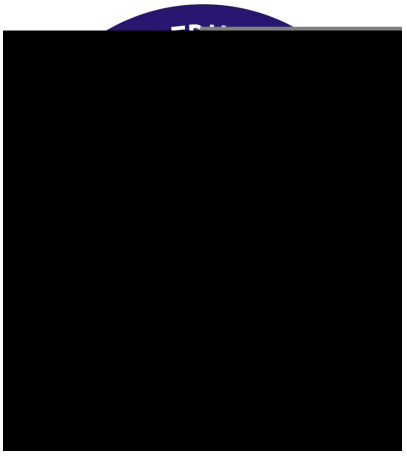
A Study of Quadratic Number Fields

Simran Tinani

A dissertation submitted for the partial fulfilment

of BS-MS dual degree in Science



Indian Institute of Science Education and Research Mohali

April 2018

Certificate of Examination

This is to certify that the dissertation titled **A Study of Quadratic Number Fields** submitted by **Simran Tinani** (Reg. No. MS13010) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Abhik Ganguli | Dr. Amit Kulshrestha | Prof. Kapil Hari Paranjape (Supervisor)

Dated: April 20, 2018

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Prof. Kapil Hari Paranjape at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Simran Tinani
(Candidate)

Dated: April 20, 2018

In my capacity as the supervisor of the candidates project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Prof. Kapil Hari Paranjape
(Supervisor)

Acknowledgment

I would first like to thank my thesis advisor Prof. Kapil Hari Paranjape of the Mathematics department at Indian Institute of Science Education and Research Mohali, for his valuable guidance and inputs, and also for the initial ideation of this project. Prof. Kapil has been supportive, helpful, and patient throughout the one year course of this thesis project. He has allowed me a great amount of independence in my work, while also providing direction when necessary.

The freedom I have had in my thesis research has allowed me to shape this project to best suit my interests and capabilities, and the regular supervision and inputs by Prof. Kapil have helped me maintain the rigour and quality of my work. I also acknowledge Prof. Kapil for his approachable and friendly demeanour, and for the fun facts, anecdotes, and mathematical jokes that he often told me. These conversations with him not only taught me a lot, but also relieved my stress and uplifted my mood.

I would also like to thank the experts who were involved in the validation survey for this research project: Dr. Abhik Ganguli and Dr. Amit Kulshrestha. I especially acknowledge them for their patience and insightful questions during my first thesis presentation.

I also thank the entire community of IISER Mohali: the director, administration, faculty, staff, and students, for helping maintain a highly intellectual and stimulating academic environment, as well as a warm and comfortable social environment at IISER Mohali.

I further acknowledge my parents and friends for their constant encouragement, support, and unwavering faith in me. The strength and comfort I have received from the people close to me have played a big role in my successful completion of this thesis.

Notation

$\mathbb{I}$	Identity Matrix(in appropriate dimensions)
$\mathbf{Z}$	The ring of integers
$\mathbf{Q}$	The field of rational numbers
$\mathbf{C}$	The field of complex numbers
$Gal(L/K)$	The Galois group of the field extension $K \subseteq L$
$\frac{\mathbf{Z}}{\mathbf{nZ}}$	The cyclic group of order n
$\mathcal{O}_K$	The ring of integers of the field K
d_K	The fundamental discriminant of number field K
$H(K)$	The ideal class group of number field K
h_K	The class number of number field K

Abstract

The goal of this project is to form an understanding of quadratic number fields of both positive and negative discriminants D, and in particular, their class groups. We begin by establishing a correspondence between the ideal class group and the form class group, which consists of equivalence classes of binary quadratic forms. We further explore Gauss's class number problems and use the correspondence established to compute class numbers for different values of the discriminant D, and to derive other results about the structure of the ideal class group. We then look at the splitting of prime ideals in field extensions of a Dedekind domain, and then apply this theory specifically to prime numbers in $\mathbf{Q}$ to obtain their prime ideal factorizations in quadratic number fields. The theory of ramification of prime numbers is then used as background knowledge to further study the ideal class group, and derive various results on the class number. In particular, unramified field extensions are studied in detail. The Hilbert class field is briefly introduced.

Contents

Notation **4**

Abstract **5**

1 Pre-requisite Knowledge **8**
1.1 Fields and Galois Theory 8
1.2 Quadratic Number Fields and Rings of Integers 10
1.2.1 Ring of Integers is Finitely-Generated 10
1.2.2 DVR's and Dedekind Domains 12

2 Binary Quadratic Forms **14**
2.1 Introduction 14
2.2 Reduction of primitive positive definite forms 15
2.3 Reduction of primitive indefinite forms 19
2.3.1 Algorithm to Reduce Primitive Indefinite Forms 20
2.3.2 Algorithm: Determination of a complete set of representatives of $SL_2(\mathbf{Z})$-equivalence classes of indefinite forms with given discriminant $D > 0$ 20
2.4 The Form Class Group 21
2.5 Primes represented by forms 22

3 The Picard Group and Narrow Picard Group **23**
3.1 Orders 23
3.2 Ideals of Orders and Invertibility 24
3.3 Picard Groups and Class Numbers 25
3.4 Narrow Picard Groups 26

4 Associating Binary Quadratic Forms and Ideals **27**
4.1 Associating Binary Quadratic Forms to Ideals 27
4.1.1 Two Correctly Ordered Bases Produce Equivalent Forms . . . 28
4.2 Associating Ideals to Binary Quadratic Forms 29

5 Using the two points of view **30**
5.1 Gauss composition law and the group structure 30
5.2 Explicit Determination of Picard Group 32
5.2.1 Computing the Picard Group for d = -47 32
5.2.2 Computing the Picard group for d = 12 33

5.3 Class numbers 34
5.3.1 Units, automorphisms, Pell's equation 35
5.4 On Gauss's Class Number Problems: Some Computations 35
5.4.1 Class Number 13 and Some Techniques 37

6 Splitting of Prime Ideals in Field Extensions 40
6.1 Introduction 40
6.2 The Chebotarev Density Theorem 45
6.3 Ramification in Number Fields 49
6.3.1 Ramification in Quadratic Number Fields 52

7 Factorization of the Class Number 56
7.1 Class numbers of fields with discriminant having only two odd prime factors 56
7.2 The Hilbert Class Field:
A Brief Introduction 60
7.2.1 Properties of the Hilbert Class Field 62
7.3 Unramified Extensions of Quadratic Number Fields 62

Chapter 1

Pre-requisite Knowledge

In the chapter below we state a number of results without proofs. Some common references are [1], [2], and [3].

1.1 Fields and Galois Theory

Let K be a field and F an extension field of K. This means that F is a vector space over K, $\dim_K(F) = [F : K]$,

$$1_K = 1_F$$

Recall that if $u \in F$ is algebraic over K, then

- $K(u) = K[u]$
- $K(u) \cong \frac{K[x]}{(f)}$ where f is the minimal polynomial of u and $\deg f = n$
- $[K(u) : K] = n$
- $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of $K(u)$ over K

Also recall that a finite-dimensional extension field of K is finitely-generated (as a ring over K) and algebraic.

Definition 1.1.1 (K-homomorphism)**.** Let E and F be extension fields of K. A nonzero map

$$\sigma : E \to F$$

which is both a field and a K-module homomorphism is called a K-homomorphism.

It is easy to see that a field homomorphism σ is a K-homomorphism if and only if it fixes K element-wise. K-automorphisms are defined similarly.

Definition 1.1.2 (Galois Group of F over K)**.** The Galois group of a field extension F over K is defined as the group of all $K-$ automorphisms of F, i.e.

$$Gal(F/K) = Aut_K F$$

Theorem 1.1.1. *Let F be an extension field of K and $f \in K[x]$. If $u \in F$ is a root of f and $\sigma \in Aut_K F$, then $\sigma(u)$ is also a root of f.*

Note that $F = K \Rightarrow Aut_K F = 1$. However, the converse is not true. For example, take

$$K = \mathbf{Q}, F = \mathbf{Q}(\sqrt[3]{2}) \neq \mathbf{Q}$$

Here, $F \neq K$ but $Aut_K F = 1$ because the only possible images of $\sqrt[3]{2}$ under an automorphism are the roots of $x^3 - 2$ (by the above theorem), the other two of which are complex.

Definition 1.1.3 (Fixed field, Galois Extension)**.** Let F be an extension field of K and E be an intermediate field. Let H be a subgroup of $Aut_K F$. Then,

1. $F^H = \{v \in F \mid \sigma(v) = v, \forall\ \sigma \in H\}$ is an intermediate field of the extension $K \subset F$
2. $Aut_E F = \{\sigma \in Aut_K F \mid \sigma(u) = u, \forall\ u \in E\}$ is a subgroup of $Aut_K F$

F^H is called the fixed field of H in F. F is called a Galois extension of K if the fixed field of $Aut_K F$ is K.

