomic extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where ζ_n is a primitive n-th root of unity. See [16] for proofs of these facts. First, note that this extension is Galois, as $\mathbb{Q}(\zeta_n)$ is the splitting field of $X^n - 1$ over $\mathbb{Q}$. Moreover, recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and the extension degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is $\varphi(n)$, where φ is Euler's totient function. The minimal polynomial of ζ_n over $\mathbb{Q}$ is the n-th cyclotomic polynomial $\Phi_n(X)$:

$$\Phi_n(X) = \prod_{\substack{m \le n-1 \\ \gcd(m,n)=1}} (X - \zeta_n^m)$$

The compositum of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$ equals $\mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)})$ and the intersection $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\gcd(m,n)})$. In particular, if $\gcd(m,n) = 1$, then $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Before getting to the main results of this section, we will need a result about ramification in abelian extensions of the form $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_m)$ that are guaranteed by the Kronecker-Weber theorem. This is the following:

Theorem 2.2.2. Let $K/\mathbb{Q}$ be an abelian extension with conductor n. Then, a prime $p \in \mathbb{Z}$ ramifies in K if and only if it ramifies in $\mathbb{Q}(\zeta_n)$.

We prove this proposition shortly. The ring of integers of $\mathbb{Q}(\zeta_n)$ is very simple: just $\mathbb{Z}[\zeta_n]$. However, this is not easy to prove, see [42, Proposition 10.2] for a proof. Knowing this allows us to describe explicitly the factorization of $p\mathbb{Z}[\zeta_n]$ into prime ideals of $\mathbb{Q}(\zeta_n)$, using Theorem 1.5.6. This turns out to be a very nice description:

Proposition 2.2.3 ([42, Proposition 10.3])**.** Let $n = \prod p^{v_p}$ be the prime factorization of n. For every prime number p, let f_p denote the smallest positive integer such that

$$p^{f_p} \equiv 1 \pmod{n/p^{v_p}}.$$

Then, the factorization of p into prime ideals of $\mathbb{Q}(\zeta_n)$ is

$$p\mathbb{Z}[\zeta_n] = (\mathfrak{p}_1 \dots \mathfrak{p}_k)^{\varphi(p^{v_p})}$$

where the $\mathfrak{p}_j$ are distinct and each has inertial degree f_p over (p).

Proof. By the Dedekind-Kummer criterion (Theorem 1.5.6), since $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, we know every prime p factors in exactly the same way as the minimal polynomial of ζ_n factors into irreducibles modulo p. Therefore, it suffices to show that

$$\Phi_n(X) = (q_1(X) \dots q_k(X))^{\varphi(p^{v_p})} \pmod{p}$$

where the $q_i(X)$ are distinct and irreducible polynomials over $\mathbb{F}_p$ with degree f_p. Fix a $p \mid n$ and denote $n = p^{v_p} m$ where $p \nmid m$. Letting ζ_i vary over the primitive m-th roots of unity and η_j vary over the primitive

p^{v_p}-th roots of unity, one sees that the products $\zeta_i\eta_j$ vary over the primitive n-th roots of unity, because $\gcd(m, p^{v_p}) = 1$. Thus, we have the factorization

$$\Phi_n(X) = \prod_{i,j}(X - \zeta_i\eta_j)$$

Observe that we have the Frobenius identity $X^{p^{v_p}} - 1 \equiv (X-1)^{p^{v_p}} \bmod p$ in characteristic p, which implies in particular that $\eta_j - 1 \equiv 0 \bmod p$. In particular, for any prime ideal $\mathfrak{p} \mid p$, this means that $\eta_j \equiv 1 \bmod \mathfrak{p}$. Reducing the above factorization mod $\mathfrak{p}$ yields

$$\Phi_n(X) \equiv \prod_i (X - \zeta_i)^{p^{v_p}} \equiv \Phi_m(X)^{\varphi(p^{v_p})} \pmod{\mathfrak{p}}$$

where the first equality follows by collecting the number of times the same ζ_i appears in the factorization, and the second by our earlier observation. It follows that without loss of generality, we can discard the case $p \mid n$, since by the above it reduces to the case $p \nmid n$. Henceforth, assume $p \nmid n$.

By assumption, the characteristic p of $\mathbb{Z}[\zeta_n]/\mathfrak{p}$ does not divide n. This implies the polynomials $X^n - 1$ and its derivative nX^{n-1} do not share a root modulo $\mathfrak{p}$, whence $X^n - 1$ has no multiple roots modulo $\mathfrak{p}$. Hence, passing to the quotient ring $\mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_n]/\mathfrak{p}$ maps the n-th roots of unity bijectively onto the n-th roots of unity modulo $\mathfrak{p}$, because there are no roots that are the same modulo $\mathfrak{p}$. In particular, a primitive n-th root of unity must remain a primitive n-th root of unity modulo $\mathfrak{p}$. The smallest field extension of $\mathbb{F}_p$ containing this root must be $\mathbb{F}_{p^{f_p}}$, because f_p is defined as the smallest positive integer such that $n \mid (p^{f_p} - 1) = |\mathbb{F}_{p^{f_p}}^\times|$. Thus, $\mathbb{F}_{p^{f_p}}$ is a splitting field for the reduced polynomial $\overline{\Phi}_n(X)$ modulo p; since $\Phi_n(X) \mid (X^n - 1) \bmod p$, Φ_n also has no multiple roots modulo $\mathfrak{p}$. If $\overline{\Phi}_n$ factors into irreducibles over $\mathbb{F}_p$ as

$$\overline{\Phi}_n(X) = \overline{q}_1(X) \dots \overline{q}_k(X)$$

then each $\overline{q}_i$ is the minimal polynomial of a primitive n-th root of unity in $\mathbb{F}_{p^{f_p}}^\times$. Thus, each $\overline{q}_i$ has degree f_p, and we are done. □

We emphasize two corollaries of this proposition:

Corollary 2.2.4. Let p be prime and $r \geq 1$. The only prime that ramifies in $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ is p itself, with $e = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}]$.

Proof. For any prime $q \neq p$, the proposition implies that $f_q = \phi(p^r) = p^{r-1}(p-1) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}]$, so q is unramified in $\mathbb{Q}(\zeta_{p^r})$. For p, we obtain that $f_p = 1$, so p ramifies with ramification index $e = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}]/f_p = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}]$. □

Corollary 2.2.5. A prime $p \in \mathbb{Z}$ ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p \mid n$.

Proof. If $p \mid n$, then $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_n)$. The previous corollary and Proposition 1.5.3 together imply that p ramifies in $\mathbb{Q}(\zeta_n)$. Conversely, suppose that p does not divide $n = \prod_i p_i^{v_i}$. Again by the previous corollary, this means p is unramified in $\mathbb{Q}(\zeta_{p_i^{v_i}})$ for each p_i: in particular, by Proposition 1.5.3 this means p cannot ramify in the compositum $\mathbb{Q}(\zeta_n)$. □

Using these results, we can finish the proof of Theorem 2.2.2.

Proof of Theorem 2.2.2. The forwards direction is straightforward: if p ramifies in K, it must ramify in $\mathbb{Q}(\zeta_n)$ by Proposition 1.5.3. The previous corollary then shows that $p \mid n$. Conversely, suppose p is unramified in K. We wish to show p is also unramified in $\mathbb{Q}(\zeta_n)$. Write $n = p^k m$ with $p \nmid m$. We claim that the inertia field (see Theorem 2.1.4) of p in $\mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_m)$. We know that p is unramified in $\mathbb{Q}(\zeta_m)$ since $p \nmid m$, so clearly $\mathbb{Q}(\zeta_m)$ is contained in the inertia field. To show $\mathbb{Q}(\zeta_m)$ is indeed the inertia field, it suffices to show p (more precisely, the primes lying over p in $\mathbb{Q}(\zeta_m)$) are ramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m)$ with trivial inertial degree. We have the sequence of inequalities

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] \geq e_{\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_m)} = e_{\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_m)} \cdot e_{\mathbb{Q}(\zeta_m)|\mathbb{Q}} = e_{\mathbb{Q}(\zeta_n)|\mathbb{Q}} \geq e_{\mathbb{Q}(\zeta_{p^k})|\mathbb{Q}} = [\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] \tag{1}$$

where all the ramification indices are at the primes lying over p, the subscripts denoting in which field extension the prime ideals are. The first equality follows since p is unramified in $\mathbb{Q}(\zeta_m)$ by Corollary 2.2.4 and the second equality follows by Proposition 1.5.3. The final inequality follows as $\mathbb{Q}(\zeta_{p^k})$ is a subextension of $\mathbb{Q}(\zeta_n)$ as $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_{p^k})$. Since $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_{p^k})$ and m and p^k are coprime, we can also deduce that

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] = [\big(\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_{p^k})\big) : \mathbb{Q}(\zeta_m)] = [\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{p^k})] = [\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}]$$

This implies the inequalities in (1) are actually equalities. In particular, $e_{\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_m)} = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)]$ for p, which shows our claim. By assumption, p is unramified in K, so $K \subset \mathbb{Q}(\zeta_m)$, whence $n = m$ and $p \nmid n$, which completes the proof. □

Using the Kronecker-Weber theorem, we can obtain strong results about how the primes of $\mathbb{Q}$ factor in an abelian extension. In what follows, we will define the *Artin map* in this special case and convey its usefulness via some examples.

Let $K/\mathbb{Q}$ be an abelian extension with conductor m. Galois theory implies that K is the fixed field of some subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, denote this subgroup by $I_{K,m}$. Moreover, there is a surjective homomorphism $\beta : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q})$, given by restriction $\sigma \mapsto \sigma|_K$.
Suppose p is a prime with $p \nmid m$. Then, p is unramified over $\mathbb{Q}(\zeta_m)$ and consequently over K (Proposition 1.5.3). Since $K/\mathbb{Q}$ is an abelian extension, it makes sense to talk about the decomposition group of p itself: since p is unramified in K, the corresponding inertia group E is trivial. This means that we have an isomorphism $D \cong \overline{G} = \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ by Corollary 2.1.6, where $\mathfrak{p}$ is a prime lying over (p) (it does not matter which $\mathfrak{p}$ we pick as $K/\mathbb{Q}$ is abelian). Recall that $\overline{G}$ is the Galois group of an extension of finite fields, and is thus cyclic, generated by the Frobenius automorphism. In particular, $D \cong \overline{G}$ is generated by a 'Frobenius element' F_p, such that $F_p(x) \equiv x^p \bmod \mathfrak{p}$ for any $\mathfrak{p}$ lying over (p), i.e., F_p induces the Frobenius automorphism on the residue field $\mathcal{O}_K/\mathfrak{p}$. We thus obtain a map $p \mapsto F_p$ for each prime p unramified in K.

Let us denote the subgroup of $I_\mathbb{Q}$ generated by the prime ideals unramified in K as $I_\mathbb{Q}^{\mathrm{un}}$. Note by Theorem 2.2.2 these are exactly the prime ideals unramified in $\mathbb{Q}(\zeta_m)$, and moreover there is an isomorphism $I_\mathbb{Q}^{\mathrm{un}} \to (\mathbb{Z}/m\mathbb{Z})^\times$ by sending $(a) \mapsto a \bmod m$ (cf. Corollary 2.2.5). We can now formally extend the map $p \mapsto F_p$ to a homomorphism from $I_\mathbb{Q}^{\mathrm{un}}$ to $\mathrm{Gal}(K/\mathbb{Q})$. Precisely, what this means is the following: take $(a) \in I_\mathbb{Q}^{\mathrm{un}}$, and let a have prime factorization $a = p_1 p_2 \dots p_n$ (where of course none of the p_i ramify in K,

cf. Theorem 1.5.8). Then

$$F_a = F_{p_1} \cdot F_{p_2} \dots F_{p_n}$$

Let us call this homomorphism the *Artin map* of $K/\mathbb{Q}$.

The point here is that this Artin map factors through the surjective homomorphism $\beta : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q})$. We claim that $\beta(p) = F_p$ for p prime with $p \nmid m$. Take $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $r \not\equiv p \bmod m$, and suppose $\beta(r) = F_p$. The image of r under β is the map that takes ζ_m to ζ_m^r. This is equal to F_p precisely when $\zeta_m^r \equiv \zeta_m^p \bmod \mathfrak{p}$ for some prime $\mathfrak{p}$ of K lying over p. Now, note that $x - \zeta_m$ is a factor of $\Phi_m(x)$, and in particular $1 - \zeta_m$ divides $\Phi_m(1)$ in $\mathbb{Z}[\zeta_m]$. However, $\Phi_m(x)$ divides the polynomial $\frac{x^m-1}{x-1} = 1 + x + x^2 + \dots + x^{m-1}$, and consequently, $1 - \zeta_m$ divides $1 + 1 + 1^2 + \dots + 1^{m-1} = m$ in $\mathbb{Z}[\zeta_m]$. Hence, the only primes dividing $1 - \zeta_m$ are the primes laying over m. Observe this argument works the same for any m-th root of unity chosen, not just ζ_m; in particular $\zeta_m^r - \zeta_m^p = \zeta_m^r(1 - \zeta_m^{p-r})$ is only divisible by primes laying over m, hence cannot be 0 modulo $\mathfrak{p}$, unless $p \equiv r \bmod m$. Thus, $\beta(p) = F_p$, as required.

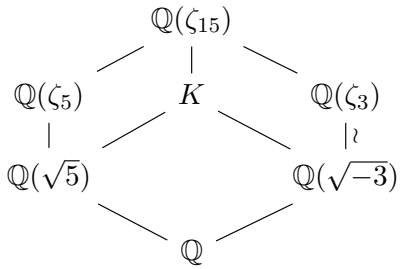
All together, this yields the following result:

Theorem 2.2.6 (Artin reciprocity for $\mathbb{Q}$)**.** Let $K/\mathbb{Q}$ be an abelian extension with conductor m. Then, we have the following exact sequence of groups:

$$1 \to I_{K,m} \to (\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q}) \to 1.$$

Thus, the Artin map induces an isomorphism between $(\mathbb{Z}/m\mathbb{Z})^\times / I_{K,m}$ and $\mathrm{Gal}(K/\mathbb{Q})$, and as we have noted, $(\mathbb{Z}/m\mathbb{Z})^\times$ is isomorphic to $I_{\mathbb{Q}}^{\mathrm{un}}$. A more high-level way to put this is that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ has been realized (canonically) in terms of the arithmetic of K. In addition to this explicit description of the Galois group, we can also describe the splitting behaviour of a prime p in K using the machinery established above.

Example 2.2.7 ([22])**.** Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$. We will use the Artin map to show that a prime $p \in \mathbb{Z}$ splits completely in K precisely when $p \equiv 1, 4 \bmod 15$. First, we will show that the conductor of K is 15. Note that K is the compositum of the fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-3})$. One sees that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ (because $\zeta_3 = (1+\sqrt{-3})/2$); furthermore, $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$, and $\mathbb{Q}(\sqrt{5})$ is not contained in any $\mathbb{Q}(\zeta_n)$ with $n < 5$, so $\mathbb{Q}(\sqrt{5})$ has conductor 5. As the compositum of $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-3})$, K is contained in the compositum $\mathbb{Q}(\zeta_5) \cdot \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_{15})$. This argument also shows $\mathbb{Q}(\zeta_{15})$ is the smallest cyclotomic extension containing K. We thus have the following lattice of fields:



We have $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_5)) \times \mathrm{Gal}(\mathbb{Q}(\zeta_3)) \cong \langle a \bmod 5 \rangle \times \langle b \bmod 3 \rangle$, where we have picked generators a, b of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)) \cong (\mathbb{Z}/5\mathbb{Z})^\times$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_3)) \cong (\mathbb{Z}/3\mathbb{Z})^\times$ respectively. The extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})$ is quadratic, so $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})) \cong \langle a^2 \bmod 5 \rangle$ (note a^2 has order 2). Since $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, by Galois

theory we obtain $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/K) \cong \langle a^2 \bmod 5\rangle \times \langle 1 \bmod 3\rangle$. Given a prime $p \in \mathbb{Z}$, we want to compute the order of the corresponding Frobenius element (cf. Proposition 2.3.2). By Artin reciprocity, this is the same as computing the order of $pI_{K,15}$ in $(\mathbb{Z}/15\mathbb{Z})^\times/I_{K,15}$. Picking an explicit generator $a = 3$, we obtain $I_{K,15} \cong \langle 4 \bmod 15\rangle$. We deduce that the Frobenius element corresponding to p is trivial precisely when $p \equiv 1, 4 \bmod 15$. That is, $p \in \mathbb{Z}$ splits completely in K if and only if $p \equiv 1, 4 \bmod 15$.

2.3 The main objects of class field theory

In this section, we define the Artin map associated with an extension of number fields L/K (satisfying certain conditions). This is a generalization of the Artin map from the previous section, although here the situation can become much more complicated, for the following reasons:

- We do not have an analogue of the Kronecker-Weber theorem classifying general abelian extensions of number fields L/K – the relative ease with which we have been able to construct the Artin map for abelian extensions $K/\mathbb{Q}$ is because ramification in K is governed by ramification in the cyclotomic field $\mathbb{Q}(\zeta_n)$ given by Kronecker-Weber. In the general setting, this becomes much more difficult, and in fact we will have to limit our attention to extensions where every prime is unramified.
- In general, a number ring $\mathcal{O}_K$ does not have to be a PID, as $\mathbb{Z}$ was, so we cannot simply pick a single generator for a prime ideal. Moreover, number rings $\mathcal{O}_K$ can have more units than just ± 1, even infinitely many: see Dirichlet's unit theorem. So even if a prime ideal is principal, it is not clear which generator should be chosen.

We also define the Hilbert class field $\mathbb{H}(K)$ of a number field K, the maximal unramified abelian extension of K. As we will see, the Hilbert class field is a natural construction to make in our context. The final result of this section (which we do not prove here) is the Artin reciprocity theorem, which says that $\mathrm{Cl}(K) \cong \mathrm{Gal}(\mathbb{H}(K)/K)$.

We introduce some definitions: in the previous section, we have been able to largely ignore infinite primes, but we will need to introduce them here. The prime ideals of $\mathcal{O}_K$ are referred to as finite primes or places. The *infinite primes* of $\mathcal{O}_K$ or K are defined based on the embeddings of $K \to \mathbb{C}$: a real infinite prime is a real embedding of K whereas a complex infinite prime is a conjugate pair of complex embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$. We say an infinite prime σ of K *ramifies* in L if σ is real but it has an extension to L that is complex. Note that under this definition complex infinite primes are always unramified.

Example 2.3.1. The only infinite prime of $\mathbb{Q}$ is the identity map $\mathbb{Q} \hookrightarrow \mathbb{C}$ (this is why we did not need to consider infinite primes in the previous section). This extends to complex conjugation in $\mathbb{Q}(\sqrt{-2})$, hence the infinite prime of $\mathbb{Q}$ ramifies in $\mathbb{Q}(\sqrt{-2})$. However, in $\mathbb{Q}(\sqrt{2})$, the infinite prime of $\mathbb{Q}$ is unramified.

2.3.1 The Artin map

The Frobenius automorphism. We begin by recalling the Frobenius automorphism from field theory. The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ for a prime p has cyclic Galois group of order n generated by the p-th power map $t \mapsto t^p$ on $\mathbb{F}_{p^n}$. In general, any extension of finite fields is of the form $\mathbb{F}_{q^n}/\mathbb{F}_q$ for $q = p^n$ a prime power; note the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a subgroup of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_p)$ by Galois theory, since $\mathbb{F}_q \supset \mathbb{F}_p$. Thus, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is itself cyclic, with order q^{n-1} and generator the q-th power map $t \mapsto t^q$. This generator is called the *Frobenius automorphism*, denoted Frob_q. See [38, p. 54] for a proof.

Notation. Let L/K be an extension of number fields with degree n and Galois group G. Let $\mathfrak{p}$ be a prime of K *unramified* in L with $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$. Denote by l/k the corresponding residue field extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ and its Galois group as $\overline{G}$. Recall that this is an extension of finite fields.

We define the *Artin symbol* $(L/K, \mathfrak{P})$ to be the element of G that acts as the Frobenius automorphism on the residue field extension l/k. Explicitly, this means that

(1) $(L/K, \mathfrak{P})(\mathfrak{P}) = \mathfrak{P}$,

(2) For all $\alpha \in \mathcal{O}_L$, $(L/K, \mathfrak{P})(\alpha) \equiv \alpha^q \bmod \mathfrak{P}$, where $q = |k|$ the size of the residue field.

Any automorphism that satisfies the first condition must be an element of $D_{\mathfrak{P}|\mathfrak{p}}$ by definition. Furthermore, $\mathfrak{p}$ is unramified in L, so the inertia group $E_{\mathfrak{P}|\mathfrak{p}}$ is trivial and consequently $D_{\mathfrak{P}|\mathfrak{p}} \cong \overline{G}$ by Corollary 2.1.6. We have said that the Artin symbol acts as the Frobenius automorphism on l/k, which precisely means that the reduction of the Artin symbol via the isomorphism $\overline{G} \cong D_{\mathfrak{P}|\mathfrak{p}}$ (described in section 2.1) is the Frobenius automorphism, which is condition (2).