Theorem 1.1.2 (Fundamental Theorem of Galois Theory)**.** *Let F, K, H, F^H, E, $Aut_E F$ be as above. If F is Galois over K, then the correspondence*

$$H \to F^H$$

is a bijection from the set of subgroups of $Gal(F/K) := Aut_K F$ to the set of subfields of the extension $K \subset F$, and its inverse is given by the map $E \to Aut_E F$.

Definition 1.1.4 (Splitting Field)**.** Let K be a field, $f \in K[x]$ be a polynomial of positive degree. An extension field F of K is said to be a splitting field over K of f if f **splits in** $F[x]$, and $F = K(u_1, u_2, \ldots, u_n)$, where $u_1, u_2, \ldots, u_n$ are the roots of f in F. $F \supseteq K$ is said to be a splitting field over K of the set S of polynomials if every polynomial in S splits in $F[x]$ and F is generated over K by the roots of all polynomials in S. If S is finite and $S = \{f_1, f_2, \ldots, f_n\}$, then a splitting field of S is the same as a splitting field of the single polynomial $f = f_1 f_2 \ldots f_n$.

Definition 1.1.5 (Galois Closure)**.** The Galois Closure of extension $K \subseteq F$ in a fixed algebraic closure $\bar{F}$ is a field which is minimal among all Galois extensions of F containing K, i.e. it is the intersection of all Galois extensions of F containing K.

Definition 1.1.6 (Separable Extensions)**.** A separable extension is an algebraic field extension $E \supset F$ such that for every $\alpha \in E$, the minimal polynomial of α over F is a separable polynomial, i.e., its formal derivative is not zero when evaluated at any of its roots, or equivalently, its roots are distinct in an algebraic closure of K. An extension that is not separable is said to be inseparable.

Definition 1.1.7 (Normal Extensions)**.** An algebraic field extension $L \supset K$ is called normal (we also say that L is normal over K) if every monic irreducible polynomial over K that has at least one root in L, splits over L. In other words, if $\alpha \in L$, then all conjugates of α over K (i.e., all roots of the minimal polynomial of α over K) belong to L.

1.2 Quadratic Number Fields and Rings of Integers

Definition 1.2.1 (Number Field)**.** An algebraic number field, or simply a number field, is a finite degree extension of the field $\mathbf{Q}$ of rational numbers.

Definition 1.2.2 (Quadratic Number Field)**.** A degree two number field is called a quadratic number field.

Theorem 1.2.1. *Every quadratic number field is of the form* $\mathbf{Q}(\sqrt{d})$ *where* d *is a square-free integer.*

Let L be a field and A be a ring such that $A \subseteq L$.

Definition 1.2.3. An element $\alpha \in L$ is said to be integral over A if α satisfies a nonzero monic polynomial equation with coefficients in A.

Theorem 1.2.2. *An element* $\alpha \in L$ *is integral over* A *if and only if* $A[\alpha]$ *is a finitely generated* A*-module. Consequently, the set of elements of* L *that is integral over* A *constitutes a ring.*

Definition 1.2.4 (Integral Closure)**.** The integral closure of A in L is the ring of elements of L integral over A.

A is called integrally closed if it is its own integral closure in its field of fractions.

Proposition 1.2.1. *A UFD is integrally closed.*

Proposition 1.2.2. *Let* K *be the field of fractions of* A *and* L *a finite extension field of* K*. Assume that* A *is integrally closed. Then, an element* $\alpha \in L$ *is integral over* A *if and only if its minimal polynomial over* K *had coefficients in* A*.*

Theorem 1.2.3. *The ring of integers of a number field is integrally closed.*

1.2.1 Ring of Integers is Finitely-Generated

In this subsection, we prove that the ring of integers $\mathcal{O}_K$ is a finitely generated $\mathbf{Z}$-module. Let A be an integrally closed Noetherian domain with field of fractions K. Let L be a separable and finite field extension of K, and let B be the integral closure B of A in L.

Proposition 1.2.3. *Let* A *be an integrally closed domain with field of fractions* K*, and let* B *be the integral closure of* A *in a separable extension* L *of* K *of degree* m*. There exist free* A*-submodules* M *and* M' *of* L *such that*

$$M \subseteq B \subseteq M'$$

Thus, B *is a finitely generated* A*-module if* A *is Noetherian, and it is free of rank* m *if* A *is a PID.*

Corollary 1.2.1. *The ring of integers in a number field* L *is the largest subring that is finitely generated as a* $\mathbf{Z}$*-module.*

Proof. Apply the above proposition to the special case where $A = \mathbf{Z}$, $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{d})$) to conclude that the ring of integers $\mathcal{O}_K$ is a finitely generated $\mathbf{Z}$-module. It is known to also be a subring. Moreover, if $B \subseteq K$ is any finitely generated $\mathbf{Z}$-module, any element of B must be integral over $\mathbf{Z}$, and thus $B \subseteq \mathcal{O}_K$. □

Remark 1.2.1. *Since $\mathcal{O}_K$ is finitely generated over $\mathbf{Z}$, every ideal of it is also finitely generated (as an ideal). Thus, it is a Noetherian ring.*

Definition 1.2.5 (Integral Basis)**.** When K is a number field (i.e. a finite extension of $\mathbf{Q}$), a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ for $\mathcal{O}_K$ as a $\mathbf{Z}$-module is called an integral basis for K.

Definition 1.2.6. Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ for $\mathcal{O}_K$ be an integral basis of $\mathcal{O}_K$ and let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of embeddings (injective homomorphisms) of K into the complex numbers. The **discriminant** d_K of K is the square of the determinant of the n by n matrix B whose (i, j)-entry is $\sigma_i(b_j)$.

$$\Delta_K = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & \vdots & \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{pmatrix}^2$$

Equivalently, the trace from K to $\mathbf{Q}$ can be used. Specifically, define the trace form to be the matrix whose (i, j)-entry is $Tr_{K/Q}(b_i b_j)$. This matrix equals $B^T B$, so the discriminant of K is the determinant of this matrix.

Theorem 1.2.4. *Let K be a quadratic field. Let m be the unique square-free integer such that $K = \mathbf{Q}(\sqrt{m})$. Then, the set $\mathcal{O}_K$ of algebraic integers in K is given by*

$$\mathcal{O}_K = \begin{cases} \mathbf{Z} + \mathbf{Z}(\sqrt{m}), & \text{if } m \equiv 2, 3 \pmod 4, \\ \mathbf{Z} + \mathbf{Z}(\frac{1+\sqrt{m}}{2}), & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

Thus, an integral basis for the quadratic field $\mathbf{Q}(\sqrt{m})$ is $[1, \theta]$, where $\theta = \sqrt{m}$ if $m \equiv 2, 3 \pmod 4$ and $\theta = \frac{1+\sqrt{m}}{2}$ if $m \equiv 1 \pmod 4$.

A simple computation also shows that the discriminant d_K of K is given by

$$d_K = \begin{cases} 4m, & \text{if } m \equiv 2, 3 \pmod 4, \\ m, & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

Definition 1.2.7 (Fundamental Discriminant)**.** An integer which is the discriminant of a quadratic field is called a fundamental discriminant.

Clearly, d is a fundamental discriminant if and only if $d \equiv 1 \pmod 4$ and d is squarefree, or $d = 4k$ where $k \in \mathbf{Z}$ squarefree such that $k \equiv 2, 3 \pmod 4$.

There exists a unique quadratic number field for every fundamental discriminant.

Theorem 1.2.5 (Units of Imaginary Quadratic Fields)**.** *Let K be an imaginary quadratic field and let $U(\mathcal{O}_K)$ denote the group of units of its ring of integers $\mathcal{O}_K$. Then*

$$U(\mathcal{O}_K) = \begin{cases} \{\pm 1, \pm i\} \cong \mathbf{Z}_4, & if K = \mathbf{Q}(\sqrt{-1}) \\ \{\pm 1, \pm\omega, \pm\omega^2\} \cong \mathbf{Z}_6, & if K = \mathbf{Q}(\sqrt{-3}) \\ \{\pm 1\} \cong \mathbf{Z}_2, & otherwise \end{cases}$$

1.2.2 DVR's and Dedekind Domains

Definition 1.2.8 (Dedekind Domain)**.** A Dedekind domain is an integral domain A such that

1. A is Noetherian
2. A is integrally closed
3. Every nonzero prime ideal of A is maximal

Proposition 1.2.4. *Localizations of Dedekind domains are Dedekind.*

Theorem 1.2.6. *$\mathcal{O}_K$ is a Dedekind domain for any algebraic number field K.*

Definition 1.2.9 (Basis of an ideal)**.** Let K be an algebraic number field of degree n. Let I be a nonzero ideal of $\mathcal{O}_K$. If $\{\eta_1, \ldots, \eta_n\}$ is a set of elements of I such that every element $\alpha \in I$ can be expressed uniquely in the form

$$\alpha = x_1\eta_1 + \ldots + x_n\eta_n, \text{ with } x_1, \ldots, x_n \in \mathbf{Z},$$

then $\{\eta_1, \ldots, \eta_n\}$ is called a basis for ideal I.