Essentially, what we are doing above is 'lifting' the Frobenius automorphism from the residue field extension. We summarize a few properties of the Artin symbol in the following proposition. Property (a) is of particular interest, as it shows how the Artin symbol of a prime describes how that prime factors.

Proposition 2.3.2.

(a) The Artin symbol is uniquely defined, and has order f in G. In particular, if $(L/K, \mathfrak{P}) = 1$, then $\mathfrak{p}$ splits completely.

(b) If $\sigma \in \mathrm{Gal}(L/K)$, then
$$\sigma \left(\frac{L/K}{\mathfrak{P}} \right) \sigma^{-1} = \left(\frac{L/K}{\sigma(\mathfrak{P})} \right)$$

Proof. (a) is proved via the isomorphism $D_{\mathfrak{P}|\mathfrak{p}} \cong \overline{G}$. Since $\overline{G}$ is cyclic with generator the Frobenius automorphism Frob_q, the element of $D_{\mathfrak{P}|\mathfrak{p}}$ corresponding to Frob_q under this isomorphism must also have order g: this element is the Artin symbol, so uniqueness follows. As in Proposition 2.2.3, if the Artin symbol is trivial, this means $f = 1$. Since we start with an unramified prime, $e = 1$ already and so $\mathfrak{p}$ splits completely in L. For (b), note that by Proposition 2.1.2, we have $\sigma(L/K, \mathfrak{P})\sigma^{-1} \in D_{\sigma(\mathfrak{P})|\mathfrak{p}}$. The Artin symbol $(L/K, \sigma(P))$ is unique by (a), so we only need to check if $\sigma(L/K, \mathfrak{P})\sigma^{-1}$ reduces to the Frobenius automorphism mod $\sigma(\mathfrak{P})$. However, this is straightforward: pick $\beta \in \mathcal{O}_L$ and set $\alpha = \sigma^{-1}(\beta)$. Then,

$$\sigma(L/K, \mathfrak{P})\sigma^{-1}(\beta) = \sigma(L/K, \mathfrak{P})(\alpha) \equiv \sigma(\alpha^q) = \beta^q \pmod{\sigma(\mathfrak{P})}$$

and we are done. □

We compute the Artin symbol in some familiar examples:

Example 2.3.3. (a) Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, and let $p \in \mathbb{Z}$ be a prime unramified in K. Since $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, we can identify it with $\{\pm 1\}$. Then, the Artin symbol corresponding to p is either $+1$ or -1 depending on whether p splits or stays inert in K (if p splits as $\mathfrak{p}\mathfrak{p}'$, the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ takes $\mathfrak{p} \to \mathfrak{p}'$). This is the content of Corollary 1.5.10 and the subsequent remark.

(b) Let $K = \mathbb{Q}(\zeta_n)$ with ζ_n a primitive n-th root of unity. Take $p \in \mathbb{Z}$ prime with $p \nmid n$, as otherwise p ramifies in K by Corollary 2.2.5. Let $\mathfrak{p}$ be a prime lying over p and denote $\sigma = (L/K, \mathfrak{P})$ to be the corresponding Artin symbol. We claim σ is such that $\sigma(\zeta_n) = \zeta_n^p$. A $\mathbb{Z}$-basis of $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ is given by $1, \zeta_n, \ldots, \zeta_n^{n-1}$, and so taking an arbitrary element of $\mathcal{O}_K$ we have

$$\left(\sum_{i \leq n} a_i \zeta_n^i\right)^p \equiv \sum_{i \leq n} a_i^p \zeta_n^{ip} \equiv \sum_{i \leq n} a_i \zeta_n^{ip} = \sigma\left(\sum_{i \leq n} a_i \zeta_n^i\right) \bmod \mathfrak{p}$$

where the second congruence follows because we are in characteristic p, and the third equality follows since σ reduces to the Frobenius automorphism modulo $\mathfrak{p}$. From this, our claim follows. This is exactly what we have computed in the previous section.

We discuss briefly why we need $\mathfrak{p}$ to be unramified in L. In showing uniqueness of the Artin symbol, we have used the fact that $D_{\mathfrak{P}|\mathfrak{p}} \cong \overline{G}$, which is *not* true if $\mathfrak{p}$ ramifies in L. If $\mathfrak{p}$ ramifies in L, the corresponding inertia group $E_{\mathfrak{P}|\mathfrak{p}}$ is nontrivial, which means we cannot 'lift' the Frobenius automorphism from $\mathrm{Gal}(l/k)$ as we have done earlier (at least not in a well-defined way). This is one reason why class field theory is so difficult to develop in the general case; one needs to get around this issue somehow. This can be done by introducing the language of ideles and adeles, see [42, Chapter 6].

As in the preceding section, we would like to formally extend the Artin symbol to a map $I_K \to \mathrm{Gal}(L/K)$. However, in a general abelian extension L/K, we do not have the Kronecker-Weber theorem. Hence, we need to generalize the machinery of the previous section: we need suitable analogues for the 'conductor of L' and the Galois group $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

We define a *modulus* $\mathfrak{m}$ for K as a formal product

$$\prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$$

over all primes $\mathfrak{p}$ of K, finite or infinite. Here, the $n_\mathfrak{p}$ are non-negative with at most finitely many nonzero; if $\mathfrak{p}$ is a complex infinite prime $n_\mathfrak{p} = 0$, and if $\mathfrak{p}$ is a real infinite prime, $n_\mathfrak{p} \leq 1$. If all the $n_\mathfrak{p} = 0$, we set $\mathfrak{m} = 1$. Thus, we may regard a modulus $\mathfrak{m}$ as a product $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0 \subset \mathcal{O}_K$ is an integral ideal and $\mathfrak{m}_\infty$ is a (formal) product of distinct real infinite places of K. This is the right generalization of the conductor from the previous section (cf. Corollary 2.2.5).

Example 2.3.4. Let $K = \mathbb{Q}(\sqrt{-2})$, and define $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ where $n_\mathfrak{p} = 1$ for $\mathfrak{p} = (2), (3)$ and the real infinite prime of $\mathbb{Q}$, and zero elsewhere. We can write $\mathfrak{m} = (6)\infty$, where ∞ denotes the real infinite prime of $\mathbb{Q}$.

The modulus allows us to generalize the usual class group. Define $I_K^\mathfrak{m}$ be the group of fractional ideals of K coprime to each finite prime occuring in the product $\mathfrak{m}$. Let $P_K^\mathfrak{m}$ be the subgroup of $I_K^\mathfrak{m}$ consisting of principal fractional ideals generated by elements $\alpha \in K^\times$ satisfying:

(1) for any finite prime power $\mathfrak{p}^e \mid \mathfrak{m}$, we have $\alpha \equiv 1 \bmod \mathfrak{p}^e$ and,

(2) for any real infinite prime σ appearing in $\mathfrak{m}$, $\sigma(\alpha) > 0$.

The *ray class group* $\mathrm{Cl}^\mathfrak{m}(K)$ is defined as the quotient $I_K^\mathfrak{m}/P_K^\mathfrak{m}$.

These definitions allow us to set up the Artin map in this general setting where L/K be an abelian extension of number fields. Note that since $\mathrm{Gal}(L/K)$ is abelian, as in the previous section it makes sense to talk about the Artin symbol of $\mathfrak{p}$ for a prime $\mathfrak{p}$ of K; let us write this as $(L/K, \mathfrak{p})$. For $\mathfrak{m}$ divisible by each prime of K that ramifies in L, we define the Artin map to be the homomorphism

$$I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K), \qquad \mathfrak{p} \mapsto (L/K, \mathfrak{p})$$

Since $I_K^{\mathfrak{m}}$ consists of the ideals coprime to the finite primes of $\mathfrak{m}$, it contains in particular the primes of K that are unramified in L. In the special case where $K = \mathbb{Q}$, this is exactly the Artin map of the previous section. With this, we can state the appropriate generalization of Theorem 2.2.6:

Theorem 2.3.5 (Artin reciprocity)**.** There exists a modulus $\mathfrak{m}$, including all (finite and infinite) primes that ramify in L, such that $P_K^{\mathfrak{m}}$ is contained in the kernel of the Artin map.

Proof. See [42, Chapter 6, Theorem 5.5]. □

In particular, we obtain a homomorphism $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ that is in fact surjective (see section 2.4). The smallest formal product $\mathfrak{m}$ for which Artin reciprocity holds is called the *conductor* of L/K. We say L/K is the *ray class field* corresponding to the modulus $\mathfrak{m}$ if L/K has conductor dividing $\mathfrak{m}$ and the map $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is an isomorphism. In fact we have the following:

Theorem 2.3.6 (Existence)**.** For any modulus $\mathfrak{m}$, there exists a corresponding ray class field.

Proof. See [42, Chapter 6, Theorem 6.1]. □

This statement motivates the construction of the Hilbert class field, which we explore in the following section.

2.3.2 The Hilbert class field

One says an extension L/K is *unramified* if it is unramified at all primes (finite and infinite) of K.

Example 2.3.7.

(a) $\mathbb{Q}$ has no unramified extensions. This is the content of Corollary 1.5.9.

(b) Let $K = \mathbb{Q}(\sqrt{-5})$ and $L = K(i)$. We have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and by an application of Dedekind-Kummer, $2\mathcal{O}_K$ factors as $\mathfrak{p}^2$, where $\mathfrak{p} = (2, 1 + \sqrt{-5})$. Note that in L/K, the only prime that can ramify is 2, which can be seen in 2 ways. First, the only prime that ramifies in $\mathbb{Q}(i)/\mathbb{Q}$ is 2, so the only prime that can ramify in L/K is the prime lying over 2 in K; second, we could compute the relative discriminant $\mathrm{disc}(L/K)$ (see Remark 1.2.12) and use Theorem 1.5.8. We can write $L = K(\alpha)$ where $\alpha = (1 + \sqrt{5})/2$; α has minimal polynomial $x^2 - x - 1$, which remains irreducible modulo $\mathfrak{p}$. All the embeddings $K \to \mathbb{C}$ are complex, hence L/K is an unramified extension.

In the previous section, we have said that there exists a ray class field corresponding to any modulus $\mathfrak{m}$. What happens if we take $\mathfrak{m}$ to be an empty formal product? This happens eg. if we consider an unramified abelian extension L/K, because then Artin reciprocity yields an isomorphism $\mathrm{Cl}(K) \to$

$\mathrm{Gal}(L/K)$. Motivated by this, we define the *Hilbert class field* $\mathbb{H}(K)$ of K to be the maximal unramified abelian extension of K.

Corollary 2.3.8. Given a number field K, its Hilbert class field exists, and moreover one has the isomorphism $\mathrm{Gal}(\mathbb{H}(K)/K) \cong \mathrm{Cl}(K)$.

Proof. Both these assertions follow from the Existence theorem of the previous section with $\mathfrak{m} = 1$. □

This is why class field theory is so named – it is the theory dealing with 'class fields' such as the Hilbert class field and the ray class fields defined earlier.

Example 2.3.9. (a) By Artin reciprocity, the degree of $\mathbb{H}(K)$ over K is equal to $h(K)$. Thus, any number field with $h(K) = 1$ has $\mathbb{H}(K) = K$.

(b) Let $K = \mathbb{Q}(\sqrt{-5})$. We have seen that $L = \mathbb{Q}(\sqrt{-5}, i)$ is an unramified extension of K; moreover L/K is abelian as a quadratic extension. In fact, L is the Hilbert class field of K (see [37, Remark 4.11] and the corresponding footnotes).

While the failure of unique factorization in an arbitrary number ring is not ideal, it does raise the following question: can any number field K be embedded into a number field L with class number 1? More precisely, does there exist a finite extension L/K such that $h(L) = 1$? The answer to this question is intimately related to the Hilbert class field, as we will see in Chapter 5.

2.4 The Chebotarev density theorem

In this section, we briefly discuss the Chebotarev density theorem. In the previous section, we have seen how to associate the Artin symbol, which is an element of $\mathrm{Gal}(K/\mathbb{Q})$ to each unramified prime of an abelian extension $K/\mathbb{Q}$. We would now like to ask if given an element in $\mathrm{Gal}(K/\mathbb{Q})$, whether it is the Artin symbol of some prime. First, we define the notion of *natural density*: let S be a set of finite primes of a number field K. One says S has natural density δ if

$$\lim_{n\to\infty} \frac{|\{\mathfrak{p} \in S \mid N(\mathfrak{p}) \leq n\}|}{|\{\mathfrak{p} \mid N(\mathfrak{p}) \leq n\}|} = \delta$$

We are now ready to state Chebotarev's density theorem.

Theorem 2.4.1 (Chebotarev density)**.** Let L/K be a Galois extension of number fields and let $C \subset G = \mathrm{Gal}(L/K)$ be some conjugacy class of G. Then, the set

$$\{\mathfrak{p} \text{ prime of } K \mid \mathfrak{p} \text{ unramified}, \ (L/K, \mathfrak{p}) \in C\}$$

has natural density $|C|/|G|$.

Earlier, we have talked about the primes of K that split completely in L: in particular, we have seen that we can determine which primes split completely using the corresponding Artin symbols (cf. Example 2.2.7 and Proposition 2.3.2). It turns out that knowing which primes split in an extension is enough to determine the extension, which is shown by the following theorem.

Theorem 2.4.2. Let K be a number field and suppose L and M are Galois over K. Denote the set of primes of K that split in L as $\mathrm{Spl}(L/K)$. Then, we have

$$L \subset M \iff \mathrm{Spl}(L/K) \supset \mathrm{Spl}(M/K)$$

Proof. See [37, Theorem 8.38]. □

This theorem says that the data given by the primes that split in an extension L/K characterizes the extension itself. This means that to characterize the Galois extensions of a number field K, it is enough to classify the primes which can split completely. For abelian extensions of K, the tools of class field theory allow us to characterize these primes by congruence conditions – the Artin symbol is defined via a congruence modulo $\mathfrak{p}$, and $\mathfrak{p}$ splits completely when its Artin symbol is trivial (cf. Example 2.2.7, where we get congruence conditions modulo 15).

We have said at the beginning of chapter 1 that the class group of K 'measures' how far $\mathcal{O}_K$ is from being a PID. Using the Chebotarev density theorem, we can make this vague statement concrete: by Artin reciprocity, we have the isomorphism $\mathrm{Cl}(K) \cong \mathrm{Gal}(\mathbb{H}(K)/K)$ given by the Artin map, which takes every prime $\mathfrak{p}$ to its corresponding Artin symbol. In particular, $(\mathbb{H}(K)/K, \mathfrak{p})$ is trivial precisely when $\mathfrak{p}$ is trivial in $\mathrm{Cl}(K)$, i.e. when $\mathfrak{p}$ is principal. Note that these are also the primes that split completely in $\mathbb{H}(K)$ by Proposition 2.3.2. Taking the conjugacy class $C = \{1\} \subset \mathrm{Gal}(\mathbb{H}(K)/K)$, Chebotarev density implies that the density of the primes $\mathfrak{p}$ with $(\mathbb{H}(K)/K, \mathfrak{p}) = 1$ is

$$\frac{1}{|\mathrm{Gal}(\mathbb{H}(K)/K)|} = \frac{1}{|\mathrm{Cl}(K)|} = \frac{1}{h(K)}.$$

Hence, the density of principal primes in K is the reciprocal of the class number of K. Since every ideal of $\mathcal{O}_K$ factors into prime ideals by Theorem 1.4.3, we see that the larger the class number, the 'more' prime ideals are not principal, whence 'more' ideals are not principal (Theorem 1.4.3).

Finally, we prove the Artin map is surjective using the Chebotarev density theorem. Fix an unramified abelian extension L/K, and note that L/K is abelian so each $\sigma \in \mathrm{Gal}(L/K)$ is its own conjugacy class. Chebotarev density implies that for each $\sigma \in \mathrm{Gal}(L/K)$, the set of primes $\mathfrak{p}$ of K with Artin symbol σ has density $1/|\mathrm{Gal}(L/K)|$, so there is at least one $\mathfrak{p}$ with $(L/K, \mathfrak{p}) = \sigma$. Hence, the Artin map is surjective.

Chapter 3

Divisibility by 2

In this chapter, we begin to discuss the problem of divisibility of class numbers of quadratic number fields. Here, we look at the simplest case – divisibility by 2, a case that was first treated by Gauss in his Disquisitiones Arithmeticae [23]. Our aim in this chapter is to show the following result:

Theorem 3.2.7. There are infinitely many quadratic number fields with even class number.

In the first section, we establish the theory of integral quadratic forms. This is a rather simple and elegant theory, and we provide many examples to illustrate our results. We also implement some algorithms in Python for computing with quadratic forms, see the appendix for the relevant code. The goal of this section is to put a abelian group structure on quadratic forms of a certain discriminant (see Theorem 3.1.14) and characterize when this group has an element of order 2 (Theorem 3.1.15).

The second section establishes a certain isomorphism between the class group of a quadratic number field $\mathrm{Cl}(K)$ and the group of reduced quadratic forms with discriminant $\mathrm{disc}(K)$ (Proposition 3.2.5). This isomorphism makes it easy to show the main result of this chapter – that there are infinitely many quadratic number fields with even class number. Indeed, this result follows as a corollary of the isomorphism, see Corollary 3.2.7.

The material of this chapter is sourced from chapters 3 and 7 of Cox's 'Primes of the form $x^2 + ny^2$' [17]. The reader is also encouraged to look Buell's 'Binary Quadratic Forms' [11], which the author found very helpful.

3.1 Quadratic forms

3.1.1 Basic definitions

A binary integral quadratic form is a homogenous polynomial of degree 2 over $\mathbb{Z}$ in two variables; that is, it is a polynomial of the form

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

with integer coefficients a, b, c. We say a quadratic form is *primitive* if $\gcd(a, b, c) = 1$. Note that any quadratic form is a multiple of a primitive one, by factoring out the gcd of the coefficients. For this reason, we typically assume forms are primitive by default unless otherwise stated.

Computing with quadratic forms directly can get quite cumbersome. Hence, for any quadratic form $f(x,y) = ax^2 + bxy + cy^2$, we define a corresponding matrix $M_f = \left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$. Then, we have

$$f(x,y) = \frac{1}{2}\begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$$

Example 3.1.1. Let $f(x,y) = 2x^2 + y^2$ be a quadratic form. This form is primitive as $\gcd(2,1) = 1$, and the associated matrix is $M_f = \left(\begin{smallmatrix} 4 & 0 \\ 0 & 2 \end{smallmatrix}\right)$.

A natural question to ask given a quadratic form is what values it can take. We say an integer m is *represented* by a quadratic form $f(x,y)$ if there exist integers x and y solving the equation

$$m = f(x,y).$$

The question of which primes can be represented by a given form (more generally, which numbers can be) is a classical one, and dates back to Fermat, who asked which primes can be represented as a sum of two squares $x^2 + y^2$. See the first chapter of [17] for a (quick) historical introduction.

Example 3.1.2. Consider as in the previous example $f(x,y) = 2x^2 + y^2$. Clearly, f represents 2 as $f(1,0) = 2$, but f does not represent 7 or -1.

We can define a notion of equivalence between quadratic forms. We say two forms $f(x,y)$ and $g(x,y)$ are *equivalent* if there are integers p, q, r and s such that

$$f(x,y) = g(px + qy, rx + sy)$$

with $ps - qr = \pm 1$. If $ps - qr = 1$, one says f and g are *properly equivalent.*

Example 3.1.3. The forms $f(x,y) = x^2 + 2xy + 3y^2$ and $g(x,y) = x^2 + 6y^2$ are equivalent under $(x,y) \mapsto (x + y, -y)$. We have $1(-1) - 1 \cdot 0 = -1$ so this is indeed a equivalence (but not a proper one).

Let $f(x,y) = ax^2 + bxy + cy^2$ and let g be a form equivalent to f, i.e. $g(x,y) = f(px + qy, rx + sy)$ with $ps - qr = \pm 1$. Defining the matrix $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$, we can see that $\det P = \pm 1$, so P is in particular invertible. We have

$$\begin{aligned} 2g(x,y) &= 2f(px + qy, rx + sy) \\ &= \begin{bmatrix} px + qy & rx + sy \end{bmatrix} M_f \begin{bmatrix} px + qy \\ rx + sy \end{bmatrix} \\ &= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix}^T M_f \begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \end{aligned}$$

so that

$$M_g = P^T M_f P.$$

Since P is invertible, the above shows that equivalent forms must represent the same numbers: suppose

two forms f and g are equivalent. If $g(x,y) = m$ for some x and y, then

$$m = \frac{1}{2}\begin{bmatrix} x & y \end{bmatrix} M_g \begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{2}\begin{bmatrix} x & y \end{bmatrix} P^T M_f P \begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{2}\left(P\begin{bmatrix} x \\ y \end{bmatrix}\right)^T M_f \left(P\begin{bmatrix} x \\ y \end{bmatrix}\right)$$

Example 3.1.4. The converse of the above does not hold: forms that represent the same integers need not be equivalent! A standard example is given by the forms $f(x,y) = x^2+xy+y^2$ and $g(x,y) = x^2+3y^2$. By completing the square on $f(x,y)$ one has $f(x,y) = (x+y/2)^2 + 3(y/2)^2$. Setting $u = x + y/2$ and $v = y/2$ we obtain $f(x,y) = u^2 + 3v^2$; it remains to show that y can always be chosen even. This is straightforward to do: note first that f is symmetric in x and y, i.e. $f(x,y) = f(y,x)$. Also note that $f(-x-y,y) = f(x,y)$: this means that if y is odd, we can always replace $f(x,y)$ with $f(y,x)$ or $f(y,-x-y)$ depending on whether x is even or odd. Hence, we can always pick y even, whence f and g represent the same numbers. However, they are not equivalent, see the following example.

We define the *discriminant* of a form $f(x,y) = ax^2 + bxy + cy^2$ to be $D = b^2 - 4ac$. The sign of D affects what numbers f can represent. In particular, we have the following identity

$$4af(x,y) = (2ax+by)^2 - Dy^2$$

Note from the above that if $D < 0$, then f can only represent either positive or negative numbers depending on the sign of a. In this case, we call f either *positive* or *negative definite* respectively. If $D > 0$, then f can represent both positive and negative numbers – in this case we say f is *indefinite.*

Example 3.1.5. The form $f(x,y) = x^2+xy+y^2$ of the previous example has discriminant -3 and is thus positive definite. The form $h(x,y) = x^2 + xy - y^2$ has discriminant 5 and is thus indefinite. Note that $g(x,y) = x^2 + 3y^2$ of the previous example has discriminant -12, and hence is not equivalent to f.

We make some useful observations about the discriminant. First, that the discriminant remains invariant under equivalence: suppose the forms f and g have discriminants D and D' respectively, and that f and g are equivalent as $f(x,y) = g(px+qy, rx+sy)$. We compute that $D = (ps-qr)^2 D'$, so indeed $D = D'$ when $ps - qr = \pm 1$.
Second, that $D = b^2 - 4ac \equiv b^2 \pmod 4$. Hence, the discriminant of a quadratic form can only be $0, 1 \pmod 4$. The converse is also true: every integer $D \equiv 0, 1 \pmod 4$ is the discriminant of some quadratic form. Define the *principal form* F_D of discriminant $D \equiv 0, 1 \pmod 4$ as

$$F_D(x,y) = \begin{cases} x^2 - \dfrac{D}{4}y^2, & D \equiv 0 \pmod 4 \\ x^2 + xy + \dfrac{1-D}{4}y^2, & D \equiv 1 \pmod 4 \end{cases} \tag{1}$$

It is easily seen that the form $F_D(x,y)$ has discriminant D.

3.1.2 Reduced forms

In this subsection, we work only with (primitive) positive definite forms. There is also a similar theory of reduced forms for indefinite forms, however the required modifications to the theory are not too difficult and in the interest of space we do not cover them in detail. Sticking to positive definite forms also makes the theory quite elegant, as we will see.

We say a primitive positive definite form $ax^2 + bxy + cy^2$ is *reduced* if

$$|b| \leq a \leq c, \quad \text{and} \quad b \geq 0 \text{ if } |b| = a \text{ or } a = c.$$

Example 3.1.6. The form $x^2 + xy + y^2$ has $|b| = a = c$, moreover $b \geq 0$ so it is reduced. The form $3x^2 + y^2$ is not reduced since $c < a$: however note that it is equivalent to the reduced form $x^2 + 3y^2$ via $(x, y) \mapsto (-y, x)$.

The following lemma gives a first characterization of the integers represented by a reduced form.

Lemma 3.1.7. Let $f(x, y) = ax^2+bxy+cy^2$ be a reduced form. Then, a is the smallest integer represented by f. Moreover, either c is the smallest integer represented by f that does not have the form ax^2, or $c = ax^2$ for some x and c is the smallest integer to be represented in two distinct ways by f.

Proof. Since f is reduced, note that we have $a \leq c$. We claim that if $f(x, y) < c$, then $y = 0$. Since f is reduced, we have $|b| \leq a$, so that

$$f(x, y) = ax^2 + bxy + cy^2 \geq ax^2 - a|xy| + cy^2 = a\left(|x| - \frac{|y|}{2}\right)^2 + \frac{3cy^2}{4} \geq 3c \quad \text{for} \quad |y| \geq 2$$

The only case left to check is when $|y| = 1$: in this case

$$f(x, y) \geq a(x^2 - |x|) + c \geq c$$

and it follows that if $f(x, y) < a \leq c$ then $y = 0$. The smallest value of $f(x, 0) = ax^2$ is at $x = \pm 1$, therefore a is the smallest integer represented by f. The second part of the lemma also follows from the above: if c is of the form ax^2 for some x, then $f(0, \pm 1) = f(\pm x, 0) = c$ and c is represented two different ways; otherwise c is the smallest integer not of the form ax^2 to be represented by f. □

As mentioned in the introduction to this section, our goal is to ultimately define a group structure on quadratic forms with discriminant D. In view of this, the main theorem of this subsection is as follows:

Theorem 3.1.8. Every primitive positive definite form is properly equivalent to a unique reduced form.

We separate the proof of Theorem 3.1.8 into two lemmas: Lemma 3.1.9 and Lemma 3.1.11. First we show that any form is properly equivalent to a reduced form – this is done in a constructive way, so the proof of Lemma 3.1.9 in fact yields an algorithm to compute the reduction of a given form. Second, we show in Lemma 3.1.11 that no two reduced forms can be properly equivalent, which finishes the proof. We begin with the first step.

Lemma 3.1.9. Every primitive positive definite form is properly equivalent to some reduced form.

Proof. From all the forms properly equivalent to the given one, pick $f(x, y) = ax^2 + bxy + cy^2$ such that $|b|$ is minimal. First we show that f satisfies $|b| \leq a \leq c$. By way of contradiction, suppose $a < |b|$. Then,

$$g(x, y) := f(x + my, y) = ax^2 + (2am + b)xy + c'y^2$$

is properly equivalent to f for any integer m. Since $a < |b|$ by assumption, we can choose m such that $|2am + b| < |b|$ (more precisely, we can pick $m = \lfloor \frac{a-b}{2a} \rfloor$), which contradicts the minimality of $|b|$. On the other hand, if $a > c$, we can simply interchange the outer coefficients. This is accomplished via the proper equivalence $(x, y) \mapsto (-y, x)$. The resulting form satisfies $|b| \leq a \leq c$ by construction.
The next step is to show this f is indeed properly equivalent to a reduced form. By definition, f is already reduced unless $b < 0$ and $a = -b$ or $a = c$. In this case, the form $f'(x, y) = ax^2 - bxy + cy^2$ would be a reduced form, so we only need to show f is properly equivalent to f'. We check each case: suppose first that $a = -b$. Then, the map $(x, y) \mapsto (x + y, y)$ is a proper equivalence taking $ax^2 - axy + cy^2$ to $ax^2 + axy + cy^2$. In the other case if $a = c$, we can interchange the outer coefficients as before via the proper equivalence $(x, y) \mapsto (-y, x)$. This completes the proof. □

As mentioned before, the proof of Lemma 3.1.9 provides an algorithm that takes any primitive positive definite form $f(x, y) = ax^2 + bxy + cy^2$ and returns a reduced form to which f is properly equivalent. We describe the algorithm below; see the appendix for an implementation in Python.

INPUT. A triple of integers (a, b, c) that defines the quadratic form.

0. If $D = b^2 - 4ac < 0$ continue to step 1, else stop here.
1. If $c < a$, replace (a, b, c) with the properly equivalent form $(c, -b, a)$.
2. If $|b| > a$, replace (a, b, c) with the properly equivalent form (a, b', c') where $b' = b + 2ma$ with $m = \lfloor \frac{a-b}{2a} \rfloor$, and c' is found via the discriminant $D = b^2 - 4ac = b'^2 - 4ac'$.
3. Repeat steps 1 and 2 until $|b| \leq a \leq c$.

Example 3.1.10. Let $g(x, y) = 17x^2 - 23xy + 13y^2$. We have $c < a$ so we perform step 1 and replace g with the equivalent form $13x^2 + 23xy + 17y^2$. Here, $|23| > 13$, so we perform step 2 and compute $m = -1$, so that $b' = -3$ and $c' = 7$. Once again, $13 = a > c' = 7$, so we swap a and c'. Hence, g is equivalent to the reduced form $7x^2 + 3xy + 13y^2$.

Next, we would like to show no two distinct reduced forms are properly equivalent. The key step in the proof is using the fact that properly equivalent forms must represent the same numbers, via Lemma 3.1.7.

Lemma 3.1.11. Two reduced forms cannot be properly equivalent.

Proof. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be two distinct reduced forms. Suppose f is properly equivalent to g. Since equivalent forms represent the same numbers, Lemma 3.1.7 implies that $a = a'$ and $c = c'$. Moreover, f and g are properly equivalent, so have the same discriminant. Thus, $b'^2 - 4a'c' = b^2 - 4ac$, which implies $b' = -b$ (since $f \neq g$). Suppose now that $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ is the matrix taking M_f to M_g. Then,

$$\begin{bmatrix} 2a & -b \\ -b & 2c \end{bmatrix} = P^T \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} P$$

so that $a = ap^2 + bpr + cr^2$, and a is represented by f in two ways. From Lemma 3.1.7, either $r = 0$ or $c = a$. We consider the first case: if $r = 0$, then $ps = 1$. From the above matrix equation, we have $-b = 2apq + qrb + psb + 2crs$, and if $r = 0$ then $-b = 2apq + b$, which implies $|b| = a$. Thus, either $|b| = a$ or $a = c$, and since $b' = -b$ only one of the two forms can be reduced. □

Example 3.1.12.

(a) The forms $3x^2 \pm 2xy + 5y^2$ are equivalent via the transformation $(x, y) \mapsto (-x, y)$. These forms are also both reduced, since $|2| < 3 < 5$. Lemma 3.1.11 now implies these two forms cannot be properly equivalent.

(b) The forms $2x^2 \pm 2xy + 3y^2$ are also equivalent under $(x, y) \mapsto (-x, y)$, but $2x^2 - 2xy + 3y^2$ is not reduced (because $|b| = a$ but $b < 0$). Lemma 3.1.9 implies that $2x^2 - 2xy + 3y^2$ is properly equivalent to the reduced form $2x^2 + 2xy + 3y^2$.

Together, Lemma 3.1.9 and Lemma 3.1.11 complete the proof of Theorem 3.1.8. Moreover, Theorem 3.1.8 allows us to deduce that there are finitely many equivalence classes of forms under proper equivalence. Let $ax^2 + bxy + cy^2$ be a reduced form of discriminant $D < 0$. Then, we know $b^2 \leq a^2$ and $a \leq c$, so that

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \implies a \leq \sqrt{\frac{-D}{3}}$$

We have $|b| \leq a \leq \sqrt{\frac{-D}{3}}$ which means there are finitely many choices for a and b, and since $D = b^2 - 4ac$, there are consequently only finitely many reduced forms with discriminant D. From Theorem 3.1.8, since every primitive positive definite form is properly equivalent to a unique reduced one, there must be finitely many equivalence classes of forms under proper equivalence. Hence, we can partition the set of primitive positive definite forms with discriminant D into classes under proper equivalence, and we can pick a reduced form as representative for each class. Letting $h(D)$ denote the number of proper equivalence classes of primitive positive definite forms with discriminant D, we have just shown that $h(D)$ is equal to the number of reduced forms with discriminant D. We will denote the set of these equivalence classes as $C(D)$.

As a digression, the above yields an algorithm to compute all the reduced forms for a given $D < 0$. We describe this algorithm below:

INPUT. A negative integer discriminant D.

0. If $D > 0$, stop here. Otherwise, continue to the next step.
1. Set `forms` $= \{\}$, $a = 1$, $b = -a$. Continue to the next step.
2. Set $c = \frac{b^2 - D}{4a}$. If c is integer, check if (a, b, c) is reduced. If yes, add (a, b, c) to `forms` and continue to the next step.
3. Set $b \leftarrow b + 1$. If $|b| \leq a$ go to the previous step. Else, continue to the next step.
4. Set $a \leftarrow a + 1$. If $a \leq \sqrt{-D/3}$, set $b = -a$ and go to step 2. Otherwise, stop and return `forms`.

Example 3.1.13.

(a) Let $D = -40$. In this case, $\sqrt{\frac{-D}{3}} \approx 3.65$, so the possible values for a are $\{1, 2, 3\}$. Since $D \equiv 0 \pmod 4$, we see that $c = \frac{b^2 - D}{4a}$ is only integer when $a = 1, b = 0$ or $a = 2, b = 0$. We thus obtain $C(-40) = \{x^2 + 10y^2, 2x^2 + 5y^2\}$ and it is easily checked these are reduced.

(b) Let $D = -84$. Here, $\sqrt{\frac{-D}{3}} \approx 5.29$ so the possible values for a are $\{1, 2, 3, 4, 5\}$. Python computes that $C(-84) = \{x^2 + 21y^2, 2x^2 + 2xy + 11y^2, 3x^2 + 7y^2, 5x^2 + 4xy + 5y^2\}$.

For indefinite binary quadratic forms, a similar theory of reduced forms exists. We say an indefinite quadratic form $ax^2 + bxy + cy^2$ is *reduced* if

$$0 < b < \sqrt{D} \qquad \text{and} \qquad \sqrt{D} - b < 2|a| < \sqrt{D} + b$$

where $D = b^2 - 4ac$ is the discriminant of the form. One can in fact show that Lemma 3.1.9 goes through in a similar way. Things are a little harder though, because while there is still at least one reduced form in each proper equivalence class, there could be more than one – Lemma 3.1.11 does not hold as stated for indefinite forms. Recall the two proper equivalences we have used in the proof of Lemma 3.1.9: these are (1) interchanging the outer coefficients $(x, y) \mapsto (-y, x)$ and (2) taking $(x, y) \to (x + my, y)$, where m is defined as $\lfloor \frac{a-b}{2a} \rfloor$. Composing these equivalences in the order (1) $\to$ (2) yields another (not necessarily proper) equivalence, denote this ϕ. Gauss proved that all the reduced forms in a given proper equivalence class can be obtained by starting at a reduced form (in the class) and successively applying ϕ, which turns out to be the appropriate reformulation of Lemma 3.1.11. We do not develop the theory of indefinite forms here in the interest of brevity, the reader can see [11, Chapter 3.1] or [23, Articles 206-212] for the details. Thus, we can define $C(D)$ for indefinite forms in the same way as we have defined it for positive definite ones.

3.1.3 Composition of forms

In this subsection, we will finally put a group structure on $C(D)$, so we discuss how one can define a notion of composition for two quadratic forms. The main result of this section is Theorem 3.1.14, where we establish that $C(D)$ is a finite abelian group. Finally, we characterize the subgroup of $C(D)$ consisting of the order 2 elements. In view of the next section, this is the last ingredient in the proof of Corollary 3.2.7. In this section, we will assume that the forms we are working with are primitive.

In Example 3.1.13a, we found that $C(-40) = \{x^2 + 10y^2, 2x^2 + 5y^2\}$. We will try to identify a group structure on $C(-40)$. Note that the product of any two integers represented by $2x^2 + 5y^2$ is represented by $x^2 + 10y^2$:

$$(2a^2 + 5b^2)(2c^2 + 5d^2) = 4a^2c^2 + 10(a^2d^2 + b^2c^2) + 25b^2d^2 = (2ac + 5bd)^2 + 10(bc - ad)^2 \tag{2}$$

Similarly, the product of an integer represented by $x^2 + 10y^2$ and an integer represented by $2x^2 + 5y^2$ always yields an integer represented by the latter:

$$(a^2 + 10b^2)(2c^2 + 5d^2) = 2a^2c^2 + 20b^2c^2 + 5a^2d^2 + 50b^2d^2 = 2(ac + 5bd)^2 + 5(bc - 2ad)^2 \tag{3}$$

Together, all this suggests that $C(-40)$ must have a group structure isomorphic to $\mathbb{Z}/2\mathbb{Z}$, with the form class of $x^2 + 10y^2$ as the identity and the form class of $2x^2 + 5y^2$ the element of order 2.

In general, if we hypothesize that $C(D)$ forms a group under multiplication, we can identify the laws for composition. From what we have seen above, for $f, g \in C(D)$, we expect that these laws arise from algebraic identities of the form

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)) \tag{4}$$

where F is another quadratic form with the same discriminant and

$$B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw, \qquad i = 1, 2$$

are integral bilinear forms in the x, y and z, w. For example, from (2), one has $F(x, y) = x^2 + 10y^2$ and

$$B_1(x, y; z, w) = 2xz + 5yw, \quad B_2(x, y; z, w) = yz - xw;$$

similarly, from (3), one has

$$B_1(x, y; z, w) = xz + 5yw, \quad B_2(x, y; z, w) = yz - 2xw$$

However, finding these identities is in general not easy. One issue is that this procedure is not computationally feasible for large discriminants D, as we have to find two B_i for each pair of reduced forms. Another difficulty arises because two reduced forms can be equivalent and thus represent the same numbers, see Example 3.1.12a. Here, the procedure we have undertaken above for $C(-40)$ cannot be done, as the forms $3x^2 \pm 2xy + 5y^2$ are both reduced but equivalent, so represent the same numbers.

The theory of composing quadratic forms was first developed by Legendre. However, Legendre's treatment only used the weaker notion of equivalence between quadratic forms rather than proper equivalence, which meant there were different possible results when composing two forms. Gauss in the 1800s solved this issue completely by defining his composition law in Disquisitiones Arithmeticae [23]. However, his treatment is quite complicated because one still needs to identify the correct choice of compositions whenever there is more than one option. Therefore, in this thesis we ignore Gauss' original composition law; we instead describe a simpler composition law, due to Dirichlet.

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant $D < 0$, satisfying $\gcd(a, a', (b + b')/2) = 1$. Then, the *Dirichlet composition* of f and g is of the form

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2.$$

Here, B is the unique integer modulo $2aa'$ with $B \equiv b \pmod{2a}$, $B \equiv b' \pmod{2a'}$ and $B^2 \equiv D \pmod{4aa'}$. See [11, Proposition 4.5] for a proof that such a B exists and is unique.

While Dirichlet composition is less general than direct composition in the sense of (4) because of the condition $\gcd(a, (b + b')/2) = 1$, it is easier to carry out because there is an explicit formula for the composition – one does not have to compute the right algebraic identities every time.

We have now built up enough of the theory of quadratic forms that we can state the main result of this section:

Theorem 3.1.14. Take $D \equiv 0, 1 \pmod 4$ with $D < 0$. Then, Dirichlet composition induces a well-defined binary operation on $C(D)$ that turns it into a finite abelian group.

Proof sketch. First, we need to show Dirichlet composition is in fact well-defined at the level of proper equivalence classes and that it is a commutative and associative operation. This can be done directly using the definition of composition, but this requires one to compose equivalence classes of forms, see [11, Theorem 4.8]. One can also using the bijection $\mathrm{Cl}(K) \to C(\mathrm{disc}(K))$ established in the next section, see

[17, Theorem 7.7]. Next, we need to show the existence of an identity element. We claim the identity element is given by the principal form F_D (see (1)). Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive positive definite form and let $[f]$ be the class containing f. The first coefficient of F_D is 1, so the Dirichlet composition of f with F_D is defined. Note taking $B = b$ satisfies the congruences defining B in the definition of Dirichlet composition. Of course $B \equiv b \bmod 2a$; moreover we have seen D and b have the same parity, so B is congruent to the second coefficient of F_D mod 2. Finally, $D = b^2 - 4ac \equiv b^2 \bmod 4a$ shows the last equation holds. Then, the Dirichlet composition of f and F_D is given by

$$ax^2 + bxy + \frac{b^2 - D}{4a}y^2 = f(x,y)$$

so F_D is indeed the identity element.
Finally, we need to show the existence of inverses. Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = ax^2 - bxy + cy^2$. We claim the class $\overline{g}$ is the inverse to $\overline{f}$. The Dirichlet composition of f and g is not defined as $\gcd(a, a, (b-b)/2) = a$, and $a \neq 1$ in general. The proper equivalence $(x,y) \mapsto (-y,x)$ takes g to $g'(x,y) = cx^2 + bxy + ay^2$, and $\gcd(a, c, (b+b)/2) = \gcd(a,c,b) = 1$ since f is assumed to be primitive. As before, it is easy to check that taking $B = b$ satisfies the definition of Dirichlet composition. Thus, the composition of f and g' is given by

$$acx^2 + bxy + \frac{b^2 - D}{4ac}y^2 = acx^2 + bxy + y^2$$

It remains to show the composition of f and g' is properly equivalent to the principal form. If $D \equiv 0 \bmod 4$, the proper equivalence $(x,y) \mapsto (-y, x + by/2)$ takes the above form to the principal form:

$$\begin{bmatrix} 0 & -1 \\ 1 & \frac{b}{2} \end{bmatrix}^T \begin{bmatrix} 2ac & b \\ b & 2 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \frac{b}{2} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & -\frac{b^2}{2} + 2ac \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & -\frac{D}{4} \end{bmatrix}$$

If $D \equiv 1 \bmod 4$, then the proper equivalence $(x,y) \mapsto (-y, x + (b+1)y/2)$ works:

$$\begin{bmatrix} 0 & -1 \\ 1 & \frac{b+1}{2} \end{bmatrix}^T \begin{bmatrix} 2ac & b \\ b & 2 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \frac{b+1}{2} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & -\frac{b^2}{2} + 2ac \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & \frac{1-D}{4} \end{bmatrix}$$

This completes the proof sketch.