Definition 1.2.10 (Fractional Ideal)**.** Let R be an integral domain, and let K be its field of fractions. A fractional ideal of R is an R-submodule I of K such that there exists a non-zero $r \in R$ such that $rI \subseteq R$. Note than rI is, by definition, an ideal (in the usual sense) of R.

Two fractional ideals I and J are multiplied as follows. Let $I = \frac{1}{a}S$ and $J = \frac{1}{b}T$ where S and T are ideals of R, $a, b \in R$. Define the product

$$IJ := \frac{1}{ab}ST \text{ where}$$

$$IJ = \left\{ \sum_{n=1}^{m} i_n j_n, i_n \in I, j_n \in J, m \in \mathbf{Z}^+ \right\}$$

is the usual ideal multiplication.

Definition 1.2.11. The fractional ideal I is called invertible if there exists another fractional ideal J such that $IJ = R$.

A fractional ideal of R that is contained in R is called an integral ideal. In other words, an integral ideal is the ring ideal in the usual sense.

Definition 1.2.12 (Principal Fractional Ideal)**.** A fractional ideal I of R is called principal if it is generated by a single element of K, i.e.

$$I = aR, \text{ where } a \in K$$

Theorem 1.2.7. *In a Noetherian domain, every nonzero ideal contains a product of one or more prime ideals.*

Theorem 1.2.8. *In a Dedekind domain A, every integral ideal other than 0 and A is a product of prime ideals, and this factorization is unique.*

Theorem 1.2.9. *The set of all nonzero integral and fractional ideals of a Dedekind domain A forms an Abelian group with respect to ideal multiplication (with the empty product being equal to A). The identity element of this group is A and the inverse of an ideal $I = \prod_{i=1}^{n} P_i^{a_i}$ where $P_1, \ldots, P_n$ are distinct prime ideals, and $a_i \in \mathbf{Z}$ is*

$$I^{-1} = \prod_{i=1}^{n} P_i^{-a_i}$$

Theorem 1.2.10. *Let K be an algebraic number field. Let $\mathcal{O}_K$ be its ring of integers. Then, the set of all nonzero integral and fractional ideals of $\mathcal{O}_K$ forms an Abelian group $I(K)$ with respect to multiplication.*

Let $P(K)$ denote the subgroup of principal ideals in $I(K)$.

Definition 1.2.13. The ideal class group $H(K)$ of K defined as the quotient group

$$H(K) := \frac{I(K)}{P(K)}$$

It will be proved later that the ideal class group $I(K)$ is finite for any algebraic number field K.

Definition 1.2.14 (Class Number)**.** The class number $h(K)$ of K is the order of the ideal class group, i.e.

$$h(K) := o(H(K))$$

Theorem 1.2.11. *Let K be an algebraic number field. Let $\mathcal{O}_K$ be its ring of integers and $h(K)$ be its class number. Then, $h(K) = 1 \Leftrightarrow \mathcal{O}_K$ is a PID $\Leftrightarrow \mathcal{O}_K$ is a UFD.*

Chapter 2

Binary Quadratic Forms

In this chapter we state a number of results without proof. The detailed proofs may be found in the reference [4].

2.1 Introduction

Definition 2.1.1 (Binary Quadratic Form, Primitivity)**.** A **binary quadratic form (BQF)** is a degree two homogeneous polynomial in two variables.

An integral binary quadratic form is a BQF with integer coefficients. It looks like

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

where $a, b, c \in \mathbf{Z}$

Definition 2.1.2 (Primitive Form)**.** The integral binary quadratic form f is called **primitive** if a, b and c have no common factor.

It will be shown that for $d \neq 0$, the ideal class group of $\mathbf{Q}(\sqrt{d})$ is isomorphic to the "class group" of integral binary quadratic forms of discriminant d, which constitutes equivalence classes of binary quadratic form, under a certain equivalence relation.

Definition 2.1.3 (Equivalence of BQF's)**.** We say that two binary quadratic forms $f(x, y)$ and $g(x, y)$ are equivalent if there exist $p, q, r, s \in \mathbf{Z}$ such that $ps - rq = \pm 1$ and

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

f and g are said to be properly equivalent if $ps - rq = 1$, and this notion is used more often. Commonly, equivalence refers to proper equivalence.

We may define an action of $SL_2(\mathbf{Z})$ on the set of all integral binary quadratic forms by

$$A \star f := f(px + qy, rx + sy)$$

for an integral binary quadratic form f where

$$A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbf{Z})$$

Clearly, two integral BQF's are (properly) equivalent if and only if they lie in the same orbit of the above action.

Proposition 2.1.1. *Equivalence and proper equivalence indeed define equivalence relations on the set of integral BQF's.*

Definition 2.1.4 (Representation of Integers by BQF's)**.** An integral BQF $f(x, y)$ is said to represent an integer $a \in \mathbf{Z}$ if there exist integers $x_0, y_0 \in \mathbf{Z}$ such that $f(x_0, y_0) = a$. The representation is called proper if x_0 and y_0 are co-prime.

Proposition 2.1.2. *Two equivalent forms represent the same numbers.*

Proposition 2.1.3. *Let $a \in \mathbf{Z}$. Then $f(x, y)$ properly represents a if and only if $f(x, y)$ is properly equivalent to the form $g(x, y) = ax^2 + bxy + cy^2$ for some $b, c \in \mathbf{Z}$.*

Definition 2.1.5 (Discriminant)**.** The discriminant D of a BQF $f(x, y) = ax^2 + bxy + cy^2$ is defined as $D = b^2 - 4ac$. If $D > 0$, the form f is called indefinite. If $D < 0$, f is called definite.

Proposition 2.1.4. *If a is positive, the definite form $f(x, y) = ax^2 + bxy + cy^2$ represents only non-negative integers, and is called positive definite. If a is negative, the definite form $f(x, y) = ax^2 + bxy + cy^2$ represents only non-positive integers, and is called negative definite.*

Proposition 2.1.5. *The discriminant is invariant under the equivalence relation defined above.*

Proposition 2.1.6. *An odd integer M is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue* $\pmod 4$.

2.2 Reduction of primitive positive definite forms

Definition 2.2.1 (Reduced primitive positive definite forms)**.** A form $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $D = b^2 - 4ac$ is *reduced* if

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

Theorem 2.2.1. *Every primitive positive definite form is properly equivalent to a unique reduced form.*

The proof of this theorem involves two steps. The first one shows the existence of a reduced form equivalent to any given positive definite primitive form. The second shows the uniqueness of this reduced form

Step 1. Any positive definite primitive form is equivalent to a reduced form.

Step 1 is further divided into two steps: (A) and (B).

Step 1 (A). Any given form is properly equivalent to a form satisfying $|b| \leq a \leq c$

Proof. Among all forms properly equivalent to f, pick $f(x,y) = ax^2 + bxy + cy^2$ such that $|b|$ is minimal. If $a < |b|$, then

$$\begin{aligned} g(x,y) :&= f\left[\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right] \\ &= f(x+my, y) \\ &= a(x+my)^2 + b(x+my)y + cy^2 \\ &= ax^2 + (b+2am)xy + (am^2+bm+c)y^2 \end{aligned}$$

g is equivalent to f for any $m \in \mathbf{Z}$.

Since $a < |b|$, we can choose $m \in \mathbf{Z}$ such that $|2am + b| < |b|$, a contradiction to the choice of f. So, we must have $a \geq b$.

- If $c < |b|$, then

$$\begin{aligned} g(x,y) :&= f\left[\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right] \\ &= f(x, mx+y) \\ &= ax^2 + bx(mx+y) + c(mx+y)^2 \\ &= (a+bm+cm^2)x + (b+2mc) + cy^2 \end{aligned}$$

  Since $c < |b|$, we can choose $m \in \mathbf{Z}$ such that $|2mc + b| < |b|$, which is a contradiction to the choice of f. So, $c \geq |b|$.
  Thus, $|b| \leq a$ and $|b| \leq c$.
- If $a > c$, we need to change the outer coefficients, which is accomplished by the proper equivalence $(x,y) \to (-y,x)$ [i.e. the transformation matrix
  Therefore, $|b| \leq a \leq c$ is achieved.