In what follows, we will refer to $C(D)$ as the *form class group*.

Recall that the goal of this chapter has been to prove that there are infinitely many quadratic number fields whose class number is divisible by 2. To this end, we state the following result.

Theorem 3.1.15. Let $D \equiv 0, 1 \bmod 4$ and let r be the number of distinct odd prime factors of D. Define the number μ as follows: if $D \equiv 1 \bmod 4$, then $\mu = r$; else if $D \equiv 0 \bmod 4$, we can write $D = -4n$, and μ is determined as

$$\mu = \begin{cases} r+1 & n \equiv 1, 2 \pmod 4 \\ r & n \equiv 3 \pmod 4 \\ r+2 & n \equiv 0 \pmod 8 \\ r+1 & n \equiv 4 \pmod 8 \end{cases}$$

Then the subgroup of $C(D)$ consisting of the elements of order 2 has $2^{\mu-1}$ elements.

Proof. See [11, Corollary 4.9]. □

Note in particular there are infinitely many such discriminants D.

3.2 The correspondence between forms and ideals

In this section, we establish a bijection between the ideal class group $\mathrm{Cl}(K)$ of a quadratic number field and the form class group $C(\mathrm{disc}(K))$ of reduced forms with discriminant $\mathrm{disc}(K)$. First, we illustrate a problem that arises if K is real quadratic by way of example. Let $K = \mathbb{Q}(\sqrt{3})$, from section 1.7 we know $h(K) = 1$. We claim however that the reduced forms $\pm(x^2 - 3y^2)$ of discriminant $12 = \mathrm{disc}(K)$ are not properly equivalent. Suppose they are related via the proper equivalence $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$. Then, one must have

$$(p^2 - 3r^2)x^2 + (q^2 - 3s^2)y^2 + 2(pq - 3rs)xy = -x^2 + 3y^2.$$

In particular, we have the equation $p^2 - 3r^2 = -1$ over the integers. Reducing both sides modulo 3, one obtains $p^2 \equiv 2 \pmod 3$, but this is a contradiction. Hence, $\mathrm{Cl}(K) \neq C(12)$.

This problem arises because our definition of ideal equivalence (two ideals in $\mathrm{Cl}(K)$ are equivalent if they differ by a factor of a principal ideal) is not restrictive enough in the real quadratic case. We will thus need to modify this definition. To this end, we first define the narrow class group $\mathrm{Cl}^+(K)$. Then, we construct a map from the fractional ideals of K to the set of quadratic forms with discriminant $\mathrm{disc}(K)$ and show this map is well-defined upon reducing to equivalence classes in $\mathrm{Cl}^+(K)$ and $C(\mathrm{disc}(K))$. Finally, we show this map is indeed a bijection, and we end by proving the main result of this chapter: that there are infinitely many quadratic number fields with even class number.

The narrow class group

Recall that a number field K has n embeddings into $\mathbb{C}$. One says an embedding $\sigma : K \to \mathbb{C}$ is real if $\sigma(K) \subset \mathbb{R}$ and complex otherwise (see also the discussion following Proposition 1.2.3). We say $\alpha \in K$ is *totally positive* if $\sigma(\alpha) > 0$ for every real embedding $\sigma : K \to \mathbb{C}$. We write P_K^+ for the set of totally positive principal fractional ideals, i.e. principal fractional ideals (b) where b is a totally positive element of K. With this, we can define the *narrow class group* $\mathrm{Cl}^+(K)$ as the quotient I_K/P_K^+.

Note that $P_K^+ \subset P_K$ so $\mathrm{Cl}^+(K) \supset \mathrm{Cl}(K)$. We prove the following result that makes this relation explicit in the case of quadratic fields:

Proposition 3.2.1. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. If K is imaginary, then $\mathrm{Cl}^+(K) = \mathrm{Cl}(K)$. If K is real, $\mathrm{Cl}^+(K) = \mathrm{Cl}(K)$ if K has a unit with negative norm. Otherwise, $\mathrm{Cl}^+(K)/\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. If K is imaginary quadratic, all elements have positive norm (cf. Example 1.2.2) so $P_K = P_K^+$ and consequently $\mathrm{Cl}(K) = \mathrm{Cl}^+(K)$. Suppose K is real quadratic and that there is a $u \in U_K$ with $N(u) < 0$. Denote the nontrivial real embedding of K into $\mathbb{C}$ as σ. By Proposition 1.2.5 one has $N(u) = u \cdot \sigma(u)$; without loss of generality suppose $\sigma(u) > 0$ and $u < 0$. Take any principal fractional ideal (β), then we can always pick a totally positive generator: if β itself is not totally positive, one of $-\beta$ or $u\beta$ is. This

shows $P_K^+ = P_K$.
Otherwise, suppose K is real quadratic and all the elements of U_K have positive norm. We claim that $P_K = P_K^+ \cup \sqrt{d}P_K^+$. Only the reverse inclusion needs proof: take a principal fractional ideal $(\beta) \in P_K$. Either β is totally positive, in which case $(\beta) \in P_K^+$, else either $\beta < 0$ or $\sigma(\beta) < 0$. If both are negative, we can replace (β) with the totally positive ideal $(-\beta)$. Hence, without loss of generality, suppose $\sigma(\beta) < 0$ and $\beta > 0$. Write $\beta = a + b\sqrt{d}$ and let $\alpha = \beta/\sqrt{d} = b + a/d\sqrt{d} \in K$. We claim α is totally positive. One sees that

$$\begin{aligned} \alpha = b + \frac{a}{d}\sqrt{d} > \frac{a + b\sqrt{d}}{d} = \frac{\beta}{d} > 0 \text{ and,} \\ \sigma(\alpha) = b - \frac{a}{d}\sqrt{d} > \frac{b\sqrt{d} - a}{d} = \frac{-\sigma(\beta)}{d} > 0 \end{aligned}$$

as required. Consequently $P_K/P_K^+ \cong \mathbb{Z}/2\mathbb{Z}$. Via the third isomorphism theorem for groups, we have

$$\mathrm{Cl}^+(K)/\mathrm{Cl}(K) = \frac{(I_K/P_K^+)}{(I_K/P_K)} \cong P_K/P_K^+ \cong \mathbb{Z}/2\mathbb{Z}$$

which finishes the proof. □

We now proceed to constructing the promised correspondence between forms and ideals.

Ideals to forms

Since every fractional ideal of K is a product of prime integral ideals of $\mathcal{O}_K$ by Theorem 1.4.3, we only need to work with integral ideals. Recall that if K is a quadratic number field, $\mathcal{O}_K$ is a free abelian group with rank 2 by Theorem 1.2.9. In particular, ideals of $\mathcal{O}_K$ are free abelian groups of rank at most 2. We state a useful lemma relating the norm of an ideal of $\mathcal{O}_K$ and the discriminant of its $\mathbb{Z}$-basis:

Lemma 3.2.2. Let K be a quadratic number field and let $\{\alpha, \beta\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Suppose $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ with $\mathbb{Z}$-basis $\{\delta, \gamma\}$. Then, one has

$$N(\mathfrak{a})^2 = \frac{\mathrm{disc}(\delta, \gamma)}{\mathrm{disc}(K)}.$$

Proof. Write $\delta = a\alpha + b\beta$ and $\gamma = c\alpha + d\beta$. Denote the nontrivial embedding of $K \to \mathbb{C}$ (cf. Proposition 1.2.3) as $x \mapsto x'$ and note that

$$\mathrm{disc}(\delta, \gamma) = \det \begin{pmatrix} a\alpha + b\beta & c\alpha + d\beta \\ a\alpha' + b\beta' & c\alpha' + d\beta' \end{pmatrix}^2 = \det \left(\begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \right)^2 = \mathrm{disc}(K) \det \begin{pmatrix} a & c \\ b & d \end{pmatrix}^2$$

By [50, Theorem IX.3.7], one has that

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = \det \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

and the lemma follows. □

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and fix a $\mathbb{Z}$-basis (α, β) of $\mathfrak{a}$. We define Ψ_{IF} as a map from I_K to the set of primitive binary quadratic forms of discriminant $\mathrm{disc}(K)$ as follows:

$$\Psi_{IF}: \qquad \mathfrak{a} \mapsto f_{\mathfrak{a}}, \quad f_{\mathfrak{a}}(x,y) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}$$

First, we need to show $f_{\mathfrak{a}}$ is a legitimate integral quadratic form. As in the proof of the above lemma, denote the nontrivial embedding of $K \to \mathbb{C}$ as $x \mapsto x'$. We expand out the definition of $f_{\mathfrak{a}}$:

$$\begin{aligned}\frac{N(\alpha x + \beta y)}{N(\mathfrak{a})} &= \frac{(\alpha x + \beta y)(\alpha x + \beta y)'}{N(\mathfrak{a})} \\ &= \frac{\alpha\alpha' x^2 + (\alpha\beta' + \beta\alpha')xy + \beta\beta' y^2}{N(\mathfrak{a})} \\ &=: ax^2 + bxy + cy^2\end{aligned}$$

We claim a, b, c are integers. Since $\{\alpha, \beta\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$, an arbitrary $z = \alpha x + \beta y$ is an element of $\mathfrak{a}$. We then have $(z) \subset \mathfrak{a}$ and consequently $N(\mathfrak{a}) \mid N(z)$ as integers. In particular, this means that $a = N(\alpha)/N(\mathfrak{a})$, $c = N(\beta)/N(\mathfrak{a})$ and $a + b + c = N(\alpha + \beta)/N(\mathfrak{a})$ are integers, from which our claim follows. Moreover the form $f_{\mathfrak{a}}$ has discriminant

$$\frac{(\alpha\beta' + \beta\alpha')^2 - 4\alpha\alpha'\beta\beta'}{N(\mathfrak{a})^2} = \frac{(\alpha\beta' - \beta\alpha')^2}{N(\mathfrak{a})^2} = \frac{\mathrm{disc}(\alpha, \beta)}{N(\mathfrak{a})^2} = \mathrm{disc}(K)$$

by Lemma 3.2.2. We show that $f_{\mathfrak{a}}$ is primitive: note that $\gcd(a,b,c)^2$ must divide the discriminant $b^2 - 4ac = \mathrm{disc}(K)$. However, $\mathrm{disc}(K)$ is squarefree, except possibly a factor of 4, so $\gcd(a,b,c) \leq 2$. Finally, note that $\gcd(a,b,c)$ cannot be 2, because then $\mathrm{disc}(K)/4 = (b/2)^2 - 4(a/2 \cdot c/2) \equiv (b/2)^2 \pmod 4$, which is a contradiction. Hence, $\mathrm{disc}(a,b,c) = 1$ and $f_{\mathfrak{a}}$ is a primitive integral quadratic form.

We need to show that the form $f_{\mathfrak{a}}$ is independent of the $\mathbb{Z}$-basis (α, β) chosen. For this, we will need to introduce the notion of orientation of bases.

Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ and (α, β) a corresponding $\mathbb{Z}$-basis. We define

$$\mathrm{sgn}(\alpha, \beta) = \begin{cases} 1 & \mathrm{Re}\left(\frac{\mathrm{disc}(\alpha,\beta)}{\sqrt{\mathrm{disc}(K)}}\right) > 0 \\ -1 & \text{else} \end{cases}$$

One says a basis (α, β) is *positively oriented* if $\mathrm{sgn}(\alpha, \beta) = 1$ and *negatively oriented* else. We are now equipped to prove the following result:

Lemma 3.2.3. Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}_K$. Two distinct positively oriented $\mathbb{Z}$-bases of $\mathcal{O}_K$ yield properly equivalent $f_{\mathfrak{a}}$.

Proof. Let $\{\alpha, \beta\}$ and $\{\delta, \gamma\}$ be two distinct positively oriented $\mathbb{Z}$-bases of $\mathcal{O}_K$. Let B be the change of basis matrix so that $(\alpha, \beta) = (\delta, \gamma)B$. The matrix B has integer entries, and it must be invertible since it is a change of basis matrix. Moreover, its determinant is a unit in $\mathbb{Z}$, i.e. $\det(B) = \pm 1$. As before, let σ

be the non-identity embedding of $K \to \mathbb{C}$ and denote $\sigma(x) = x'$. Then, one has

$$\operatorname{disc}(\alpha, \beta) = \operatorname{disc}(\delta, \gamma) \det(B)$$

and consequently

$$\det(B) = \frac{\operatorname{disc}(\alpha, \beta)/\sqrt{\operatorname{disc}(K)}}{\operatorname{disc}(\delta, \gamma)/\sqrt{\operatorname{disc}(K)}} > 0$$

since both bases are positively oriented. It follows that $\det(B) = 1$. Then, we have

$$N(\alpha x + \beta y) = N((x, y)(\alpha, \beta)^T) = N((x, y)B^T(\delta, \gamma)^T) = N((X, Y)(\delta, \gamma)^T)$$

where $(X, Y) = (x, y)B^T$. Since $\det(B) = 1$, this is exactly the definition of proper equivalence. □

So indeed Ψ_{IF} is well-defined as a map. Finally, we need to show that Ψ_{IF} gives the same form for two ideals in the same class of $\mathrm{Cl}^+(K)$.

Lemma 3.2.4. If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of $\mathcal{O}_K$ that are equivalent in $\mathrm{Cl}^+(K)$, then $f_{\mathfrak{a}}$ is properly equivalent to $f_{\mathfrak{b}}$.

Proof. Since $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent in $\mathrm{Cl}^+(K)$, we can write $\mathfrak{b} = (\lambda)\mathfrak{a}$ where λ is some totally positive element of K. Let $\{\alpha, \beta\}$ be a positively oriented $\mathbb{Z}$-basis of $\mathfrak{a}$, then $\{\lambda\alpha, \lambda\beta\}$ is a $\mathbb{Z}$-basis of $\mathfrak{b}$. Moreover, this basis is positively oriented, as

$$\frac{\operatorname{disc}(\lambda\alpha, \lambda\beta)}{\sqrt{\operatorname{disc}(K)}} = \frac{\lambda\alpha\lambda'\beta' - \lambda'\alpha'\lambda\beta}{\sqrt{\operatorname{disc}(K)}} = N(\lambda)\frac{\operatorname{disc}(\alpha, \beta)}{\sqrt{\operatorname{disc}(K)}}$$

which has positive real part since $N(\lambda) > 0$. Let us say $\overline{f}$ is the equivalence class associated with the quadratic form f under proper equivalence. We compute

$$\begin{aligned}
\overline{f_{\mathfrak{b}}(x, y)} &= \overline{\frac{N(\lambda\alpha x + \lambda\beta y)}{N(\mathfrak{b})}} \\
&= \overline{\frac{N(\lambda)N(\alpha x + \beta y)}{N((\lambda)) \cdot N(\mathfrak{a})}} \\
&= \overline{\frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}} = \overline{f_{\mathfrak{a}}(x, y)} && \text{(since } N((\lambda)) = N(\lambda)\text{)}
\end{aligned}$$

Hence, $f_{\mathfrak{a}}$ is properly equivalent to $f_{\mathfrak{b}}$. □

Finally, we show Ψ_{IF} is indeed a bijection, via the following proposition:

Proposition 3.2.5. The map Ψ_{IF} is a bijection from the narrow class group $\mathrm{Cl}^+(K)$ to the form class group $C(\operatorname{disc}(K))$.

Proof. We begin by showing surjectivity. Let $ax^2 + bxy + cy^2$ be a primitive quadratic form of discriminant $\operatorname{disc}(K) =: d_K$ (positive definite when $d_K < 0$). Define the fractional ideal $\mathfrak{a}$ as

$$\mathfrak{a} = \left\langle a, \lambda\frac{b - \sqrt{d_K}}{2} \right\rangle$$

Here we mean $\mathfrak{a}$ is generated by the $\mathbb{Z}$-basis $\{\lambda a, \lambda(b-\sqrt{d_K})/2\}$. The constant λ is defined as follows: if $a > 0$ we set $\lambda = 1$, and otherwise $\lambda = \sqrt{d_K}$. We show this basis is positively oriented:

$$\operatorname{disc}\left(a, \lambda\frac{b-\sqrt{d_K}}{2}\right) = \begin{bmatrix} \lambda a & \lambda' a \\ \lambda\frac{b-\sqrt{d_K}}{2} & \lambda'\frac{b+\sqrt{d_K}}{2} \end{bmatrix} = aN(\lambda)\sqrt{d_K}$$

where we once again denote the nontrivial embedding of K as $x \mapsto x'$. Note that we have used $\lambda\lambda' = N(\lambda)$ by Proposition 1.2.5. When $a > 0$, then $N(\lambda) = N(1) = 1$, and when $a < 0$, then $N(\lambda) = N(\sqrt{d_K}) = -d_K$. Hence, the basis is always positively oriented. By Lemma 3.2.2, we have $N(\mathfrak{a}) = aN(\lambda)$. We compute $\Psi_{IF}(\mathfrak{a})$:

$$\begin{aligned} f_{\mathfrak{a}} &= \frac{N\left(\lambda a x + \lambda\frac{b-\sqrt{d_K}2}{y}\right)}{N(\mathfrak{a})} \\ &= \frac{N(\lambda)a^2x^2 + N(\lambda)\frac{b^2-d_K}{4}y^2 + N(\lambda)abxy}{aN(\lambda)} \\ &= ax^2 + bxy + cy^2 \end{aligned}$$

hence Ψ_{IF} is surjective.

Next, we show injectivity. Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are two distinct fractional ideals of $\mathcal{O}_K$ such that $f_{\mathfrak{a}}$ is properly equivalent to $f_{\mathfrak{b}}$. Let $\{\alpha_1, \beta_1\}$ and $\{\alpha_2, \beta_2\}$ be positively oriented bases of $\mathfrak{a}$ and $\mathfrak{b}$ respectively. Since $f_{\mathfrak{a}}$ and $f_{\mathfrak{b}}$ are properly equivalent, there exists a matrix $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ with $\det P = 1$ such that $f_{\mathfrak{a}}(x, y) = f_{\mathfrak{b}}(px + qy, rx + sy)$, i.e.

$$\frac{N(\alpha_1 x + \beta_1 y)}{N(\mathfrak{a})} = \frac{N(\alpha_2(px + qy) + \beta_2(rx + sy))}{N(\mathfrak{b})} \tag{1}$$

Consider the quadratic polynomial $f_{\mathfrak{a}}(x, 1)$. This has roots $x = -\beta_1/\alpha_1$ and β_1'/α_1'. These must be equal to the roots of the expression on the right of (1) when we set $y = 1$. These roots are

$$-\frac{r\alpha_2 + s\beta_2}{p\alpha_2 + q\beta_2}, \quad \text{and} \quad -\frac{r\alpha_2' + s\beta_2'}{p\alpha_2' + q\beta_2'}$$

Hence, there must exist some $\lambda \in K$ such that one of

$$\begin{cases} r\alpha_2 + s\beta_2 = \lambda\beta_1 \\ p\alpha_2 + q\beta_2 = \lambda\alpha_1 \end{cases} \quad \text{or} \quad \begin{cases} r\alpha_2 + s\beta_2 = \lambda\beta_1' \\ p\alpha_2 + q\beta_2 = \lambda\alpha_1' \end{cases} \tag{2}$$

holds. Note that we can always choose $\lambda > 0$. Substituting either of the equations of (2) into (1), we obtain that $N(\lambda) = N(\mathfrak{b})/N(\mathfrak{a}) > 0$. We claim the second case of (2) cannot occur: in this case, we have the matrix equality

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} \alpha_2 & \alpha_2' \\ \beta_2 & \beta_2' \end{pmatrix} = \begin{pmatrix} \lambda\alpha_1' & \lambda'\alpha_1 \\ \lambda\beta_1' & \lambda'\beta_1 \end{pmatrix}$$

Taking determinants then square roots on both sides, we obtain $\operatorname{disc}(\alpha_2, \beta_2) = -\operatorname{disc}(\lambda\alpha_1, \lambda\beta_1)$, which implies

$$\frac{\operatorname{disc}(\alpha_2, \beta_2)}{\operatorname{disc}(\alpha_1, \beta_2)} = -\lambda\lambda' = -N(\lambda) < 0$$

but this is a contradiction, since both bases are chosen to be positively oriented. Hence, only the first case of (2) can hold. We see that $\{\lambda\alpha_1, \lambda\beta_1\}$ is a $\mathbb{Z}$-basis of $\mathfrak{b}$, as the equations of (2) define a change of basis. Thus, $\mathfrak{a} = (\lambda)\mathfrak{b}$, hence Ψ_{IF} is injective. This completes the proof. □

The main result

Combining the bijection established above and Theorem 3.1.14, we obtain the following result:

Theorem 3.2.6. Let K be a quadratic number field with discriminant d_K. Then, one has an isomorphism $C(d_K) \cong \mathrm{Cl}^+(K)$ between the group of reduced forms with discriminant d_K and the narrow class group of K.

Proof sketch. It remains to show that the bijection Ψ_{IF} is an isomorphism. As mentioned in the proof sketch of Theorem 3.1.14, one can either use Ψ_{IF} to show that Dirichlet composition of two quadratic form classes corresponds to the product of the corresponding ideal classes in $\mathrm{Cl}^+(K)$, as in [17, Theorem 7.7], or work directly with forms, see [11, Theorem 6.20]. □

The main result of this chapter follows as a corollary to this theorem.

Corollary 3.2.7. There are infinitely many quadratic number fields with even class number.

Proof. By Proposition 3.2.1, the class number $h(K)$ is always a multiple of $|\mathrm{Cl}^+(K)|$. Theorem 3.1.15 shows that there are infinitely many discriminants D (both negative and positive) for which $C(D)$ has an element of order 2. Consequently, by the previous theorem, it follows that there are infinitely many quadratic fields with even class number. □

Chapter 4

Divisibility in the general case

In this chapter, we will try to answer the question of 'how many' quadratic number fields there are with class number divisible by a given $g > 2$. In chapter 3, we have already seen that there are infinitely many quadratic number fields with class number divisible by 2. We will prove similar results for $g > 2$ due to Ankeny and Chowla [1] in the imaginary case and Weinberger [52] in the real case.

We also provide estimates on the number of quadratic number fields K with $g \mid h(K)$ for a given $g > 2$, due to Murty [40]. Let us make precise what we mean by estimate. We define the quantity

$$N_g(X)^- = \#\{0 < d \leq X : g \mid h(\mathbb{Q}(\sqrt{-d})\},$$

where X is some positive real number. We can also define the analogous

$$N_g(X)^+ = \#\{0 < d \leq X : g \mid h(\mathbb{Q}(\sqrt{d})\}$$

for real quadratic fields. We will give asymptotic lower bounds on $N_g(X)^{-/+}$ in terms of X.

The proofs of Ankeny-Chowla and Weinberger follow the same thread. We give a sketch of the argument for the reader's benefit. First, both take a special choice of discriminant d depending on x and g, where x is some integer. The goal is to show there are infinitely many quadratic fields $\mathbb{Q}(\sqrt{d})$ (resp. $\mathbb{Q}(\sqrt{-d})$) with an element of order g in the class group. Then, the argument essentially consists of 2 steps:

Step 1. (Bounding step) We show there are infinitely many d satisfying a certain property. Ankeny and Chowla take $d = 3^g - x^2$ and show that there are infinitely many squarefree d (Lemma 4.1.3). Weinberger takes $d = x^{2g} + 4$ and shows that there are infinitely many x (and consequently infinitely many d) such that the polynomial $T^k - 4$ is irreducible modulo x (Lemma 4.2.3).

Step 2. (Order g step) For each of the infinitely many d obtained in the previous step, we construct an ideal $\mathfrak{a}$ such that it has order g in the class group. Ankeny and Chowla's argument directly leverages the factoring properties provided by their choice of d by considering how the prime (3) factors in $\mathbb{Q}(\sqrt{-d})$ (Lemma 4.1.4). Weinberger constructs the ideal $\mathfrak{a}$ directly and proves by contradiction that it must have order g (Lemma 4.2.4).

Combining these two steps gives that there are infinitely many quadratic fields $K = \mathbb{Q}(\sqrt{d})$ (resp. $\mathbb{Q}(\sqrt{-d})$) with an element of order g in the class group. Note that in the case of real quadratic fields, we have to do

more work, as we need knowledge of the unit group U_K in order to study when ideals are principal (see Proposition 4.2.2).

Notation. We write $f(x) = O(g(x))$ to mean that there exists a x_0 such that $|f(x)| \leq C|g(x)|$ for $x \geq x_0$, for some positive constant C. We will also often use the notation $f(x) \gg g(x)$ to mean $g(x) = O(g(x))$.

4.1 The imaginary case

Let $g > 2$ be an odd integer. Set $d = 3^g - x^2$ with x odd and $0 < x^2 < 3^g/2$. In this section, we will show there are infinitely many imaginary quadratic fields of the form $K = \mathbb{Q}(\sqrt{-d})$ with $g \mid h(K)$. The results of this section are due to [1].

As described in the beginning of this chapter, we separate the argument into two steps: the bounding step and the order g step. In the proof of Ankeny and Chowla, the bounding step consists of showing there are infinitely many squarefree integers of the form d. This is accomplished in Lemma 4.1.3. Before we do this, we will require an elementary estimate on the prime counting function $\pi(x)$. This lemma was adapted from Problem 1.1.26 of [41].

Lemma 4.1.1. Let $\pi(x)$ be the prime-counting function, i.e. define $\pi(x) = \#\{\text{primes } p \leq x\}$ for $x > 0$. Then, one has the bound

$$\pi(x) \leq \frac{10x \log(2)}{\log(x)}$$

for all $x \geq 2$.

Proof. Recall the fact that $\binom{n}{k}$ is an integer for $n \geq k \geq 0$. The first observation that we make is that

$$\prod_{\substack{n \leq p \leq 2n \\ p \text{ prime}}} p \mid \binom{2n}{n}$$

We can deduce that

$$\prod_{\substack{n \leq p \leq 2n \\ p \text{ prime}}} p \leq \binom{2n}{n}$$

and consequently

$$\sum_{\substack{n \leq p \leq 2n \\ p \text{ prime}}} \log p \leq \log \binom{2n}{n} \leq 2n \log 2 \tag{1}$$

by taking logarithms on both sides, and using the fact that

$$\binom{n}{k} \leq 2^n$$

for any $n \geq k \geq 0$. We define

$$\vartheta(n) = \sum_{\substack{p \leq n \\ p \text{ prime}}} \log p.$$

Then (1) shows that

$$\vartheta(2n) - \vartheta(n) \leq 2n \log 2.$$

We claim that

$$\vartheta(2^r) \leq 2^{r+1} \log 2.$$

We prove this by induction: the base case $r = 0$ is clear as $\vartheta(1) = 0$ by definition. Suppose the claim is true for some $r \geq 0$. Then,

$$\vartheta(2^{r+1}) \leq 2^{r+1} \log 2 + \vartheta(2^r) \leq 2^{r+1} \log 2 + 2^{r+1} \log 2 = 2^{r+2} \log 2$$

which shows the claim. For any integer $x \geq 2$, we can always find r so that $2^r \leq x \leq 2^{r+1}$; fix such an r. Then, we have

$$\vartheta(x) \leq \vartheta(2^{r+1}) \leq 2^{r+1} \log 2 \leq 4x \log 2.$$

Now, we would like to turn the above into an inequality involving $\pi(x)$. To this end, note that

$$\sum_{\sqrt{x} < p \leq x} \log p \leq \vartheta(x) \leq 4x \log 2$$

Each term in the sum on the left is at least $\log \sqrt{x}$; moreover there are $\pi(x) - \pi(\sqrt{x})$ of them, so we have

$$\log(\sqrt{x})(\pi(x) - \pi(\sqrt{x})) \leq 4x \log 2$$

This means that

$$\pi(x) - \pi(\sqrt{x}) \leq \frac{8x \log 2}{\log x}$$

The number of primes $\leq x$ is of course less than x for any $x \geq 2$, so $\pi(x) \leq x$. Hence, the above implies that

$$\pi(x) \leq \sqrt{x} + \frac{8x \log 2}{\log x}$$

and finally we deduce that

$$\pi(x) \leq \frac{10x \log 2}{\log x},$$

as

$$\sqrt{x} \leq \frac{2x \log 2}{\log x}$$

which can be verified directly by the graph of $f(x) = 2\sqrt{x} \log 2 - \log x$. □

Remark 4.1.2. The above is a much weaker version of the prime number theorem, which says $\pi(x) = O(\frac{x}{\log x})$.

Now, we proceed to estimating the number of squarefree values of d. The following is Lemma 1 of [1].

Lemma 4.1.3. Let N be the number of squarefree integers of the form $3^g - x^2$, where g and x are as above. Then for g sufficiently large, we have $N \gg 3^{g/2}$.

Proof. After fixing g, there are $3^{g/2}/\sqrt{2}$ choices for x; we can only choose half of these since x is odd.

Thus, the number of integers of the required form is

$$\frac{1}{2\sqrt{2}}3^{g/2} + O(1)$$

We would like d to be squarefree, so it suffices to remove any number divisible by the square of a prime. First, suppose $3^g - x^2$ is divisible by 4. Since g is odd, this implies $x^2 \equiv 3^g \equiv -1 \bmod 4$, which is a contradiction. Hence, $4 \nmid 3^g - x^2$. Next, note that $9 \mid 3^g - x^2$ precisely when $3 \mid x$, so we remove such numbers. We have

$$\frac{1}{6\sqrt{2}}3^{g/2} + O(1)$$

of these. Finally, let $p > 3$ be prime. The number of $3^g - x^2$ such that $p^2 \nmid 3^g - x^2$ is

$$\frac{1}{p^2\sqrt{2}}3^{g/2} + O(1)$$

Now, we can deduce a lower bound on N, by removing the numbers $3^g - x^2$ divisible by the square of a prime.

$$N \geq \frac{3^{g/2}}{\sqrt{2}}\left[\frac{1}{2} - \frac{1}{6} - \sum_{\substack{p^2 \leq 3^g \\ p>3 \text{ prime}}} \left(\frac{1}{p^2} + O(1)\right)\right]$$

Using the previous lemma, we know that $\pi(3^{g/2}) \leq 20\log(2/3)\frac{3^{g/2}}{g}$, i.e., $\pi(3^{g/2}) = O\left(\frac{3^{g/2}}{g}\right)$. Applying this to the sum above, we have that

$$\sum_{\substack{p^2 \leq 3^g \\ p>3 \text{ prime}}} \left(\frac{1}{p^2} + O(1)\right) = \sum_{\substack{p^2 \leq 3^g \\ p>3 \text{ prime}}} \frac{1}{p^2} + \pi(3^{g/2})O(1) = \sum_{\substack{p^2 \leq 3^g \\ p>3 \text{ prime}}} \frac{1}{p^2} + O\left(\frac{3^{g/2}}{g}\right)$$

and substituting this into the inequality

$$N \geq \frac{3^{g/2}}{\sqrt{2}}\left[\frac{1}{2} - \frac{1}{6} - \sum_{\substack{p^2 \leq 3^g \\ p>3 \text{ prime}}} \frac{1}{p^2} + O\left(\frac{3^{g/2}}{g}\right)\right]$$

We can bound the sum on the right from above:

$$\sum_{\substack{p^2 \leq 3^g \\ p>3 \text{ prime}}} \frac{1}{p^2} \leq \sum_{n \geq 5} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 - \frac{1}{4} - \frac{1}{9} - \frac{1}{16} < \frac{1}{4}$$

and so it follows that

$$N \geq 3^{g/2}\left[\frac{1}{12\sqrt{2}} + O\left(\frac{3^{g/2}}{g}\right)\right]$$

The expression in the brackets is positive, so for g sufficiently large, we conclude that $N \gg 3^{g/2}$. □

This concludes the bounding step. Now, we proceed to the order g step. That is, we must show that for each of the infinitely many squarefree d obtained from the previous lemma, $\mathbb{Q}(\sqrt{-d})$ has an element of order g in its class group. The following lemma is Theorem 1 of [1].

Lemma 4.1.4. Let g and d be as before. Then, if d is squarefree then $\mathbb{Q}(\sqrt{-d})$ has an element of order g in its class group.

Proof. Because g and x are odd, we have $d = 3^g - x^2 \equiv -1 - 1 \equiv 2 \bmod 4$, so Theorem 1.2.7 implies that $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} = \mathbb{Z}[\sqrt{-d}]$. Moreover, Corollary 1.5.10 implies that (3) factors into conjugate prime ideals $\mathfrak{p}\mathfrak{p}'$ in $\mathbb{Q}(\sqrt{-d})$. Let m be the order of $\mathfrak{p}$ in the class group, that is let m be the minimal integer such that $\mathfrak{p}^m$ is principal. Let $\mathfrak{p}^m = (\alpha)$ where $\alpha = u + v\sqrt{-d}$. Then,

$$(3^m) = (u + v\sqrt{-d})(u - v\sqrt{-d}) = (u^2 + v^2 d)$$

and since the only units of $\mathbb{Q}(\sqrt{-d})$ are ± 1 by Dirichlet's unit theorem, it follows that $3^m = u^2 + v^2 d$. If $v \neq 0$, we have $3^m \geq d > 3^g/2$ which can only happen if $m \geq g$. However, note that

$$(3^g) = (x^2 + d) = (x + \sqrt{-d})(x - \sqrt{-d})$$

Since $\mathfrak{p}$ and $\mathfrak{p}'$ are conjugate ideals, we must have $\mathfrak{p}^g = (x + \sqrt{-d})$. Thus, $m \mid g$, but this is impossible unless either $m = g$ or $v = 0$. In the latter case, $u^2 = 3^m$, but $m \mid g$ which means m is odd, a contradiction. Hence, $m = g$ and we are done. □

Putting everything together, we obtain the main result. The argument is adapted from section 3 of [1].

Theorem 4.1.5. For any odd $g > 2$, there are infinitely many imaginary quadratic fields K with $g \mid h(K)$.

Proof. Let N denote the number of $d = 3^g - x^2$ that are squarefree. By Lemma 4.1.3, we know $N \gg 3^{g/2}$. Moreover, by Lemma 4.1.4, we know from each of these d we obtain the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, that has an element of order g in its class group. Pick t large enough so that $g^t \nmid h(K)$ for all of these K. Then, we obtain a new set of quadratic fields with an element of order g in their class group, distinct from the ones already obtained. Repeating this argument yields infinitely many imaginary quadratic fields with an element of order g in the class group, so we are done. □

We end this section by proving a simple asymptotic lower bound on $N_g(X)^-$.

Theorem 4.1.6. $N_g(X)^- \gg X^{1/2}$.

Proof. Set $X = 3^g$; of course $d < 3^g = X$, and it follows from Lemma 4.1.3 and the argument of Theorem 4.1.5 that $N_g(X)^- \gg X^{1/2}$. □

We mention a better bound, due to Murty [40]:

Theorem 4.1.7 (Murty I)**.** Let $g \geq 3$. Then, $N_g(X)^- \gg X^{1/2+1/g}$.

The proof of Theorem 4.1.7 is quite technical so we do not reproduce it here. The basic idea Murty uses is to first bound the number of squarefree values of the quadratic polynomial $f(n) = n^2 + c$, then show that

if $d = m^g + n^2$, $\mathbb{Q}(\sqrt{-d})$ has an element of order g in its class group. Putting these together by setting $c = -m^g$ yields the desired result.

4.2 The real case

Set $d = x^{2g} + 4$ where x is some integer and $g > 2$ odd. In this section, we will show there are infinitely many real quadratic fields of the form $K = \mathbb{Q}(\sqrt{d})$ with $g \mid h(K)$ (if x satisfies certain conditions, see Lemma 4.2.3). The results in this section are due to [52].

Once again, we separate the argument into two steps. In the proof of Weinberger, the bounding step consists of showing there are infinitely many primes x such that $T^k - 4$ is irreducible modulo x for any odd k. This is quite different from Ankeny and Chowla's argument, but the idea is the same – the bounding step provides infinitely many x and consequently infinitely many d. The order g step then consists of showing that a particular ideal $\mathfrak{a}$ has order g in the class group of $\mathbb{Q}(\sqrt{d})$, for the infinitely many d so obtained. Since we are in the real quadratic case, we also need knowledge of the unit group in order to work with generators of principal ideals directly: in the proof of Lemma 4.1.4, we have used that imaginary quadratic fields have only finitely many units, which we cannot do in the real setting. Hence, we need to compute the fundamental unit of $\mathbb{Q}(\sqrt{d})$, which is accomplished in Proposition 4.2.2.

We begin by stating the following technical lemma, which we will use frequently in the rest of our argument, especially when working with expressions involving traces. This result is Lemma 3 of [52].

Lemma 4.2.1. Let $r, s \in \mathbb{Z}$ and denote by ρ_1, ρ_2 the roots of the polynomial $T^2 - rT - s = 0$. Define the quantity $c_j(r, s) = \rho_1^j + \rho_2^j$. Then,

(a) There are integers f_ν such that

$$c_j(r, s) = \sum_{\nu=0}^{\lfloor j/2 \rfloor} f_\nu r^{j-2\nu} s^\nu$$

If j is odd, then $f_0 = 1$ and $f_{(j-1)/2} = j$.

(b) When $r, s \geq 1$ and $j > 1$, then $c_j(r, s) \geq r^j$.

Proof. Note that

$$c_j(r, s) = rc_{j-1}(r, s) + sc_{j-2}(r, s) \tag{1}$$

with $c_0(r, s) = 2$ and $c_1(r, s) = r$. It follows that the f_ν must be rational, as we have

$$(r+s)^j = r^j + s^j + \sum_{k=1}^{j-1} \binom{j}{k} r^{j-k} s^k \implies c_j(r, s) = (r+s)^j - s^j - \sum_{k=1}^{j-1} \binom{j}{k} r^{j-k} s^k - \text{ (other terms)}$$

where we repeatedly use the binomial theorem to conclude that all the terms on the right-hand side have rational coefficients in the r and s. Now, by (1) and induction on j part (a) follows. Part (b) also follows similarly: the statement holds for $j = 2$ since $c_2(r, s) = r^2 + 2s \geq r^2$, and by induction on j, we have

$$c_{j+1}(r, s) = rc_j(r, s) + sc_{j-1}(r, s) \geq r^{j+1} + sr^{j-1} \geq r^{j+1}$$

where the first inequality uses the induction hypothesis, the second that $r, s \geq 1$. □

Now, we are able to compute the fundamental unit of $\mathbb{Q}(\sqrt{d})$. The following result is Lemma 4 of [52].

Proposition 4.2.2. Take x prime with $x > g$. Set $d = x^{2g} + 4$ and let $K = \mathbb{Q}(\sqrt{d})$. Suppose $K \neq \mathbb{Q}(\sqrt{5})$. Then, the fundamental unit of K is $\alpha = (x^g + \sqrt{d})/2$.

Proof. We can compute the norm and trace of α as in Example 1.2.2:

$$N(\alpha) = -1, \quad \mathrm{Tr}(\alpha) = x^g$$

Note that α is thus a unit, by Lemma 1.3.1. Let ε denote the fundamental unit of K which is normalised so that $\varepsilon > 1$ (see Example 1.3.3). Since ε generates the unit group, $\alpha = \varepsilon^j$ for some j. Moreover, α has norm -1, so ε must also have norm -1, and j must be odd. Write $\varepsilon = a + b\sqrt{d}$ and note that

$$-\frac{1}{\varepsilon} = -\frac{1}{a + b\sqrt{d}} = -\frac{a - b\sqrt{d}}{a^2 - b^2 d} = a - b\sqrt{d}$$

so $-1/\varepsilon$ is the image of ε under the embedding $K \to \mathbb{C}$ given by $x + y\sqrt{d} \mapsto x - y\sqrt{d}$ (see Example 1.2.4). Let $f_\varepsilon(T) = T^2 - rT - 1$ be the minimal polynomial of ε, and observe that by the above, $-1/\varepsilon$ is the second root of f_ε. In particular, since $\varepsilon > 1$, we must have $r = \mathrm{Tr}\,\varepsilon = \varepsilon - 1/\varepsilon > 0$. Let ρ_1 and ρ_2 denote the roots of f_ε, as in Lemma 4.2.3. We have

$$x^g = \mathrm{Tr}(\alpha) = \mathrm{Tr}(\varepsilon^j) = \rho_1^j + \rho_2^j = c_j(r, 1) \qquad (*)$$

where the third equality of $(*)$ follows because the minimal polynomial of ε^j is still quadratic, and must have $-1/\varepsilon^j$ as a root. Hence, $c_j(r, 1) = x^g$. From part (a) of Lemma 4.2.1, we know that $r \mid c_j(r, 1)$, since j is odd. Moreover, x is prime and $r \mid c_j(r, 1) = x^g$, so that $r = x^k$ for some $1 \leq k \leq g$. Note it is not possible that $r = 1$, because then $\varepsilon = (1 + \sqrt{5})/2$ and $K = \mathbb{Q}(\sqrt{5})$, but we have assumed this is not the case. Part (b) of Lemma 4.2.1 implies that $x^g = c_j(r, 1) \geq r^j = x^{jk}$, so that $g \geq jk$. Since j is odd, part (a) gives us that

$$\frac{c_j(r, 1)}{r} \equiv j \pmod{x}$$

where we use that $r = x^k$. Since x is prime with $x > g$, $g \geq jk$ implies that $\gcd(x, j) = 1$. Furthermore, $c_j(r, 1) = x^g$ and $r = x^k$, so $c_j(r, 1)/r = x^{g-k}$. However, the above congruence implies $\gcd(c_j(r, 1)/r, x) = 1$, so that $g = k$. It follows that $j = 1$ and $\varepsilon = \alpha$, as required. □

Now, we proceed to the bounding step. The following is adapted from Lemma 2 of [52].