□

Step 1 (B) Any form f with $|b| \leq a \leq c$ is properly equivalent to a reduced form.

Proof. The form $f(x,y) = ax^2 + bxy + cy^2$, $|b| \leq a \leq c$ is reduced unless $b < 0$ and ($a = c$ or $a = -b$).
In these cases, $ax^2 - bxy + cy^2$ is reduced. So, we only need to show that the forms $f(x,y) = ax^2 \pm bxy + cy^2$ are properly equivalent in these cases.

- If a = -b,
  the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ provides the required equivalence.
- If a = c,
  the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ provides the required equivalence.

□

Step 2. Uniqueness of the reduced form.

We need to prove that different reduced forms cannot be properly equivalent.

Claim: The outer coefficients of a reduced form give the minimum values properly represented by any equivalent form. The three smallest values taken by the form $f(x,y) = ax^2 + bxy + cy^2$ are a, c, and $a - |b| + c$.

Proof. If $f(x,y) = ax^2 + bxy + cy^2$, $|b| \leq a \leq c$, then

$$\begin{aligned} f(x,y) &\geq ax^2 - |b| \min(x^2, y^2) + cy^2 \\ \Rightarrow f(x,y) &\geq (a - |b| + c) \min(x^2, y^2) \end{aligned}$$

So, whenever $xy \neq 0$, $f(x,y) \geq a - |b| + c \geq c$. Thus, the smallest nonzero value of $f(x,y)$ is a, at $(\pm(1,0)$.

So, the smallest nonzero value of $f(x,y)$ (at $\pm(1,0)$) is a. Further, if $c > a$, then c is he next smallest number represented by f (at $\pm(0,1)$).

Further, if $c > a$, c is the next smallest number represented properly by $f(x,y)$ (at $\pm(0,1)$). □

Proof of uniqueness:

Case 1. $|b| < a < c$.

As per the claim above, the three smallest numbers represented properly by f are $a < c < a - |b| + c$.

Let $g(x,y)$ be a reduced form equivalent to $f(x,y)$. Then, f and g are reduced and represent the same numbers. So, f and g have the same minimum value represented, i.e. a. We can assume that $g(x,y)$ has a as the coefficient of x^2.

Let $g(x,y) = ax^2 + b'xy + c'y^2$. We know $a = a' \leq c$ because g is reduced.

If $a = c'$, then $g(x,y) = a$ has four proper solutions, namely $\pm(1,0)$, $\pm(0,1)$. But, $f \equiv g$. This is a contradiction because $f(x,y) = a$ has precisely two proper solutions, $\pm(1,0)$. So, $a < c'$.

Now, a, c' are the smallest values of the form g and a, c are the smallest values of the form f. Thus, $c = c'$. Since f and g also have the same discriminant, we have $b' = \pm b$ and so $g(x,y) = ax^2 \pm bxy + cy^2$.

It remains to prove that $f(x,y) = g(x,y)$ when f is properly equivalent to g.

Let

$$g(x,y) = f\left[\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right] = f(px + qy, rx + sy)$$

where $ps - qr = 1$

We have $a = g(1,0) = f(p,r)$, $c = g(0,1) = f(q,s)$ (proper representations).

So, $(p,r) = \pm(1,0)$, $(q,s) = \pm(0,1)$. Since $ps - qr = 1$,
$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
Thus, $f(x,y) = g(x,y)$.

Case 2. $|b| = a$ or $a = c$ (so $b \geq 0$)

The argument in case 1 breaks down because $a \leq c \leq a - |b| + c$ are no longer distinct.

Case 2(A). $a \neq c$ and $|b| = a$

Here, we must have $a < c$ and $b \geq 0$, so $b = a$, and since f and g have the same two smallest values, $c = c'$. Moreover, the two forms have the same discriminant, so $b = \pm b'$ Now, $a = g(1,0) = f(p,r)$, $c = g(0,1) = f(q,s)$. Thus, $(p,r) = \pm(1,0)$; $(q,s) = \pm(0,1)$, $ps - qr = 1$.
So, $\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
Thus, $f(x,y) = g(x,y)$.

Case 2(B). $a = c$ and $|b| \neq a$

Again, $b \geq 0$.
Here, $a = c < a - |b| + c = a - b + c = 2a - b$ are the smallest two values of f. The smallest two values of g are a and c'. Thus, $c' = 2a - b$.

$$\begin{aligned} b^2 - 4a^2 &= b'^2 - 4ac' \\ &= b'^2 - 4a(2a - b) \\ &= b'^2 - 8a^2 + 4ab \\ \Rightarrow b^2 - b'^2 &= 4ab - 4a^2 \end{aligned}$$

We have $g(x,y) = f\left[\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right]$

$$ax^2 + b'xy + c'y^2 = f(px + qy, rx + sy)$$

Thus $a = g(1,0) = f(p,r) = f(q,s)$, so $(p,r) = \pm(1,0)$ or $\pm(0,1)$, and $(q,s) = \pm(0,1)$ or $\pm(1,0)$.
So, $\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
So, $g(x,y) = f(x,y)$ or $f(y,-x)$ or $f(-y,x)$, so $g(x,y) = ax^2 - bxy + ay^2$ or $ax^2 + bxy + ay^2$, so $b = \pm b'$. But, $b \geq 0$ and g is reduced, so $b' = b$.
Thus, $f = g$.

Case 2(C) $a = |b| = c$

We have $b \geq 0$, so $a = b = c$

$$g(x,y) = f(px+qy, rx+sy) = a[(px+qy)^2 + (px+qy)(rx+sy) + (rx+sy)^2]$$

So,

$$a = g(1,0) = f(p,r) = a(p^2 + pr + r^2)$$

$$a = g(0,1) = f(q,s) = a(q^2 + qs + y^2)$$
$$\begin{aligned} a = g(1,-1) &= f(p-q, r-s) \\ &= a(p^2 + q^2 - 2pq + r^2 + s^2 - 2rs + pr - ps - qr + qs) \\ &= a[x^2 + y^2 + xy] \end{aligned}$$

Thus, $a = a^{'}$, $a = b^{'}$, $a = c^{'}$ and so $f(x,y) = g(x,y)$.

Algorithm to Reduce Primitive Positive Definite Forms

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

Step 1. If $a > c$, $f \sim g = cx^2 - bxy + ay^2$ via $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ Thus, we may assume that $c \geq a$.

Step 2. If $|b| > a$, then $f \sim g$, where

$$\begin{aligned} g(x,y) &= f[\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}] \\ &= f(x + my, y) \\ &= a^2x^2 + (2am + b)xy + c^{'}y^2 \end{aligned}$$

Let $b^{'} = 2am + b$, $b^{'2} - 4ac^{'} = D$ so that $c^{'} = \frac{b^{'2} - D}{4a}$.

Choose m such that $|2am + b| < |a|$ ($m > 0$ if $b > 0$, $m < 0$ if $b < 0$).

Then, g satisfies $|b^{'} \leq a^{'} = a$.

Repeat steps 1 and 2 till $|b^{'}| \leq a^{'} = a \leq c^{'}$.

Step 3. If $|b^{'}| = a$ or $a = c$ and $b^{'} < 0$, then the required reduced form is $ax^2 - b^{'}xy + c^{'}y^2$. Else, g is already, by definition, in reduced form.

The algorithm terminates in a finite number of steps because the number of positive definite forms of a given discriminant is finite, since we have $D = b^2 - 4ac$, $b^2 \leq a^2 \leq ac$, $D = b^2 - 4ac \leq -3a$, so $ac \leq -\frac{D}{3}$, thus, there are finitely many choices for ac, and $|b| \leq a \leq c$ (recall that each of them is an integer).

2.3 Reduction of primitive indefinite forms

Definition 2.3.1. A primitive indefinite form of a nonsquare discriminant $D > 0$ is reduced if

$$\left|2|a| - \sqrt{D}\right| < b < \sqrt{D}$$

This is equivalent to $D = b^2 - 4ac$,

$$0 < b < \sqrt{D}$$

and

$$|a| + |c| < \sqrt{D}$$

The latter equivalent definition of reduced forms shows that the number of indefinite forms of a given discriminant is finite.

The next theorem is stated without proof.

Theorem 2.3.1. *Let f be a reduced indefinite form. Then, there exists $n \geq 1$ such that the reduced forms equivalent to f are precisely*

$$\rho(f), \rho^2(f), \ldots, \rho^n(f),$$

where

$$\rho : Form_p(d) \to Form_p(d)$$

is the reduction map.

2.3.1 Algorithm to Reduce Primitive Indefinite Forms

1. Let $f = [a, b, c]$ be an indefinite primitive form with discriminant $D > 0$ (nonsquare). If f is reduced, terminate the algorithm.

2. Let $b' \in \mathbf{Z}$ be such that $b' \equiv -b \pmod{2}c$, i.e. find $m \in \mathbf{Z}$ such that $b' = -b + 2mc$ and

   - $-|c| < b' < |c|$ if $|c > \sqrt{D}$
   - $\sqrt{D} - 2|c| < b' < \sqrt{D}$ if $|c| < \sqrt{D}$
   - $c' = \frac{b'^2 - D}{4c}$

3. Continue the algorithm with the neighbour $\rho([a, b, c]) = [c, b', c']$

Theorem 2.3.2. *The indefinite form reduction algorithm terminates in a finite number of steps.*

Sketch of proof. Let $[a_0, b_0, c_0]$ be an indefinite form of discriminant $D > 0$. It can be shown, in a manner similar to the definite case, that at every step $i \geq 1$ of the above algorithm, either the neighbour $[a_i, b_i, c_i]$ is reduced, or it satisfies $|c_i| < |c_{i-1}|$. Since $c_i \in \mathbf{Z}$, the process terminates with at most $|c_i|$ iterations. In this case, uniqueness need not hold.

2.3.2 Algorithm: Determination of a complete set of representatives of $SL_2(\mathbf{Z})$-equivalence classes of indefinite forms with given discriminant $D > 0$

1. Determine the set R of all reduced forms $[a, b, c]$ of discriminant D by using the fact that $|a| + |c| < \sqrt{D}$, $0 < b < \sqrt{D}$, $b^2 - 4ac = D$

2. For each reduced form f, compute $\rho^n(f)$, $n \geq 1$, until obtaining a cycle $\{f, \rho(f), \ldots, \rho^N(f), \rho^{N+1}(f) = f\}$. ($\rho$ denotes the map of the reduction algorithm). Remove $\rho^i(f)$ from R for $1 \leq\leq N$.

3. R is a complete reduced set of representatives of $SL_2(\mathbf{Z})$-equivalence classes of indefinite forms with discriminant D.

2.4 The Form Class Group

Definition 2.4.1 (Principal Forms)**.** We define the principal forms as

$$\begin{cases} x^2 - \frac{D}{4}y^2 & \text{if } D \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1-D}{4}y^2 & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Let $C_p^+(d)$ denote the set of equivalence classes of properly equivalent primitive (positive definite if $d < 0$) BQF's of discriminant d.

Once it is established that the ideal class group is isomorphic to $C_p^+(d)$, we will have proved that the ideal class group is finite.

Lemma 2.4.1. *Assume that $f(x,y) = ax^2+bxy+cy^2$ and $g(x,y) = a'x^2+b'xy+c'y^2$ have discriminant D and satisfy $\gcd(a, a', \frac{b+b'}{2}) = 1$ (since b and b' have the same parity, $\frac{b+b'}{2} \in \mathbf{Z}$). Then, there is a unique integer B modulo $2aa'$ such that*

$$B \equiv b \pmod{2a}$$

$$B \equiv b' \pmod{2a'}$$

$$B^2 \equiv D \pmod{4aa'}$$

Definition 2.4.2 (Dirichlet decomposition)**.** Given primitive positive definite forms $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ with discriminant $D < 0$ and $\gcd\left(a, a', \frac{b+b'}{2}\right) = 1$, the Dirichlet decomposition of f and g is given by

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

where

$$B \equiv b \pmod{2a},\ B \equiv b \pmod{2a'},\ B^2 \equiv D \pmod{4aa'}$$

Proposition 2.4.1. *Given $f(x,y)$ and $g(x,y)$, the Dirichlet decomposition $F(x,y)$ is a primitive positive definite form of discriminant D.*

Theorem 2.4.1. *Let $D \equiv 0, 1 \pmod 4$ be negative. Let $C_p^+(D)$ be the set of classes of primitive positive definite forms of discriminant D. The Dirichlet composition induces a well-defined binary operation on $C_p^+(D)$ which makes $C_p^+(D)$ into a finite abelian group whose order is the class number $h(D)$. Furthermore, the identity element of $C_p^+(D)$ is the class containing the principal form*

$$\begin{cases} x^2 - \frac{D}{4}y^2 & \textit{when } D \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1-D}{4}y^2 & \textit{when } D \equiv 1 \pmod 4 \end{cases}$$

and the inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class $ax^2 - bxy + cy^2$.

*$C_p^+(D)$ is called the **form class group**.*

2.5 Primes represented by forms

Proposition 2.5.1. *For $d \equiv 0, 1 \pmod 4$ and $\gcd(n, d) = 1$, n is properly represented by a principal form of discriminant d if and only if d is a square modulo $4n$.*

Proof. We have $\gcd(n, d) = 1$. Since n is represented by a form f of discriminant d, by Proposition 2.0.3, we must have $f \equiv \tilde{f} = [n, b, c]$, $b, c \in \mathbf{Z}$,

$$d = \Delta(\tilde{f}) = b^2 - 4nc \equiv b^2 \pmod{4n}$$

Conversely, let n be an integer co-prime to d, and suppose that there exists $b \in \mathbf{Z}$ such that $d \equiv b^2 \pmod{4n}$, so there exists $c \in \mathbf{Z}$ such that $d = b^2 - 4nc$. Then, the form $[n, b, c]$ has discriminant d and properly represents n. Moreover, it is primitive, since if $e \mid n, b, c$, then $e \mid D$, so $e = \pm 1$, since $\gcd(n, d) = 1$. □

In the above proof, in the case when $d \equiv 0 \pmod 4$, the condition is reduced to d being a square modulo n. [This requires proof only in the "if" case. Suppose $D \equiv b^2 \pmod m$. Let $b' = b$, if b is even, and $b' = b + m$, if b is odd.

Then $D \equiv b \pmod m$, and, since m is odd and $D \equiv 0 \pmod 4$, D and b' are both even. This means that $D \equiv b'2 \pmod 4 m$ (4 divides both D and b'^2/ So, $D \equiv b^2 - 4mc$ for some integer c. So, we have the form $f(x, y) = mx^2 + bxy + cy^2$, which is of discriminant D, properly represents m, and is primitive, since m and D are co-prime.

When $h_f(d) = 1$, all forms are mutually equivalent and since equivalent forms properly represent the same integers, this criterion lets us know when an integer is represented by a given form.

Corollary 2.5.1. *Let n be an integer and p be an odd prime that does not divide n. Then p is represented by a primitive form of discriminant $4n$ if and only if $(\frac{-n}{p}) = 1$.*

Proof. Note that a primitive form represents a prime p if and only if it properly represents p. Now, $(\frac{-4n}{p}) = (\frac{-n}{p})(\frac{2}{p})^2$. The result follows from the previous theorem and the discussion following it.

□

Proposition 2.5.2. *If $n = 1, 2, 3, 4, 7$, $p \neq n$ is an odd prime, then p is represented by $x^2 + ny^2$ if and only if $(\frac{-n}{p}) = 1$.*

Sketch of proof. We have seen that p is represented by a form of discriminant $4n$, where $\gcd(p, n) = 1$ if and only if $(\frac{-n}{p}) = 1$. It is clear that the form $x^2 + ny^2$ has discriminant $-4n$ and represents p whenever $(\frac{-n}{p}) = 1$. It only needs to be shown that in the cases $n = 1, 2, 3, 4, 7$, the only form classes with discriminant $-4n$ are $x^2 + ny^2$. This is done by calculating all the reduced forms $[a, b, c]$ of discriminant $-4n$ for each of the given n, using the reduced criteria $|b| \leq a \leq \frac{\sqrt{D}}{3}$. For example, in the case $n = 2$, we have $|b| \leq a \leq \frac{\sqrt{8}}{3} < 2$. Since $1 - 4c = -8$ has no integer solutions, we must have $b = 0$, $a = 1$, $c = 2$, so that the only reduced form of discriminant -8 is $x^2 + 2y^2$.

The other cases are argued out similarly.

The case $n = 1$ gives *Fermat's two squares theorem: An odd prime p can be expressed as a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Chapter 3

The Picard Group and Narrow Picard Group

In this chapter we state a number of results without proof. The detailed proofs may be found in the reference [4].

3.1 Orders

Definition 3.1.1 (Order)**.** An order in a number field K is a subring $\mathcal{O} \subset K$ containing 1 such that

1. $\mathcal{O}$ is a finitely generated $\mathbf{Z}$-module
2. $\mathcal{O}$ contains a $\mathbf{Q}$-basis of K

1 implies that $\mathcal{O}_K$ contains any order of K, 1 and 2 imply that $\mathcal{O}$ is a free $\mathbf{Z}$-module of rank 2, 2 implies that K is the field of fractions of $\mathcal{O}$. Thus, $\mathcal{O}_K$ itself is an order, and contains all other orders. It is called the maximal order of K.