Lemma 4.2.3. For any odd k, there are infinitely many primes p such that $P(T) = T^k - 4$ is irreducible mod p.

Proof. Let K be the splitting field of P over $\mathbb{Q}$. Note that P has no roots in $\mathbb{Q}$ (by eg. the rational root theorem) so $K \neq \mathbb{Q}$. Let $\alpha_i = \zeta_k^i \sqrt[k]{4}$, where ζ_k is a primitive k-th root of unity. Then, over K, P factors as

$$P(T) = (T - \alpha_1) \dots (T - \alpha_k)$$

Note that $K = \mathbb{Q}(\alpha_1, \dots, \alpha_k)$ by definition of a splitting field. Define the map σ on the generators of K by $\sigma(\alpha_i) = \alpha_{i+1}$. This must be a $\mathbb{Q}$-automorphism of K. Hence, σ is an element of $\mathrm{Gal}(K/\mathbb{Q})$. Note σ

has order k since ζ_k is a primitive root, and that σ acts transitively on the $\alpha_1, \ldots, \alpha_k$. That is, if we view $\mathrm{Gal}(K/\mathbb{Q})$ as a subgroup of S_k (via its action on the k roots of P), then $\mathrm{Gal}(K/\mathbb{Q})$ contains a k-cycle. By Chebotarev density, we deduce that there are infinitely many unramified primes p of $\mathbb{Q}$ such that the Artin symbol $(K/\mathbb{Q}, \mathfrak{p})$ is a member of the conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$ containing σ, where $\mathfrak{p}$ is a prime lying over p. In particular, this means that the Artin symbol $(K/\mathbb{Q}, \mathfrak{p})$ has order k. By Corollary 2.1.6, this implies $\overline{G}_{\mathfrak{p}|p} = \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p}/\mathbb{F}_p)$ is generated by an element of order k, so $|\overline{G}_{\mathfrak{p}|p}| = k = [(\mathcal{O}_K/\mathfrak{p}) : \mathbb{F}_p]$. Note that $P \bmod p$ is separable: since p is unramified in $K/\mathbb{Q}$ by assumption, it is also unramified in $\mathbb{Q}(\zeta_k)/\mathbb{Q}$, by Proposition 1.5.3 (since $\mathbb{Q}(\zeta_k) \subset K$). By Theorem 2.2.2 this implies $p \nmid k$, so $P \bmod p$ is separable. Moreover, $\alpha_1, \ldots, \alpha_k \in \mathcal{O}_K$ because they satisfy the integral equation $T^k - 4$, and consequently the reductions $\overline{\alpha}_1, \ldots, \overline{\alpha}_k$ modulo $\mathfrak{p}$ are in $\mathcal{O}_K/\mathfrak{p}$. Thus, $P \bmod p$ splits over $\mathcal{O}_K/\mathfrak{p}$. Since $[(\mathcal{O}_K/\mathfrak{p}) : \mathbb{F}_p] = k = \deg(P \bmod p)$, it follows that $\mathcal{O}_K/\mathfrak{p}$ is the splitting field of $P \bmod p$ over $\mathbb{F}_p$. Now, Proposition 4.5 of [38] implies that $P \bmod p$ is irreducible over $\mathbb{F}_p$ if and only if $\overline{G}_{\mathfrak{p}|p}$ acts transitively on the roots of $P \bmod p$. However, evidently $\overline{G}_{\mathfrak{p}|p}$ acts transitively on the k roots of $P \bmod p$ because it is generated by $\overline{\sigma}$. This completes the proof. □

Finally, we proceed to the order g step; that is, we will show $\mathbb{Q}(\sqrt{d})$ has an element of order g in the class group. Consider the ideal

$$\mathfrak{a} = (x^2, 2 + \sqrt{d})$$

We compute the norm of $\mathfrak{a}$:

$$\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right]/\mathfrak{a} = \frac{\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right]}{(x^2, 2+\sqrt{d})} \cong \frac{\mathbb{Z}[T]}{(T^2 - T - d/4, 2T+1, x^2)} \cong \frac{\mathbb{Z}[T]}{(2T+1, x^2)} \cong \mathbb{F}_{x^2}$$

where the final equality follows as x is assumed prime. Hence, $N(\mathfrak{a}) = x^2$. Next, we compute

$$\mathfrak{a}^g = (x^{2g}, x^{2g-2}(2+\sqrt{d}), \ldots, (2+\sqrt{d})^g) = (2+\sqrt{d}) \cdot (2 - \sqrt{d}, x^{2g-2}, \ldots, (2+\sqrt{d})^{g-1})$$

This shows $\mathfrak{a} \subset (2+\sqrt{d})$, and moreover we have $N(\mathfrak{a}^g) = x^{2g} = N((2+\sqrt{d})) = |N(2+\sqrt{d})|$, so we obtain an equality of ideals $\mathfrak{a}^g = (2+\sqrt{d})$. This implies the order of $\mathfrak{a}$ in the ideal class group divides g, so we are nearly done. It remains to show the order of $\mathfrak{a}$ in the ideal class group cannot be smaller than g. To this end, we state the following lemma, which is Theorem 1 of [52].

Lemma 4.2.4. Take g, x and d as in the previous lemma. Then, there are infinitely many x such that the order of $\mathfrak{a}$ in the class group of $\mathbb{Q}(\sqrt{d})$ is g when g is odd and $g/2$ when g is even.

Proof. By way of contradiction, let us suppose otherwise. That is, we suppose there exists an m dividing g such that $\mathfrak{a}^m = (\beta)$ is principal, so that $g = mk$ for some $k \geq 0$. Here, k must be either odd or 4, because we have assumed $m < g$ when g odd and $m < g/2$ when g even. We know that $\mathfrak{a}^g = (2+\sqrt{d})$, thus $(\beta)^k = (\beta^k) = (2+\sqrt{d})$. This implies

$$\beta^k = \pm(2+\sqrt{d})\alpha^j \tag{1}$$

for some j, since the generators of equal principal ideals can only differ by a unit. Note that j is determined completely modulo k because we can divide by any terms of the form α^k and (1) only changes upto a unit. We split into cases based on the value of k.

Suppose first that $k = 4$ (i.e. suppose g is even). Then, of course $\beta^4 > 0$ (since we are working in a real quadratic field), which implies the right-hand side of (1) is also positive. We compute

$$N(\beta^4) = N((2+\sqrt{d})\alpha^j) = (-1)^{j+1}x^{2g}$$

because $N(2+\sqrt{d}) = -x^{2g}$. Note the image of β^4 under the nontrivial embedding $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ is also positive, so the norm $N(\beta^4)$ must also be by Proposition 1.2.5. In particular, j must be one of ± 1. Expanding out (1), we can thus write down an expression for β^4, taking $b = (-1)^{(j-1)/2}$:

$$\beta^4 = \frac{x^{2g} + 2bx^g + 4 + (2 + bx^g)\sqrt{d}}{2} \tag{2}$$

One can see that $\beta^4 \notin \mathbb{Q}$ (because $2+bx^g \neq 0$ by choice of x), which means $\beta \notin \mathbb{Q}$. Note that $N(\beta) = \pm x^{g/2}$, and thus the minimal polynomial of β takes the form $T^2 - rT \pm x^{g/2}$, where $r = \mathrm{Tr}(\beta)$. We can compute the trace of β^4 from (2) (see Example 1.2.2):

$$\mathrm{Tr}(\beta^4) = x^{2g} + 2bx^g + 4$$

so we have

$$x^{2g} + 2bx^g + 4 = \mathrm{Tr}(\beta^4) = c_4(r, \pm x^{g/2}) = r^4 \pm 4x^{g/2}r^2 + 2x^g \tag{3}$$

using Lemma 4.2.1. Here, the second equality follows using the same argument as in the third equality of $(*)$ of the previous lemma. Suppose $j = 1$, then (3) implies

$$x^{2g} + 4 = r^4 \pm 4x^{g/2}r^2 \implies r^2 = (x^{g/2} \pm 1)^2 + 1$$

which has no solutions for $x \geq 2$. Suppose that $j = -1$, then (3) implies

$$(x^g - 2)^2 + 4x^g = (r^2 \pm 2x^{g/2})^2$$

We recall that x was chosen prime and larger than g, so in particular x is odd. Reducing modulo 8, we thus obtain a contradiction: since $x^g - 2$ is odd, $(x^g-2)^2$ can only be 1 mod 8, and $4x^g$ can only be 4 mod 8. Hence, $\mathfrak{a}$ must have order $g/2$.

Suppose next k is odd. That is, we are supposing that g is odd and $\mathfrak{a}$ has order m, so that $g = mk$. In this case, we can absorb the possible extra minus sign of (1) in the $\pm$ into β. Define the sequences (of integers) (y_n) and (z_n) by the following:

$$\frac{y_i + z_i\sqrt{d}}{2} := (2+\sqrt{d})\alpha^i$$

for $i \geq 0$. Evidently $y_0 = 4$ and $z_0 = 2$. We claim that $y_i \equiv 4 \bmod x$ and $z_i \equiv 2 \bmod x$ for all i. We proceed by induction: suppose the claim holds for some $i > 0$. Then, we have

$$\frac{y_{i+1} + z_{i+1}\sqrt{d}}{2} = (2+\sqrt{d})\alpha^{i+1} = \alpha \cdot \frac{y_i + z_i\sqrt{d}}{2}$$

and expanding on both sides, we obtain expressions for y_{i+1} and z_{i+1}:

$$\begin{aligned} y_{i+1} &= \frac{x^g y_i + z_i d}{2}, & z_{i+1} &= \frac{x^g z_i + y_i}{2} \\ &= \frac{x^g(y_i + x^g z_i)}{2} + 2z_i & &= \frac{x^g z_i}{2} + \frac{y_i}{2} \\ &\equiv 0 + 2 \cdot 2 = 4 & &\equiv \frac{4}{2} = 2 \pmod{x} \end{aligned}$$

where we have used the induction hypothesis in the final congruences. This shows our claim; in particular $z_i \neq 0$ for $i \geq 0$. Thus, $\beta = y_j/2 + (z_j/2)\sqrt{d}$ is not rational, because $z_j \neq 0$. Consequently, β has minimal polynomial of the form $T^2 - rT \pm x^{2g/k}$, and so

$$y_j = \mathrm{Tr}(\beta^k) = c_k(r, \pm x^{2g/k})$$

Since k is odd, part (b) of Lemma 4.2.1 implies

$$c_k(r, \pm x^{2g/k}) \equiv r^k = y_j \equiv 4 \pmod{x}$$

Let e be the maximal odd divisor of g and let x be one of the infinitely many primes for which $T^e - 4$ is irreducible modulo x from Lemma 4.2.3. Note that k divides e, as k too is an odd divisor of g. Then, if there exists a solution to the above equation; that is, if there exists an r_0 such that $r_0^k \equiv 4 \bmod x$, then $T^k - 4$ factors as

$$(T^k - 4) = (T - r_0)f(T) \equiv (T - r_0)f(T) \pmod{x} \tag{4}$$

for some polynomial $f \in \mathbb{Z}[T]$. In particular, it follows that

$$T^e - 4 = (T^{e/k} - 4)f(T^{e/k}) \equiv (T^{e/k} - 4)f(T^{e/k}) \pmod{x}$$

by substituting $T = T^{e/k}$ into (4). This contradicts Lemma 4.2.3, so we conclude that $\mathfrak{a}$ indeed has order g. Moreover, this argument shows that there are infinitely many prime x for which $d = x^{2g} + 4$ has an element of order g in its class group. □

Theorem 4.2.5. For any odd $g > 2$, there are infinitely many real quadratic fields K with $g \mid h(K)$.

Proof. From the previous lemma, we have obtained infinitely many x and therefore infinitely many d such that $\mathbb{Q}(\sqrt{d})$ has an element of order g in its class group. It remains to show only finitely many of these $\mathbb{Q}(\sqrt{d})$ so obtained are the same. That is, given $b > 0$ squarefree, we need to show there are only finitely many x such that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{b})$. Suppose $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{b})$, then there exists an integer y such that

$$d = x^{2g} + 4 = by^2.$$

This equation has only finitely many solutions in x and y by [39, Chapter 28, Theorem 4][1]. Hence, there are indeed infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with $g \mid h(K)$. □

We end this section by mentioning an asymptotic lower bound on $N_g(X)^+$, due to Murty [40]:

[1] One could also for instance use Faltings' theorem [21].

Theorem 4.2.6 (Murty II)**.** Let $g \geq 3$. Then, $N_g(X)^+ \gg X^{1/2g-\varepsilon}$ for any $\varepsilon > 0$.

Proof sketch. The idea here is to modify Lemma 4.2.3 to obtain a bound on the number of prime ideals $\mathfrak{p}$ so that $T^k - 4$ is irreducible modulo $\mathfrak{p}$, see [40, Theorem 2]. □

Remark 4.2.7. It is interesting to note that the conditions on x in the above argument (i.e. x needs to be prime such that $T^k - 4$ is irreducible modulo x, see Lemma 4.2.3) are too restrictive. See Ichimura [28], who showed that the class number of $K = \mathbb{Q}(\sqrt{x^{2g}+4})$ is divisible by g for any $g \geq 2$ and any odd $x \geq 3$. We speculate that Ankeny and Chowla were quite close to this result, as they show in Theorem 2 of [1] that if $d = x^{2g} + 1$ is squarefree, the class number of the real quadratic field $K = \mathbb{Q}(\sqrt{d})$ is divisible by g, for $g > 4$. However, they are unable to show there are infinitely many such squarefree d.

Chapter 5

Quadratic fields with high p-rank

In this chapter, we study the p-rank of the class group. A lot can be said about the 2-part of the class group of a quadratic number field. For instance, we have shown (Theorem 3.1.15) that the number of generators of the 2-part can be determined by the number of odd primes dividing the field discriminant. The remaining part of the class group is not so well understood. Yamamoto [53] was the first to show that there are infinitely many imaginary quadratic fields with a subgroup of the form $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$ in their class groups, for any $g \geq 2$. Later on, Craig [18] was able to show there exist infinitely many quadratic fields with 3-rank at least 3. Explicit examples of class groups with 3-rank 3 and 4 were subsequently given by Diaz y Diaz [19]. Tools from the theory of elliptic curves have also been used to tackle this problem, for instance by Mestre [36], whose method we will cover briefly in section 5.2.

Our primary motivation in this chapter is that the p-rank of the class group is of significance in the class field tower problem, and we will discuss this connection briefly in section 5.1. In section 5.2, we compute examples of imaginary quadratic fields with 5-rank equal to 3 using Mestre's method of [36], thus providing a negative solution to the class field tower problem. Finally, in section 5.3, we prove a lower bound on the p-rank of the class group of a general number field of degree n, due to Connell and Sussman [15].

Let us define the notion of p-rank and p-part. By the fundamental theorem for finitely generated abelian groups [50, Theorem IX.3.1], any finite abelian group G decomposes as the direct product of cyclic groups as

$$G \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{k_n}\mathbb{Z}$$

where the p_i are (not necessarily distinct) primes. We say the *p-part* of G is the direct product of the factors with order divisible by p, denoted by G_p. The p-part of G can therefore be viewed as a finite-dimensional vector space over $\mathbb{F}_p$. The *p-rank* of G is defined as the number of factors in this decomposition whose order is divisible by p, or equivalently, the dimension of G_p over $\mathbb{F}_p$ as a vector space.

5.1 Motivation: the class field tower problem

Recall the class number problem (see the discussion at the end of section 1.4), that asks which quadratic number fields K have $h(K) = 1$. Instead of this, we can rather ask the weaker question: which quadratic

fields K can be embedded into a number field L with $h(L) = 1$? We will call this the **embeddability problem**. It turns out that the answer to this question is linked to the Hilbert class field of chapter 2.

One can iterate the Hilbert class field of K by inductively taking $\mathbb{H}^m(K) = \mathbb{H}(\mathbb{H}^{m-1}(K))$ for $m \geq 2$. We obtain the tower of fields

$$K = \mathbb{H}^0(K) \subset \mathbb{H}(K) \subset \cdots \subset \mathbb{H}^m(K) \subset \cdots \subset \mathbb{H}^\infty(K)$$

where $\mathbb{H}^\infty(K)$ is the union of the fields $\mathbb{H}^m(K)$ for all $m \geq 1$. We call this the *class field tower* of K. One says the class field tower *stabilizes* if $\mathbb{H}^\infty(K)$ is a finite extension of K, or equivalently, if there exists an index $m \geq 1$ such that $\mathbb{H}^{m+1}(K) = \mathbb{H}^m(K)$. The problem of determining for which K this tower stabilizes is the **class field tower problem**. Solving this problem is in fact equivalent to solving the embeddability problem, as the following theorem will show:

Theorem 5.1.1. Let K be a number field. There exists a finite extension L/K with $h(L) = 1$ if and only if the class field tower of K stabilizes.

Proof. Suppose the class field tower of K stabilizes, i.e. there exists some $m \geq 0$ so that $\mathbb{H}(\mathbb{H}^m(K)) = \mathbb{H}^m(K)$, and by Artin reciprocity, this implies $h(\mathbb{H}^m(K)) = [\mathbb{H}^{m+1}(K) : \mathbb{H}^m(K)] = 1$, so K can be embedded into $L = \mathbb{H}^m(K)$ which is a finite extension of K with class number 1. For the forward direction, see [44, Proposition 1]. □

The solution to the class field tower problem was given by Golod and Shafarevich [26] in 1964 using the theory of cohomology of groups, applied specifically to p-groups (groups with order p^n for prime p). Their main theorem is the following group-theoretic result:

Theorem 5.1.2 ([26])**.** Let G be a finite p-group. Let d denote the minimal number of generators $g_1, \ldots, g_d$ of G, and let r denote the minimal number of relations in the g_i such that G has a finite presentation

$$G = \langle g_1, g_2, \ldots, g_d \mid \xi_1, \xi_2, \ldots, \xi_r \rangle$$

Then, $r > \frac{(d-1)^2}{4}$.

Let us sketch briefly why this result is useful in our context. One defines the *Hilbert p-class field* $\mathbb{H}_p(K)$ as the maximal abelian extension of K whose Galois group over K is a p-group. Analogously to the class field tower construction, we can make the *Hilbert p-class field tower* of K

$$K = \mathbb{H}_p^0(K) \subset \mathbb{H}_p(K) \subset \cdots \subset \mathbb{H}_p^m(K) \subset \cdots \subset \mathbb{H}_p^\infty(K)$$

The point of defining the p-class field tower is that $\mathbb{H}_p^\infty(K)/K$ is a subextension of $\mathbb{H}^\infty(K)/K$ by definition, so the class field tower of K does not stabilize if the p-class field tower does not stabilize for some p.

A year prior to publishing Theorem 5.1.2, Shafarevich published the following result in the setting of imaginary quadratic number fields:

Theorem 5.1.3 ([47])**.** Let $G = \mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ for K a imaginary quadratic number field and let r and d be for G as in Theorem 5.1.2. We have $r - 1 \leq d$.