To describe orders in quadratic fields more explicitly, the maximal order can be written as follows

$$\mathcal{O}_K = [1, \omega_K], \quad \omega_K = \frac{d_K + \sqrt{d_k}}{2}$$

where d_K is the discriminant of K.

Lemma 3.1.1. *Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then, $\mathcal{O}$ has finite index in $\mathcal{O}_K$, and if we set $f = [\mathcal{O}_K : \mathcal{O}]$, then*

$$\mathcal{O} = \mathbf{Z} + f\mathcal{O}_K = [1, f\Omega_K]$$

where $\omega_K = \frac{d_K + \sqrt{d_k}}{2}$

Definition 3.1.2 (Conductor)**.** The number $F = [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of the order $\mathcal{O}$.

Definition 3.1.3 (Discriminant of an order)**.** An order $\mathcal{O}$ admits an integral basis of K, so we can define the discriminant of $\mathcal{O}$ as the square of a 2×2 determinant with rows being the integral basis under the two automorphisms of the field K, in the same manner as we described the discriminant of $\mathcal{O}_K$.

Proposition 3.1.1. *The discriminant of an order $\mathcal{O}$ of conductor F is $F^2 d_K$.*

Proof. In the same way as for $\mathcal{O}_\mathcal{K}$, we can show that the discriminant of $\mathcal{O}$ is independent of the basis used, and, calculating it using the basis $[1, fw_K]$, where $\{1, w_K\}$ is an integral basis of $\mathcal{O}$, gives the discriminant $D = f^2 d_K$. □

3.2 Ideals of Orders and Invertibility

Definition 3.2.1. Let $\mathcal{O}$ be an order in K. A fractional ideal α of $\mathcal{O}$ is proper if $\mathcal{O} = \{x \in K : x\alpha \subset \alpha\}$.

Fact: All ideals in $\mathcal{O}_K$ are proper.

Notation: $[x, y] := \mathbf{Z}x + \mathbf{Z}y$

Lemma 3.2.1. *Let $\mathcal{O}$ be an order in K, $\tau \in K$ be of degree two with minimal polynomial $ax^2 + bx + c \in \mathbf{Z}[x]$. Then,*

1. *$\tilde{\mathcal{O}} = [1, a\tau]$ is an order in K, $\alpha = [1, \tau]$ is a proper fractional ideal of $\tilde{\mathcal{O}}$.*
2. *If α is proper, then $\mathcal{O} = \tilde{\mathcal{O}}$*

Proposition 3.2.1. *Let $\mathcal{O}$ be an order in K, α be a fractional ideal of $\mathcal{O}$. Then, α is invertible in $\mathcal{O}$ if an only if it is proper. The inverse in this case is given by*

$$\frac{\alpha'}{N(\alpha)}$$

where α' is the conjugate ideal of α, i.e.

$$\alpha' = \{x' : x \in \alpha\} \subset \mathcal{O}$$

Proposition 3.2.2. *Let K be a quadratic number field, $\mathcal{O}_K$ be the ring of algebraic integers in K. Let $f > 0$ be a positive integer. Then there exists a unique order R of K such that f is the order of the group $\frac{\mathcal{O}_K}{R}$. Moreover, the discriminant of R is $f^2 d$, where d is the discriminant of K. Conversely, if R is an order of K, its discriminant is $f^2 d$ for $f > 0$ and where $f = [\mathcal{O}_K : R]$*

Note that the proof of this proposition involves the result that states that the quotient of two free abelian ranks of the same rank is finite, which, in turn, is proven using the Stacked bases theorem, or using results from Lattice theory.

Definition 3.2.2 (Alternate definition of fractional ideal norm)**.** Let I be a fractional ideal of an order R. We define $N(I) = [R : I]$ where the right hand side is defined as usual.

Proposition 3.2.3. *Let I be a fractional ideal of an order R. Let γ be a nonzero element of K. Then, $N(\gamma I) = |N(\gamma)|N(I)$*

Proposition 3.2.4. *Let I be a fractional ideal of an order R. Let $\alpha_1, \alpha_2, \ldots \alpha_n$ be a $\mathbf{Z}$-basis of I. Let $\theta_1, \ldots \theta_n$ be a $\mathbf{Z}$-basis of R. Suppose $\alpha_i = \Sigma_j a_{ij}\theta_j$ for $i = 1, 2, \ldots, n$ Then,*

$$N(I) = det(a_{ij})$$

Proposition 3.2.5. *Let I and J be fractional ideals of R, $J \subset I$. Then,*

$$\left|\frac{I}{J}\right| = \frac{N(J)}{N(I)}$$

Hence, if K is an algebraic number field of degree n and R is an order of K with fractional ideal I, the norm of I is defined as follows:

There exists $\alpha \in R$, an ideal J of R such that

$$I = \frac{1}{\alpha}J$$

$$N(I) := \frac{N(J)}{N(\alpha R)} \quad \text{where } N(J) := \left|\frac{R}{I}\right|$$

3.3 Picard Groups and Class Numbers

Let $d \in \mathbf{Z}$ be a fundamental discriminant, K be a quadratic field of dscriminant d, and $\mathcal{O}$ be an order in K.

Definition 3.3.1. The Picard Group of $\mathcal{O}$ is

$$Pic(\mathcal{O}) = \frac{J(\mathcal{O})}{P(\mathcal{O})}$$

where $J(\mathcal{O})$ is the group of invertible fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ is the group of principal $\mathcal{O}$-ideals.

Definition 3.3.2. The Narrow Picard Group of $\mathcal{O}$ is

$$Pic^+(\mathcal{O}) = \frac{J(\mathcal{O})}{P^+(\mathcal{O})}$$

where $J(\mathcal{O})$ is the group of invertible fractional $\mathcal{O}$-ideals and $P^+(\mathcal{O})$ is the group of principal $\mathcal{O}$-ideals with generator of positive norm.

When $\mathcal{O} = \mathcal{O}_K$, $Pic(\mathcal{O})$ is the ideal class group $Cl(d)$ of cardinality $h(d)$, the class number.

3.4 Narrow Picard Groups

If $d < 0$, all norms are positive. So, the Picard group and the Narrow Picard group are the same for all orders. However, in the real case, we will establish a correspondence with a narrow Picard group.

Let $\mathcal{O}$ be an order in a real quadratic field K with discriminant d. By the third isomorphism theorem,

$$Pic(\mathcal{O}) = \frac{J(\mathcal{O})}{P(\mathcal{O})} \cong \frac{J(\mathcal{O})/P^+(\mathcal{O})}{P(\mathcal{O})/P^+(\mathcal{O})} = \frac{Pic^+(\mathcal{O})}{P(\mathcal{O})/P^+(\mathcal{O})}$$

where $J(\mathcal{O})$ is consists of invertible fractional ideals of $\mathcal{O}$, $P(\mathcal{O})$ consists of principal fractional ideals of $\mathcal{O}$, and $P^+(\mathcal{O}) \in P(\mathcal{O})$ consists of principal fractional ideals of $\mathcal{O}$ with generator of positive norm.

Lemma 3.4.1.

$$| \frac{P(\mathcal{O})}{P^+(\mathcal{O})} | \quad \leq 2$$

Proof.

$$|Pic^+(\mathcal{O})| = \begin{cases} |Pic(\mathcal{O})| \text{ if } \mathcal{O}^* \text{ has an element of norm -1, and} \\ |Pic^+(\mathcal{O})| = 2|Pic(\mathcal{O})| \text{ otherwise} \end{cases}$$

□

Chapter 4

Associating Binary Quadratic Forms and Ideals

We use the symbol $\bar{f}$ to denote the equivalence class of the form f under the equivalence relation described in Chapter 2, and the symbol $\overline{I}$ to denote the equivalence class of the ideal $I \in J(\mathcal{O})$ in the group $Pic^+(\mathcal{O}) = \frac{J(\mathcal{O})}{P^+(\mathcal{O})}$. In this chapter we state a number of results without proof. The detailed proofs may be found in the reference [4].

4.1 Associating Binary Quadratic Forms to Ideals

Let K be a quadratic number field and $\mathcal{O}$ be an order of conductor $F \geq 1$.

Recall that every ideal of an order in a quadratic field is a free abelian group of rank 2.