Let K be imaginary quadratic and suppose the p-class field tower of K stabilizes. Applying Theorem 5.1.2 to $G = \mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ and combining it with the above theorem, we have $d+1 \geq r \geq (d-1)^2/4$, which is a contradiction if $d \geq 7$. Note that since $\mathbb{H}_p(K)$ is defined as the maximal unramified extension of K with Galois group a p-group, it follows by applying multiplicativity of field extension degrees repeatedly that $\mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ is also a p-group, so we can set $d = d_p\mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$. By Galois theory, $\mathrm{Gal}(\mathbb{H}_p(K)/K) \subset \mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$, and by Artin reciprocity, $\mathrm{Gal}(\mathbb{H}(K)/K) \cong \mathrm{Cl}(K)$. In particular, the p-part of $\mathrm{Cl}(K)$ is isomorphic to $\mathrm{Gal}(\mathbb{H}_p(K)/K)$, because $\mathbb{H}_p(K)$ is the maximal unramified extension of K whose Galois group is a p-group. So $\mathbb{H}_p(K)$ is also the maximal subextension of $\mathbb{H}(K)$ whose Galois group is a p-group. Thus, we have $d_p\mathrm{Cl}(K) \leq d$, so if $d_p\mathrm{Cl}(K) \geq 7$, the class field tower of K does not stabilize.

By the results of chapter 3, we can make the 2-rank of the class group of a quadratic number field high: recall Theorem 3.1.15 which says the 2-rank of the class group is $\mu - 1$, where μ is as in the theorem. The constant μ is at least r, where r is the number of odd prime factors of the field discriminant. Hence, we can produce examples of quadratic number fields with 2-class field tower that does not stabilize by providing discriminants with lots of odd prime divisors. Golod and Shafarevich in [26] gave the (obvious) example $K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$, which has 7 odd prime factors in its discriminant. The 2-class field tower of K does not stabilize, which yields a negative solution to the class field tower problem.

Thus, we have seen (one reason) why one should care about the problem of finding quadratic number fields with high p-rank – to provide a negative solution to the class field tower, and hence the embeddability problem.

5.2 Constructing quadratic fields with high p-rank

In this section, we are primarily motivated by the following refinement of Golod and Shafarevich's theorems, proved by Koch and Venkov [51] in 1978:

Theorem 5.2.1. Let K be a quadratic number field and p an odd prime. If $d_p\mathrm{Cl}(K) \geq 3$, then the class field tower of K does not stabilize.

In light of this theorem, we want to find an example of a number field K with $d_p\mathrm{Cl}(K) \geq 3$ for an odd prime p. In this section, we will do this for $p = 5$ by implementing a method due to Mestre [36] that is able to produce explicit examples of imaginary quadratic fields K with $d_5\mathrm{Cl}(K) \geq 3$. This method involves constructing two unramified extensions of K from a particular elliptic curve; we do not need to establish the required geometry, so we do not do this here. For the reader's benefit, we sketch the method briefly below, using some terminology from elliptic curves freely. We direct the reader to [48] for an introduction to elliptic curves. For our purposes, we will say the following. An elliptic curve over $\mathbb{Q}$ is given by a polynomial equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the coefficients are rational numbers. If (x, y) is a point on an elliptic curve with $x \in \mathbb{Q}$ (but $y \notin \mathbb{Q}$), then $\mathbb{Q}(y)$ is a quadratic number field.

Sketch of Mestre's method. Let F be an elliptic curve defined over $\mathbb{Q}$ with a point P of rational coordinates with order 5. One then defines $E = F/\langle P \rangle$ and considers the isogeny $\phi : F \to E$. Choose

a point (x, y) on E with $x \in \mathbb{Q}$ and $y \notin \mathbb{Q}$ and define the quadratic number field $K = \mathbb{Q}(y)$. Mestre shows that under certain conditions on x, the coordinates of the points in the preimage $\phi^{-1}(x, y)$ generate an unramified extension L of K that is cyclic of degree 5, cf. [36, Proposition II.1.3]. This extension is unramified, so must be contained in the Hilbert class field of K. By Galois theory, one has $\mathbb{Z}/5\mathbb{Z} = \mathrm{Gal}(L/K) \subset \mathrm{Gal}(\mathbb{H}(K)/K)$, and by Artin reciprocity, it follows that $\mathrm{Cl}(K)$ has 5-rank at least 1.
Now, to find quadratic fields with 5-rank at least 2, Mestre takes two distinct points (x_1, y) and (x_2, y) on E, and shows that (under certain conditions, cf. [36, Proposition II.2.2]) the preimages $\phi^{-1}(x_1, y)$ and $\phi^{-1}(x_2, y)$ yield two independent[1] unramified cyclic extensions of K of degree 5, L_1 and L_2. Artin reciprocity implies that $\mathrm{Cl}(K)$ has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, hence 5-rank at least 2. Finally, Mestre computes a polynomial such that $\mathbb{Q}(y) = \mathbb{Q}(\sqrt{M(t)})$, see [46, Section 2] for the details. See [36, Section 1] for an explanation of why the method works.

In this section, we follow the work of Schoof [46]. Schoof obtains the polynomial $M(t)$ as

$$M(t) = -(t^2 + t + 1)(47t^6 + 21t^5 + 598t^4 + 1561t^3 + 1198t^2 + 261t + 47)$$

and computes the class groups of $K = \mathbb{Q}(\sqrt{M(t)})$ for various t. We implement this method in PARI (see the appendix) and search over $t = p/q$, for $1 \leq p, q \leq 750$. We have not taken into account the second hypothesis of [36, Proposition II.2.2] as Schoof says (and we confirm) that numerical evidence suggests it is needless in practice, as we still obtain a large fraction of fields with 5-rank at least 2. The quadratic fields found with 5-rank at least 3 are listed in Table 5.1. We obtain 61678 nonisomorphic such examples, which provide negative solutions for the class field tower problem. We also obtain examples with $d_5\mathrm{Cl}(K) = 1$ and 2, and there are 64342 and 215265 of these respectively; see the appendix.

Here, the first column denotes the structure of the 5-part of $\mathrm{Cl}(K)$: the tuple $(k_1, k_2, \ldots, k_n)$ corresponds to the decomposition $\mathbb{Z}/5^{k_1}\mathbb{Z} \times \mathbb{Z}/5^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/5^{k_n}\mathbb{Z}$ of the 5-part into cyclic groups. The second column is the smallest (absolute) discriminant found with that 5-part structure, and the third column is the number of fields found with that 5-part structure.

It is interesting to note that Schoof was only able to find 356 examples with only one of 5-rank equal to 4, which highlights the computing advances since the 1980's. As far as the author knows, there have been no published attempts to use Mestre's method with present-day computing power to find fields with 5-rank equal to 5 or larger (but other methods have been used, see for instance [4]). Moreover, a vast majority of the fields found this way have 5-rank at least 2: over 80%. It is unclear why this is the case, as we have neglected the second hypothesis of [36, Proposition II.2.2]. This possibly indicates that this hypothesis in Mestre's result can be weakened considerably. Notably, we find the field $K = \mathbb{Q}(\sqrt{-258559351511807})$ which has $d_5\mathrm{Cl}(K) = 4$, the smallest such example (ordered by $|\mathrm{disc}(K)|$). This is the only field found by Schoof with this 5-rank. With current computing power, it may be possible to use Mestre's method to obtain examples with 5-rank equal to 5 or even 6; these computations were only run for a few hours on a laptop computer, so using large-scale computing power could yield more interesting examples. Moreover, one could also obtain a different $M(t)$ starting with a different choice of elliptic curve, however we have not done this.

[1] One identifies the extensions L_1/K and L_2/K with the surjective maps $\mathrm{Gal}(\mathbb{H}(K)/K) \to \mathrm{Gal}(L_{1/2}/K)$ given by Galois theory. Hence, the extensions can be viewed as elements of $\mathrm{Hom}(\mathrm{Gal}(\mathbb{H}(K)/K), \mathbb{Z}/5\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{Z}/5\mathbb{Z})$ and are independent in this sense.

$\mathrm{Cl}_5(K)$	Smallest $\lvert\mathrm{disc}(K)\rvert$	# such K
$(1,1,1)$	18397407	46091
$(2,1,1)$	2048074559	12021
$(2,2,1)$	661334988497867039	114
$(3,1,1)$	477720858639	2291
$(3,2,1)$	2467652431976493743	23
$(4,1,1)$	16704202367	489
$(4,2,1)$	1293386534251356799753007	2
$(5,1,1)$	48180709664244527	104
$(5,2,1)$	88545331234505436097007	2
$(6,1,1)$	1228669972810270151	13
$(7,1,1)$	61701811292996648375279	3
$(9,1,1)$	459420647791509399591303519	1
$\#K$ with $d_5\mathrm{Cl}(K)=3$		$=$ **61154**
$(1,1,1,1)$	258559351511807	378
$(2,1,1,1)$	855964398235866239	113
$(3,1,1,1)$	894927652104957167	27
$(4,1,1,1)$	187499156194883596210959	4
$(2,2,1,1)$	346788457969070542368639	1
$(3,2,1,1)$	175290027080887236724970 87	1
$\#K$ with $d_5\mathrm{Cl}(K)=4$		$=$ **524**

Table 5.1: Imaginary quadratic K from Mestre's method with $d_5\mathrm{Cl}(K) \geq 3$

5.3 A lower bound for the p-rank

Recall Shafarevich's lower bound on $d = d_p\mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ from section 5.1:

Theorem 5.1.3 (Shafarevich)**.** Let $G = \mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ for K a imaginary quadratic number field. Let d denote the minimal number of generators $g_1, \ldots, g_d$ of G, and let r denote the minimal number of relations in the g_i such that G has a presentation $\langle g_1, \ldots, g_d \mid \xi_1, \ldots, \xi_r \rangle$. Then, $r - 1 \leq d$.

In this section, we prove the following lower bound on the p-rank of a general number field, in the spirit of Shafarevich's result.

Theorem 5.3.1. Let p be prime and L/K be an extension of number fields. Then,

$$d_p\mathrm{Cl}(L) \geq d_p\mathrm{Cl}(K) + t_{L/K} - (w_{L/K} + d_pU_L - d_pU_K)$$

This theorem was originally due to Roquette and Zassenhaus [45], but the version above is a refinement due to Connell and Sussman [15]. Here, we present the proof given in [15].

Let us setup the notation used in the statement of the theorem. Let L and K be number fields with L/K a finite extension and let p be a fixed prime. We define the following two subgroups of $K^\times$:

- R_K: the group of p-th powers in $K^\times$.
- G_K: the group of elements $\alpha \in K^\times$ such that $(\alpha) = A^p$ for A some fractional ideal of K.

Note that $R_K \subset G_K$ and the unit group $U_K \subset G_K$, because units generate the ideal (1). Next, we define

$$w_{L/K} := \dim \frac{K^* \cap R_L}{R_K}$$

where the dimension is understood as a vector space over $\mathbb{F}_p$. All subsequent dimensions should also be understood this way.

Next, we let $t_{L/K}$ be the number of prime ideals $\mathfrak{p}$ of K satisfying

(i) $\mathfrak{p}$ becomes a p-th power in L, i.e., $\mathfrak{p} = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ of L,

(ii) there exists a c coprime to p such that $\mathfrak{p}^c$ is principal in K.

The number $t_{L/K}$ is finite, since if a prime $\mathfrak{p}$ of K becomes a p-th power in L, it ramifies (with ramification index divisible by p), and there can only be finitely many ramified primes in L/K by Theorem 1.5.8.

If G is a finite abelian group, we define the subgroup $G^p = \{x \in G \mid x^p = 1\}$. Note that G^p is a subgroup of the p-part of G, and hence can be viewed as a vector space over $\mathbb{F}_p$. Moreover, the decomposition of G^p into cyclic groups has the same number of factors as the same decomposition for G_p, so $d_p G = \dim G^p$.

We begin the proof of Theorem 5.3.1 with the following lemma:

Lemma 5.3.2. There is an injective homomorphism

$$\frac{K^\times \cap G_L}{K^\times \cap R_L U_L} \hookrightarrow \mathrm{Cl}^p(L)$$

where $\mathrm{Cl}^p(L)$ is the subgroup of $\mathrm{Cl}(L)$ consisting of the elements with order p, as defined above.

Proof. For any $\alpha \in G_L$, there exists a fractional ideal A of L with $(\alpha) = A^p$. This defines a map $\varphi : G_L \to \mathrm{Cl}(L)$ by $\varphi(\alpha) = [A]$, where $[A]$ is the ideal class of A in the class group. In fact, since $[A]$ has order either 1 or p in $\mathrm{Cl}(L)$, it follows φ is a map $G_L \to \mathrm{Cl}^p(L)$. Note that φ is a homomorphism: let $\alpha, \beta \in G_L$ such that $(\alpha) = A^p$ and $(\beta) = B^p$, then

$$(\alpha\beta) = (\alpha)(\beta) = A^p B^p = (AB)^p$$

where the final equality follows since $\mathcal{O}_L$ is commutative. This shows $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. We claim the kernel of φ is $R_L U_L$. Take $\alpha \in R_L U_L$ and write $\alpha = \beta\gamma$, with $\beta \in R_L$ and $\gamma \in U_L$. One sees that $(\alpha) = (\beta\gamma) = (\beta)$ since units generate the ideal (1). However, β is a p-th power in L, and consequently the ideal (β) is also a p-th power. Hence, α gets sent to the trivial class in $\mathrm{Cl}^p(L)$ under φ. Conversely, if $\alpha \in \ker\varphi$, $\varphi(\alpha)$ is the trivial class in $\mathrm{Cl}^p(L)$, so $(\alpha) = (\beta)^p$ for some $\beta \in L^\times$. Thus, $\alpha = \beta^p\gamma$, where $\gamma \in U_L$, and it follows that $\alpha \in R_L U_L$. We thus obtain an injective homomorphism

$$\frac{G_L}{R_L U_L} \hookrightarrow \mathrm{Cl}^p(L)$$

This homomorphism is in fact surjective because any ideal class $[A] \in \mathrm{Cl}^p(L)$ has order either 1 or p; that is, either A is principal or A^p is. In either case, A^p is principal, so there exists $\alpha \in G_K$ with $(\alpha) = A^p$ by definition. Note that $K^\times \cap G_L$ is a subgroup of G_L (by eg. the second isomorphism theorem), and that $K^\times \cap R_L U_L$ is a subgroup of $R_L U_L$. It follows that $(K^\times \cap G_L)/(K^\times \cap R_L U_L)$ is a subgroup of $G_L/(R_L U_L)$,

whence we have an injective homomorphism

$$\frac{K^\times \cap G_L}{K^\times \cap R_L U_L} \hookrightarrow \frac{G_L}{R_L U_L} \cong \mathrm{Cl}^p(L)$$

which completes the proof of the lemma. □

The above lemma implies that

$$d_p \mathrm{Cl}(L) \geq \dim \frac{K^\times \cap G_L}{K^\times \cap R_L U_L}.$$

Hence, to prove Theorem 5.3.1 it suffices to provide a lower bound for the term on the right. We will do this by constructing appropriate exact sequences with $(K^\times \cap G_L)/(K^\times \cap R_L U_L)$ as a member. The following two results about exact sequences shall be helpful:

Proposition 5.3.3. Suppose the sequences of groups $1 \to A \to B \xrightarrow{f} C \to 1$ and $1 \to C \xrightarrow{g} D \to E \to 1$ are exact. Then, the sequence $1 \to A \to B \xrightarrow{g \circ f} D \to E \to 1$ is exact as well.

Proof. It is enough to check that the new sequence is exact at B and D. Note that g is injective by exactness of the sequence $1 \to C \xrightarrow{g} D \to E \to 1$. Consequently, $\ker(g \circ f) = \ker(f)$, so the new sequence is indeed exact at B. Moreover, the sequence $1 \to A \to B \xrightarrow{f} C \to 1$ is exact, so f is surjective. That is, $f(B) = C$, so that $(g \circ f)(B) = g(C)$, which shows exactness at D. □

Proposition 5.3.4. Let k be a field and

$$1 \to V_1 \to V_2 \to \cdots \to V_n \to 1$$

be an exact sequence of k-vector spaces. Then, we have

$$\sum_{i=1}^{n} (-1)^i \dim V_i = 0.$$

Proof. Denote the maps from $V_i \to V_{i+1}$ as f_i, with f_0 the first map in the sequence and f_n the last. By rank-nullity, one has $\dim V_i = \dim \ker f_i + \dim f_i(V_i)$. In particular,

$$\sum_{i=1}^{n} (-1)^i \dim V_i = \sum_{i=1}^{n} (-1)^i \dim \ker f_i + \sum_{i=1}^{n} (-1)^i \dim f_i(V_i).$$

The sequence is exact, so $\ker f_{i+1} = f_i(V_i)$. Putting this together yields the result. □

In order to use the above propositions, we will construct appropriate exact sequences, with $(K^\times \cap G_L)/(K^\times \cap R_L U_L)$ as a member. This is done as follows: note that by the third isomorphism theorem for groups, we have the isomorphisms

$$\frac{K^\times \cap R_L U_L}{R_K U_K} \cong \frac{(K^\times \cap R_L U_L)/R_K}{(R_K U_K)/R_K} = \frac{K^\times \cap R_L U_L}{R_K} \Big/ \frac{R_K U_K}{R_K}$$

$$\frac{K^\times \cap G_L}{K^\times \cap R_L U_L} \cong \frac{(K^\times \cap G_L)/R_K U_K}{(K^\times \cap R_L U_L)/R_K U_K} = \frac{K^\times \cap G_L}{R_K U_K} \Big/ \frac{K^\times \cap R_L U_L}{R_K U_K}$$

which yields the two short exact sequences

$$1 \to \frac{R_K U_K}{R_K} \to \frac{K^\times \cap R_L U_L}{R_K} \to \frac{K^\times \cap R_L U_L}{R_K U_K} \to 1$$
$$1 \to \frac{K^\times \cap R_L U_L}{R_K U_K} \to \frac{K^\times \cap G_L}{R_K U_K} \to \frac{K^\times \cap G_L}{K^\times \cap R_L U_L} \to 1$$

By Proposition 5.3.3, we can put these together to obtain the exact sequence

$$1 \to \frac{R_K U_K}{R_K} \to \frac{K^\times \cap R_L U_L}{R_K} \to \frac{K^\times \cap G_L}{R_K U_K} \to \frac{K^\times \cap G_L}{K^\times \cap R_L U_L} \to 1 \tag{1}$$

Let us denote the groups in (1) as V_1, V_2, V_3 and V_4 respectively from left-to-right. Then, Proposition 5.3.4 yields that

$$\dim V_4 = \dim V_3 - \dim V_2 + \dim V_1$$

By the second isomorphism theorem, we have

$$V_1 = \frac{R_K U_K}{R_K} \cong \frac{U_K}{R_K \cap U_K} = \frac{U_K}{U_K^p} \tag{2}$$

where $R_K \cap U_K = U_K^p$ because $R_K \cap U_K$ consists of precisely the p-th powers in U_K. It follows that $\dim V_1 = d_p U_K$.