Lemma 4.1.1. *Let I be a fractional ideal of $\mathcal{O}$. There exists $x \in K^*$ such that $xI + F\mathcal{O} = \mathcal{O}$*

Proposition 4.1.1. *Let I be an invertible ideal of $\mathcal{O}$ with the choice of an ordered* **Z***-basis (α, β). Then*

$$f_{I,(\alpha,\beta)}(x, y) := \frac{N(\alpha x + \beta y)}{N(\alpha)}$$

is a primitive binary integral quadratic form of discriminant $F^2 d_K$. Moreover, it is positive-definite when $d_K < 0$.

Note that the above definition depends upon the choice and order of the **Z**-basis for the ideal. We now introduce the concept of "correctly ordered bases", such that two different choices of correctly ordered bases yield equivalent forms.

Proposition 4.1.2. *Let I be an ideal of an order $\mathcal{O}$ in K. Then, $\frac{\mathcal{O}}{I}$ is finite. We call its cardinality the norm $N(I)$ of the ideal. Then,*

1. *For all $x \in \mathcal{O}$, $N(x\mathcal{O}) = |N(x)|$*
2. *For all invertible ideals I, J,*

$$N(IJ) = N(I)N(J)$$

3. If $(x_1, \ldots, x_n)$ is a $\mathbf{Z}$-basis of an ideal I in $\mathcal{O}$, then

$$N(I)^2 = \frac{D(x_1, \ldots, x_n)}{F^2 d_K}$$

So for the case n=2, we have

$$N(I)^2 = \frac{(\alpha\beta' - \beta\alpha')^2}{F^2 d_K}$$

$$\Rightarrow (\alpha\beta' - \beta\alpha') = \pm N(I) F \sqrt{d_K}$$

$$\Rightarrow \frac{\alpha\beta' - \beta\alpha'}{\sqrt{d_K}} \in \mathbf{R}^* \cup i\mathbf{R}^*$$

This allows the following definition.

Definition 4.1.1. Let $\mathcal{O}$ be an order of K, and I and ideal in $\mathcal{O}$. A correctly ordered basis (α, β) of I is an ordered $\mathbf{Z}$-basis of I such that

$$\frac{\alpha\beta' - \alpha'\beta}{\sqrt{d_K}} \in \mathbf{R}_{>0} \cup i\mathbf{R}_{>0}$$

Any ideal of $\mathcal{O}$ admits a correctly ordered basis, since permuting the elements of a basis that is not correctly ordered gives a correctly ordered basis. By the description of orders in a quadratic field, the order of conductor $F \geq 1$ has the correctly ordered basis $(\frac{d_K + \sqrt{d_K}}{2}, F)$.

4.1.1 Two Correctly Ordered Bases Produce Equivalent Forms

Proposition 4.1.3. *Let $\mathcal{O}$ be an order in K, I be an ideal of $\mathcal{O}$. Any two correctly ordered bases of I are equivalent under the action of an element of $SL_2(\mathbf{Z})$. Conversely, the natural action of an element of $SL_2(\mathbf{Z})$ on a correctly ordered basis of I viewed as an element of $I \times I$ gives another correctly ordered basis.*

Proposition 4.1.4. *Let $\mathcal{O}$ be an order in K, I be an ideal of $\mathcal{O}$ with two correctly ordered bases (α, β) and (δ, γ). Then, $f_{I,(\alpha,\beta)}$ and $f_{I,(\delta,\gamma)}$ are properly equivalent.*

Finally, we shall have that two equivalent ideals give equivalent classes under the restriction that this equivalence is in the Narrow Picard group.

Proposition 4.1.5. *If I, J are two ideals in an order $\mathcal{O}$ of K that are equivalent in $Pic^+(\mathcal{O})$, then $\bar{f}_I = \bar{f}_J$.*

Thus, up to equivalence, the form obtained from an ideal does not depend on the choice of a correctly ordered basis nor on ideal equivalence.

Proposition 4.1.6. *Let I, J be ideals of order $\mathcal{O}$ in K. If $\bar{f}_I$, $\bar{f}_J$, then $I = J$.*

4.2 Associating Ideals to Binary Quadratic Forms

Let $\mathcal{O}$ be an order of conductor $F \geq 1$ in a quadratic field K of discriminant d_K.

In the previous section, we showed that there is an injection from $Pic^+(\mathcal{O})$ to $C_p^+(d)$ with $d = F^2 D_K$. We now prove that this map is onto and find its inverse.

Proposition 4.2.1. *Let $f = [a, b, c]$ be a primitive binary quadratic form of discriminant $d = F^2 d_K$ with d_K a fundamental discriminant and let K be a quadratic form of discriminant d_K. Suppose that f is positive definite if $d < 0$. Then,*

$$I_f := \left[\lambda a, \lambda\left(\frac{b - f\sqrt{d_K}}{2}\right)\right]$$

with

$$\lambda = \begin{cases} 1 \text{ if } a > 0 \text{ and} \\ F\sqrt{d_K} \text{ otherwise} \end{cases}$$

is a fractional ideal of the order of conductor F in K, such that $\bar{f}_{I_f} = \bar{f}$. Moreover, the fractional ideal I_f is invertible if f is primitive.

Corollary 4.2.1. *If f and g are two equivalent primitive forms, then $I_f = I_g$.*

We may summarize all the results obtained in the following theorem:

Theorem 4.2.1. *Let $d \in \mathbf{Z}$, $d \equiv 0, 1 \pmod 4$, $d = F^2 d_K$, with d_K a fundamental discriminant. Let K be a quadratic field of discriminant d_K, $\mathcal{O}$ an order of conductor F. There exists a bijection between $Pic^+(\mathcal{O})$ and $C_p^+(d)$. The bijection is given as follows by ϕ and its inverse by ψ.*

$$\phi : Pic^+(\mathcal{O}) \to C_p^+(d)$$

$$\psi : C_p^+(d) \to Pic^+(\mathcal{O})$$

If I is an ideal class of $Pic^+(\mathcal{O})$ and (α, β) is a correctly ordered basis of any ideal of $\mathcal{O}$ contained in I,

$$\phi(I) = \frac{[N(\alpha x + \beta y)]}{N(I)} \in C_p^+(d)$$

If $f = [a, b, c]$ is a class of $C_p(d)$, let

$$\psi(\bar{f}) = \overline{\left[a, \frac{b - F\sqrt{d}}{2}\right]} \in Pic^+(\mathcal{O})$$

$\phi \cdot \psi = \psi \cdot \phi = 1$, *i.e.* $\phi^{-1} = \psi$

Chapter 5

Using the two points of view

5.1 Gauss composition law and the group structure

Definition 5.1.1 (Gaussian Composition of Forms)**.** Suppose we wish to compose forms $f_1 = A_1x^2 + B_1xy + C_1y^2$ and $f_2 = A_2x^2 + B_2xy + C_2y^2$, each primitive and of the same discriminant D. We perform the following steps:

1. Compute $\tilde{B} = \frac{B_1+B_2}{2}$ and $e = \gcd(A_1, A_2, \tilde{B})$, and $A = \frac{A_1A_2}{e^2}$.

2. Solve the system of congruences

$$\begin{aligned} x &\equiv B_1 \pmod{2\tfrac{A_1}{e}} \\ x &\equiv B_2 \pmod{2\tfrac{A_2}{e}} \\ \tfrac{\tilde{B}}{e}x &\equiv \tfrac{D+B_1B_2}{2e} \pmod{2A} \end{aligned}$$

   It can be shown that this system always has a unique integer solution modulo $2A$. We arbitrarily choose such a solution and call it B.

3. Compute C such that $D = B^2 - 4AC$. It can be shown that C is an integer. Then, $Ax^2 + Bxy + Cy^2$ is the composed form. It turns out that this composition respects proper equivalence and makes the set of classes of forms into a finite abelian group.

It turns out that this definition is equivalent to the composition of form classes that is obtained by identifying them with ideals in the narrow Picard group of the corresponding quadratic field.

For any $d \equiv 0, 1 \pmod 4$, the set $C_p^+(d)$ is in one-to-one correspondence with a narrow Picard group of a quadratic field, so it can be endowed with the structure of an abelian group.

Let $d \equiv 0, 1 \pmod 4$ be an integer and write $d = F^2 d_K$ with d_K a fundamental discriminant, $F \geq 1$. Let K be a quadratic field of discriminant d_K, $\mathcal{O} = \mathbf{Z} + F\mathcal{O}_K$ its order of conductor F. The group law $\star$ induced on $C_p^+(d)$ is explicitly given by

$$\bar{g} \star \bar{h} = \phi(\psi(\bar{g})\psi(\bar{h}))$$

($\bar{g}$, $\bar{h} \in C_p^+(d)$), with

$$\psi : C_p^+(d) \to Pic^+(\mathcal{O})$$
$$\phi : Pic^+(\mathcal{O}) \to C_p^+(d)$$

(ϕ is the inverse of ψ)

$$\psi([a,b,c]) = \left[\lambda a, \lambda\left(\frac{b - F\sqrt{d_K}}{2}\right)\right]$$

with $\lambda = 1$ if $a < 0$, $\lambda = F\sqrt{d_K}$ otherwise. And

$$\phi(I) = \overline{\frac{N(\alpha x + \beta y)}{N(I)}} \in C_P^+(d)$$

where (α, β) is a correctly ordered basis of I.