Now, we need to compute the dimensions of V_3 and V_2. This is once again done by constructing appropriate exact sequences: by the third isomorphism theorem, one has

$$\frac{K^\times \cap G_L}{G_K} \cong \frac{(K^\times \cap G_L)/(R_K U_K)}{G_K/(R_K U_K)} = \frac{K^\times \cap G_L}{R_K U_K} \Big/ \frac{G_K}{R_K U_K}$$
$$\frac{K^\times \cap R_L U_L}{K^\times \cap R_L} \cong \frac{(K^\times \cap R_L U_L)/R_K}{(K^\times \cap R_L)/R_K} = \frac{K^\times \cap R_L U_L}{R_K} \Big/ \frac{K^\times \cap R_L}{R_K}$$

which gives the following exact sequences

$$1 \to \frac{G_K}{R_K U_K} \to \frac{K^\times \cap G_L}{R_K U_K} \to \frac{K^\times \cap G_L}{G_K} \to 1$$
$$1 \to \frac{K^\times \cap R_L}{R_K} \to \frac{K^\times \cap R_L U_L}{R_K} \to \frac{K^\times \cap R_L U_L}{K^\times \cap R_L} \to 1$$

By Proposition 5.3.4, the first exact sequence yields

$$\dim V_3 = \dim \frac{G_K}{R_K U_K} + \dim \frac{K^\times \cap G_L}{G_K} = d_p \mathrm{Cl}(K) + \dim \frac{K^\times \cap G_L}{G_K}$$

The second equality follows from the argument of Lemma 5.3.2. The second exact sequence yields

$$\dim V_2 = \dim \frac{K^\times \cap R_L}{R_K} + \dim \frac{K^\times \cap R_L U_L}{K^\times \cap R_L} = w_{L/K} + \dim \frac{K^\times \cap R_L U_L}{K^\times \cap R_L}$$

Moreover, we have an injection

$$\frac{K^\times \cap R_L U_L}{K^\times \cap R_L} \hookrightarrow \frac{R_L U_L}{R_L}$$

so that by (2),

$$\dim \frac{K^\times \cap R_L U_L}{K^\times \cap R_L} \leq d_p U_L$$

We are now nearly done, it remains only to show that

$$\dim \frac{K^\times \cap G_L}{G_K} \geq t_{L/K}$$

which we accomplish by way of the following lemma:

Lemma 5.3.5. Let D be the group generated by the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ counted in the definition of $t = t_{L/K}$. Then, there is an injective homomorphism

$$\frac{D}{D^p} \hookrightarrow \frac{K^\times \cap G_L}{G_K}$$

Proof. By condition (ii) defining $t_{L/K}$, for each of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ there exists an integer c_i coprime to p such that $\mathfrak{p}_i^{c_i}$ is principal. Take $c = \operatorname{lcm}_i c_i$. For any fractional ideal $\mathfrak{q} \in D$, $\mathfrak{q}^c$ is principal, say $\mathfrak{q}^c = (\beta)$ for some $\beta \in K^\times$. Note that $\beta \in G_L$ as well by condition (i) defining the $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. We can thus define a map $D \to K^\times \cap G_L$ by $\mathfrak{q} \mapsto \beta$. This map is well-defined upto the units of $\mathcal{O}_K$, so we obtain a homomorphism by considering the map

$$\phi : D \to \frac{K^\times \cap G_L}{U_K}, \qquad \mathfrak{q} \mapsto \beta U_K.$$

Let $\mathfrak{q}_1, \mathfrak{q}_2 \in D$ with $\mathfrak{q}_1^c = (\beta)$ and $\mathfrak{q}_2^c = (\beta')$. We see that $(\mathfrak{q}_1\mathfrak{q}_2)^c = \mathfrak{q}_1^c\mathfrak{q}_2^c = (\beta)(\beta') = (\beta\beta')$, so ϕ is indeed a homomorphism. Since $U_K \subset G_K$ (noted at the beginning of the section), we obtain a homomorphism $D \to (K^\times \cap G_L)/G_K$ by composing ϕ with the inclusion map. Denote this new homomorphism by φ. It is now enough to show the kernel of φ is D^p. Suppose $\mathfrak{q} \in \ker \varphi$. Then, $\mathfrak{q}^c = (\gamma)$, where $\gamma \in G_K$. Hence, there exists a fractional ideal $\mathfrak{a}$ of K such that $\mathfrak{q}^c = \mathfrak{a}^p$, and since c is coprime to p, it follows $\mathfrak{q} = B^p$ for some fractional ideal B of K. Consequently, $\mathfrak{q} \in D^p$ and so $\ker \varphi \subset D^p$. The other inclusion follows as if $\mathfrak{q} \in D^p$ then $\mathfrak{q} = \mathfrak{a}^p$ for some $\mathfrak{a} \in D$. But then $\mathfrak{q}^c = (\gamma)$ is the p-th power of some fractional ideal of K, so $\gamma \in G_K$. This completes the proof. □

The desired inequality follows from the lemma. We claim each of the $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are in distinct classes in the quotient group D/D^p. Suppose otherwise that there are some $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are related as $\mathfrak{p}_i = \mathfrak{a}\mathfrak{p}_j$ where $\mathfrak{a} \in D^p$. But this is a contradiction: $\mathfrak{p}_i = \mathfrak{a}\mathfrak{p}_j \subset \mathfrak{p}_j$, but $\mathfrak{p}_i$ is maximal as $\mathcal{O}_K$ is Dedekind. Hence, it follows that

$$\dim \frac{K^\times \cap G_L}{G_K} \geq \dim \frac{D}{D^p} = t_{L/K},$$

which completes the proof of Theorem 5.3.1.

We note that the definition of $t_{L/K}$ is quite restrictive – $t_{L/K}$ counts the number of primes $\mathfrak{p}$ of K where *each* $\mathfrak{p}$ has ramification index divisible by p – so there is still room for improvement in the bound of Theorem 5.3.1. In fact, Martin [34] recently provided a refinement of Theorem 5.3.1.

Discussion

In this thesis, we have studied various aspects of the divisibility of the class numbers of quadratic number fields. In order to do so, we have first explored the basics of algebraic number theory and class field theory. In this final chapter, we will discuss possible future directions that could be taken from the research in this thesis. We also briefly describe some open questions related to our work.

Chapter 2 discusses a very simple version of class field theory. As we have mentioned, it is possible to introduce new ideas to incorporate extensions with ramification into the theory, see [42, Chapter 6]. There are many analytic aspects of the theory we have neglected as well, see [42, Chapter 7]. As discussed, the main theme of class field theory is that abelian extensions can be classified using congruence conditions (cf. the discussion after Theorem 2.4.1). For nonabelian extensions, the story is much more complicated. The famous Langlands programme can be thought of as the non-abelian extension of class field theory.

Chapter 3 discusses the theory of binary quadratic forms and establishes an isomorphism between the group of reduced forms of discriminant d and the (narrow) class group of $\mathbb{Q}(\sqrt{d})$. It is natural to ask whether analogues of this correspondence exist for number fields of degree $n > 2$. In his PhD thesis and following series of articles [5, 6, 7, 8], Bhargava develops analogues of Gauss' composition law for $n = 3, 4, 5$. Further research could be done aiming to obtain divisibility results using Bhargava's work.

In chapter 4, we have shown there are infinitely many quadratic fields with class number divisible by g, for any $g \geq 2$. In 1984, Azuhata and Ichimura [3] extended this result to number fields of arbitrary degree. We have also mentioned estimates on $N_g(X)^{-/+}$ by Murty [40]. Other authors have proved refinements of Murty's results, see Soundarajan [49] for the imaginary case and Yu [54] for the real case. In 2005, Bilu and Luca [10] proved an analogous estimate for number fields of arbitrary degree. There have been analogous divisibility results and estimates to those in chapter 4 for quadratic function fields in the literature. Quadratic function fields are extensions of $\mathbb{F}_q$ of the form $\mathbb{F}_q(T, \sqrt{D})$ where T is transcendental over $\mathbb{F}_q$ and D is a monic irreducible polynomial in $\mathbb{F}_q[T]$. See for instance the work of Cardon, Murty [12] and Chakraborty, Mukhopadhyay [13]. There has also been much interest in the complementary problem of *indivisibility*: given $g \geq 2$, how many quadratic fields have class number not divisible by g? Hartung [27] showed there are infinitely many such fields for any odd prime. There have been various refinements and generalizations, particularly using geometric methods, see for instance work by Ono, Skinner [43] and Kohnen, Ono [30].

In chapter 5, we have considered the problem of finding quadratic fields with high p-rank. Our discussion of this problem has been quite limited. This is because the modern approach to this problem uses tools from algebraic geometry and the theory of elliptic curves, as we have seen with Mestre's method. The ideas behind Mestre's method of section 5.2 have appeared frequently in the literature, see for instance Mestre

[35], Gillibert and Levin [25] and Kulkarni [31]. In a recent survey, Gillibert and Levin [24] discussed a new perspective unifying the results of Yamamoto [53] and Craig [18], which used only the theory developed in this thesis, and the results of Mestre [35] and Gillibert, Levin [25] which were all results using algebraic geometry. Remarkably, this unified perspective is able to easily provide stronger quantitative versions of these results: for instance, Theorem 2.5 of [24] states:

Theorem. There exist $\gg \dfrac{X^{1/11}}{\log X}$ imaginary quadratic fields K with $|\mathrm{disc}(K)| < X$ such that $d_5\mathrm{Cl}(K) \geq 3$.

which is a quantitative version of Theorem 1 in Mestre's paper [35].

It may also be interesting to perform large-scale computational searches using Mestre's methods with different choices of elliptic curves, with the aim of obtaining examples of imaginary quadratic fields with 5-rank ≥ 5. Mestre in [35] has shown there are infinitely many (real or imaginary) quadratic number fields of 5-rank ≥ 3, by constructing a certain elliptic curve. This uses an extension of the method we have discussed in section 5.2, and notably the author is unable to find a computational search undertaken using the results of [35].

Instead of looking at the p-rank of the class group, one could instead try to estimate the size of the p-part of the class group. In fact, bounds for the size of the p-part of the class group are an active area of research. For any number field K of degree n and any prime p, it is conjectured that the size $h_p(K)$ of the p-part of the class group of K satisfies $h_p(K) = O_\varepsilon(|\mathrm{disc}(K)|^\varepsilon)$ for any $\varepsilon > 0$ [9]. Here, the notation $f(x) = O_\varepsilon(g(x))$ means there exists an x_0 such that there that $|f(x)| \leq C(\varepsilon)|g(x)|$ for $x \geq x_0$. The first significant results towards this conjecture were obtained by Ellenberg and Venkatesh [20], who obtained the best-known bound $h_p(K) = O_\varepsilon(|\mathrm{disc}(K)|^{1/3+\varepsilon})$ for $(n,p) = (2,3)$ and $(3,3)$. Bhargava et al. [9] provided the first nontrivial bounds for $(n,2)$ with $n > 2$. Recently, Chan and Koymans [14] have provided a refinement of Ellenberg and Venkatesh's results in the case $(n,p) = (2,3)$.

Bibliography

[1] Nesmith Ankeny and S Chowla. "On the divisibility of the class number of quadratic fields". In: *Pacific Journal of Mathematics* 5.3 (1955), pp. 321–324.

[2] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. 1969.

[3] Takashi Azuhata and Humio Ichimura. "On the divisibility problem of the class numbers of algebraic number fields". In: *J. Fac. Sci. Univ. Tokyo* 30 (1984), pp. 579–585.

[4] Christian Bagshaw et al. "Improved methods for finding imaginary quadratic fields with high n-rank". In: *LuCaNT: LMFDB, Computation, and Number Theory* 796 (2023), p. 1.

[5] Manjul Bhargava. "Higher composition laws I: A new view on Gauss composition, and quadratic generalizations". In: *Annals of Mathematics* 159.1 (2004), pp. 217–250.

[6] Manjul Bhargava. "Higher composition laws II: On cubic analogues of Gauss composition". In: *Annals of mathematics* 159.2 (2004), pp. 865–886.

[7] Manjul Bhargava. "Higher composition laws III: The parametrization of quartic rings". In: *Annals of mathematics* 159.3 (2004), pp. 1329–1360.

[8] Manjul Bhargava. "Higher composition laws IV: The parametrization of quintic rings". In: *Annals of Mathematics* 167.1 (2008), pp. 53–94.

[9] Manjul Bhargava et al. "Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves". In: *Journal of the American Mathematical Society* 33.4 (2020), pp. 1087–1099.

[10] Yuri F Bilu and Florian Luca. "Divisibility of class numbers: enumerative approach". In: (2005).

[11] Duncan A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer, 1989.

[12] David A Cardon and M Ram Murty. "Exponents of class groups of quadratic function fields over finite fields". In: *Canadian Mathematical Bulletin* 44.4 (2001), pp. 398–407.

[13] Kalyan Chakraborty and Anirban Mukhopadhyay. "Exponents of class groups of real quadratic function fields". In: *Proceedings of the American Mathematical Society* 132.7 (2004), pp. 1951–1955.

[14] Stephanie Chan and Peter Koymans. "A new pointwise bound for 3-torsion of class groups". In: *arXiv preprint arXiv:2505.00611* (2025).

[15] Ian Connell and David Sussman. "The p-dimension of class groups of number fields". In: *Journal of the London Mathematical Society* 2.3 (1970), pp. 525–529.

[16] Keith Conrad. *Cyclotomic extensions*. Expository paper. URL: `https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf`.

[17] David A. Cox. *Primes of the form $x^2 + ny^2$*.

[18] Maurice Craig. "A type of class group for imaginary quadratic fields". In: *Acta Arithmetica* 22.4 (1973), pp. 449–459.

[19] F Diaz y Diaz. "On some families of imaginary quadratic fields". In: *Mathematics of Computation* 32.142 (1978), pp. 637–650.

[20] Jordan S. Ellenberg and Akshay Venkatesh. "Reflection Principles and Bounds for Class Group Torsion". In: *Int. Math. Res. Not.* (Jan. 2007). DOI: 10.1093/imrn/rnm002.

[21] Gerd Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". In: *Inventiones Mathematicae* 73 (1983), pp. 349–366.

[22] Dennis Garbanati. "Class field theory summarized". In: *Rocky Mountain Journal of Mathematics* 11.2 (1981).

[23] Carl Friedrich Gauss. *Disquistiones Arithmeticae*. Springer-Verlag, 1986.

[24] Jean Gillibert and Aaron Levin. "A geometric approach to large class groups: a survey". In: *Class groups of number fields and related topics* (2020), pp. 1–15.

[25] Jean Gillibert and Aaron Levin. "Pulling back torsion line bundles to ideal classes". In: *arXiv preprint arXiv:1109.3723* (2011).

[26] Evgeniy Solomonovich Golod and Igor Rostislavovich Shafarevich. "On the class field tower". In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 28.2 (1964). In Russian, pp. 261–272.

[27] Paul Hartung. "Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3". In: *Journal of Number Theory* 6.4 (1974), pp. 276–278.

[28] Humio Ichimura. "Note on the class numbers of certain real quadratic fields". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*. Vol. 73. 1. Springer. 2003, pp. 281–288.

[29] Kiran Kedlaya. *Notes on class field theory*. Course notes. 2025. URL: https://kskedlaya.org/papers/cft-ptx.pdf.

[30] Winfried Kohnen and Ken Ono. "Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication". In: *Inventiones Mathematicae* 135.2 (1999), pp. 387–398.

[31] Avinash Kulkarni. "An explicit family of cubic number fields with large 2-rank of the class group". In: *arXiv preprint arXiv:1610.07668* (2016).

[32] Hendrik W Lenstra and Peter Stevenhagen. "Artin reciprocity and Mersenne primes". In: *Nieuw Archief voor Wiskunde* 1 (2000), pp. 44–54.

[33] Daniel Marcus. *Number fields*. Springer.

[34] Daniel E Martin. "Lower bounds on the l-rank of ideal class groups". In: *arXiv preprint arXiv:2501.09865* (2025).

[35] Jean-Francois Mestre. "Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3". In: (June 1992). DOI: 10.48550/arXiv.alg-geom/9206006. eprint: alg-geom/9206006.

[36] Jean-François Mestre. "Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques". In: *Seminaire de Théorie des Nombres de Bordeaux* 9 (1980). In French. URL: http://eudml.org/doc/182069.

[37] James S. Milne. *Algebraic Number Theory (v3.08)*. 2020.

[38] James S. Milne. *Fields and Galois Theory (v5.10)*. 2022.

[39] Louis Mordell. *Diophantine equations*. 1969.

[40] M Ram Murty. "Exponents of class groups of quadratic fields". In: *Topics in Number Theory: In Honor of B. Gordon and S. Chowla*. Springer, 1999, pp. 229–239.

[41] M Ram Murty. *Problems in algebraic number theory*. 2005.

[42] Jurgen Neukirch. *Algebraic Number Theory*.

[43] Ken Ono and Christopher Skinner. "Fourier Coefficients of Half-Integral Weight Modular Forms Modulo l". In: *Annals of Mathematics* 147.2 (1998), pp. 453–470. URL: http://www.jstor.org/stable/121015.

[44] Peter Roquette. "On class field towers". In: *Algebraic Number Theory*. Ed. by John Cassels and Albrecht Fröhlich. 1967.

[45] Peter Roquette and Hans Zassenhaus. "A class rank estimate for algebraic number fields". In: *Journal of the London Mathematical Society* 1.1 (1969), pp. 31–38.

[46] René Schoof. "Class groups of complex quadratic fields". In: *Mathematics of Computation* 41.163 (1983), pp. 295–302. URL: http://eudml.org/doc/152884.

[47] IR Shafarevich. "Extensions with prescribed ramification points". In: *Publ. Math., Inst. Hautes Études Sci* 18 (1963). In Russian, pp. 71–95.

[48] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2009.

[49] K Soundararajan. "Divisibility of class numbers of imaginary quadratic fields". In: *Journal of the London Mathematical Society* 61.3 (2000), pp. 681–690.

[50] Jaap Top. *Group theory*. Lecture notes. 2016.

[51] Boris B Venkov and Helmut Koch. "The p-tower of class fields for an imaginary quadratic field". In: *Journal of Soviet Mathematics* 9 (1978), pp. 291–299.

[52] Peter J Weinberger. "Real quadratic fields with class numbers divisible by n". In: *Journal of Number Theory* 5 (1973), pp. 237–241.

[53] Yoshihiko Yamamoto. "On unramified Galois extensions of quadratic number fields". In: *Osaka Journal of Mathematics* 41 (1970), pp. 471–478.

[54] Gang Yu. "A note on the divisibility of class numbers of real quadratic fields". In: *Journal of Number Theory* 97.1 (2002), pp. 35–44.

Appendix A

Algorithms and data

A.1 Algorithms from Chapter 3

```
def isReduced(Q):
  [a,b,c]=Q
  if gcd(gcd(a, b), c) != 1:
    return False
  if abs(b) > a or c < a:
    return False
  elif (abs(b) == a or a == c) and b < 0:
    return False
  else:
    return True
```

Algorithm A.1: Algorithm to check whether a given form is reduced

```
def computeReduced(Q):
  [a,b,c]=Q
  if b*b - 4*a*c > 0:
    raise Exception("The form is indefinite")
  while abs(b) > a or c < a:
    disc = b*b - 4*a*c
    if c < a:
      tmp = a
      b = -b
      a = c
      c = tmp
    elif abs(b) > a:
      m = floor((a-b) / (2*a))
      b = b + 2 * m * a
      c = (b*b - disc) / (4 * a)
  return [a, b, c]
```

Algorithm A.2: Algorithm to compute the reduction of a given form

```
def computeClassNum(D):
```

```
  if D > 0:
    raise Exception("Algorithm does not work for real discriminants")
  if D % 4 == 2 or D%4==3:
    D = 4 * D
  a = 1
  h = 0
  lst = []
  while a <= floor(sqrt(-D/3)):
    for b in range(-a, a+1):
      c = (b*b-D)/(4*a)
      if c == int(c):
        print(a, b, c)
        if isReduced([a, b, int(c)]):
          lst.append([a, b, int(c)])
    a += 1
  return lst
```

Algorithm A.3: Algorithm to compute all the reduced forms with a given discriminant D

A.2 Algorithms and data from Chapter 5

```
M(t) = -(t^2 + t + 1) * (47*t^6 + 21*t^5 + 598*t^4 + 1561*t^3 + 1198*t^2 + 261*
    t + 47);
results = [];
{
for(p = 1,100,
for(q = 2,100,
  if(gcd(p,q)!=1, next);
  m = M(p/q);
  P = polredbest(x^2-m);
  D = nfinit(P).disc;
  C = quadclassunit(D);
  gens = C.cyc;
  p_factors = select(x -> x > 0, [valuation(x, 5) | x <- gens]);
  p_rank = #p_factors;
  output = [p/q, m, D, p_factors, p_rank];
  results = concat(results, [output]);
);
);
}
print(results);
```

Algorithm A.4: Mestre's algorithm to compute high 5-ranks

$\mathrm{Cl}_5(K)$	Smallest $\lvert\mathrm{disc}(K)\rvert$	# such K
(1)	1007	51417
(2)	1799	10359
(3)	183387287	2044
(4)	1833559327767	406
(5)	16058759	85
(6)	80411276355782567	24
(7)	489386848212469500839	6
(9)	10586972100296734802567	1
$\#K$ with $d_5\mathrm{Cl}(K) = 1$		$=$ **64342**
$(1,1)$	11199	158384
$(2,1)$	40137767	45287
$(2,2)$	2865830079	25
$(3,1)$	75979223	9205
$(3,2)$	115647158802373585239	4
$(4,1)$	10368869999	1869
$(4,2)$	16466555883220076567	1
$(5,1)$	1449192975839	408
$(6,1)$	2937871683555287	70
$(7,1)$	230652637114126219887	11
$(8,1)$	3183780676090583329322159	1
$\#K$ with $d_5\mathrm{Cl}(K) = 2$		$=$ **215265**
$(1,1,1)$	18397407	46091
$(2,1,1)$	2048074559	12021
$(2,2,1)$	661334988497867039	114
$(3,1,1)$	477720858639	2291
$(3,2,1)$	2467652431976493743	23
$(4,1,1)$	16704202367	489
$(4,2,1)$	1293386534251356799753007	2
$(5,1,1)$	48180709664244527	104
$(5,2,1)$	88545331234505436097007	2
$(6,1,1)$	1228669972810270151	13
$(7,1,1)$	61701811292996648375279	3
$(9,1,1)$	459420647791509399591303519	1
$\#K$ with $d_5\mathrm{Cl}(K) = 3$		$=$ **61154**
$(1,1,1,1)$	258559351511807	378
$(2,1,1,1)$	855964398235866239	113
$(3,1,1,1)$	894927652104957167	27
$(4,1,1,1)$	187499156194883596210959	4
$(2,2,1,1)$	346788457969070542368639	1
$(3,2,1,1)$	175290027080887236724970 87	1
$\#K$ with $d_5\mathrm{Cl}(K) = 4$		$=$ **524**

Table A.1: Data from Mestre's algorithm for $t = p/q$ where $1 \leq p, q \leq 750$