The identity element of $C_p^+(d)$ is given by $\phi(\mathcal{O})$. The inverse of $\bar{g} \in C_p^+(d)$ is

$$\phi\left(\frac{\psi(\bar{g})'}{N(I)}\right)$$

Thus, by construction,

$$Pic^+(\mathcal{O}) \cong C_p^+(d)$$

as finite abelian groups.

It is easy to check that a correctly ordered basis of the $\mathcal{O}$-ideal $\mathcal{O}$ is

$$\begin{cases} \left(\frac{F\sqrt{d_K}}{2}, 1\right) & \text{if } d_K \equiv 2,3 \pmod 4 \\ \left(F\frac{1+\sqrt{d_K}}{2}, 1\right) & \text{if } d_K \equiv 1 \pmod 4 \end{cases}$$

Thus, the identity element of $C_p^+(d)$ is

$$\phi(\mathcal{O}) = \overline{\frac{N\left(\frac{F\sqrt{d_K}}{2}X + Y\right)}{N(\mathcal{O})}} \text{ if } d_K \equiv 2,3 \pmod 4, \text{ and}$$

$$\phi(\mathcal{O}) = \overline{\frac{N\left(F\frac{1+\sqrt{d_K}}{2}X + Y\right)}{N(\mathcal{O})}} \text{ if } d_K \equiv 1 \pmod 4, \text{ i.e.}$$

$$\phi(\mathcal{O}) = \begin{cases} \left(\frac{-F^2 d_K}{4}, 0, 1\right), & \text{if } d_K \equiv 2,3 \pmod 4, \\ \left(\left(\frac{1-d_K}{4}\right)F^2, F, 1\right), & \text{if } d_K \equiv 1 \pmod 4 \end{cases}$$

We now compute inverses. We use the fact that the inverse of the class of an ideal I is simply given by the class of I'. Recall that if $f = [a,b,c]$ is a primitive binary quadratic form of discriminant $d = F^2 d_K$, with d_K a fundamental discriminant and K a quadratic field of discriminant d_K. f is positive definite if $d < 0$. The ideal corresponding to f is

$$\overline{I_f} = \left[\lambda a, \lambda\frac{b - F\sqrt{d_K}}{2}\right]$$

(where $\lambda = 1$ if $a > 0$ and $\lambda = F\sqrt{d_K}$ otherwise), which is a fractional ideal of the order of conductor F in K. So, $\overline{f_{I_f}} = f$. Moreover, $\overline{I_f}$ is invertible if f is primitive.

By the calculations,

$$\overline{[a,b,c]}^{-1} = \overline{[c,b,a]} = \overline{[a,-b,c]}$$

which is reduced when $[a,b,c]$ is reduced.

5.2 Explicit Determination of Picard Group

We need to calculate the number of classes of forms of discriminant d. This is equivalent to calculating the number of non-equivalent reduced forms with discriminant d. We need $[a,b,c]$ with $b^2 - 4ac = d$, $B^2 \leq a^2 \leq ac$ $d = b^2 - 4ac \leq -3ac$. So, $ac \leq -\frac{d}{3}$. Also, $d + 4ac = b^2 \geq 0$, which means that $ac \geq -\frac{d}{4}$, and $d + 4ac$ is a perfect square.

Summarising, we may use the following facts to calculate $C_p^+(d)$

- $\frac{d}{4} \leq ac \leq -\frac{d}{3}$
- $d + 4ac$ is a perfect square.

5.2.1 Computing the Picard Group for d = -47

Here,

$$11 \leq \frac{47}{4} \leq ac \leq \frac{47}{3} \leq 16$$

and $d + 4ac = -47 + 4ac$ is a perfect square.

So, $11 \leq ac \leq 16$. We check the values of $-47 + 4ac$ for each of the possible values of ac.

- $ac = 11$ $-47 + 4ac = -3$, which is not a perfect square
- $ac = 12$ $-47 + 4ac = 1$, which is a perfect square
- $ac = 13$ $-47 + 4ac = 5$, which is not a perfect square
- $ac = 14$ $-47 + 4ac = 9$, which is a perfect square
- $ac = 16$ $-47 + 4ac = 17$, which is not a perfect square

Thus, ac = 12 or 14 The corresponding values of b must satisfy $b^2 - 4ac = -47$, or $b^2 - 48 = -47 \Rightarrow b = \pm 1$, and $b^2 - 56 = -47 \Rightarrow b = \pm 3$

Case: $b = \pm 1, ac = 12$ The forms are:
$[1,1,12]$, $[2,1,6]$, $[2,-1,6]$, $[3,1,4]$, $[3,-1,4]$. (Note that $[1,-1,12]$ is not reduced)

Case: $b = \pm 3, ac = 12$. Since the only factorizations of 12 are $1 \cdot 12$, $2 \cdot 6$, and $3 \cdot 4$, none of these possibilities for a and c along with $b = \pm 3$ gives a reduced form.

Thus, there are only 5 reduced forms of discriminant -47, i.e. $|C_p^+(d)| = 5$. We now give the correspondence between $Cl(-47)$ and $C_p^+(-47)$.

Let $K = \mathbf{Q}(\sqrt{-47})$ be the quadratic field with discriminant -47. Note that $F = 1$ here.
$-47 \equiv 1 \pmod 4$, so a correctly ordered $\mathbf{Z}$-basis of $\mathcal{O}_K$ is

$$\left(\frac{1+\sqrt{-47}}{2}, 1\right)$$

The class of $\mathcal{O}_K$ in $Cl(-47)$ corresponds to the identity element in $C^+(-47)$, which is $\overline{\left[F^2\frac{1-d_K}{4}, F, 1\right]} = \overline{\left[\frac{1+47}{4}, 1, 1\right]} = \overline{[12, 1, 1]} = \overline{[1, 1, 12]}$.

The ideal associated to the class $[2, 1, 6]$ is

$$\left[a, \left(\frac{b - F\sqrt{d_K}}{2}\right)\right] = \left[2, \frac{1-\sqrt{-47}}{2}\right]$$

and so $[2, 1, 6]$ is associated to the ideal $\left[2, \frac{1+\sqrt{-47}}{2}\right]$.

$[3, 1, 4]$ is associated to the ideal $\left[3, \frac{1-\sqrt{-47}}{2}\right]$

$[3, -1, 4]$ is associated to the ideal $[3, \frac{1+\sqrt{-47}}{2}]$.

Thus, we have systematically determined a complete set of representatives of the ideal class group. This group is

$$\left\{\left[1, \tfrac{1+\sqrt{-47}}{2}\right] = \mathcal{O}_K, \left[2, \tfrac{1+\sqrt{-47}}{2}\right], \left[2, \tfrac{1-\sqrt{-47}}{2}\right], \left[3, \tfrac{1-\sqrt{-47}}{2}\right], \left[3, \tfrac{1+\sqrt{-47}}{2}\right]\right\} \cong \frac{\mathbf{Z}}{5\mathbf{Z}}$$

5.2.2 Computing the Picard group for d = 12

$d = 12 \equiv 0 \pmod 4$
For positive d, a form $ax^2 + bxy + cy^2$ is reduced if and only if

$$| \, |a| + |c| \, | < \sqrt{d}$$

and

$$0 < b < \sqrt{d}$$

Here, that means $|a| + |c| < 2\sqrt{3}$, so $|a| + |c| \leq 3$ (since they are integers) and $0 < b \leq 3$, $(d = b^2 - 4ac)$

We cannot have a or c equal to 0, since 12 is not a perfect square. The possibilities are: $a = \pm 1, c = \pm 1$, $a = \pm 2, c = \pm 2$, $a = \pm 1, c = \pm 2$. Also, $b^2 = 12 - 4 \cdot 2 = 4 \Rightarrow b = 2$ But, $|a| = |c| = 1$ gives $b = \pm 4$, which is not possible by the second condition. Arguing similarly, we find that the reduced forms are:
$[2, 2, -1], [-2, 2, 1], [1, 2, -2], [-1, 2, 2]$.

Applying the reduction algorithm to $[-2, 2, 1]$, we get that the cycle associated to $[-2, 2, 1]$ is

$$[-2, 2, 1] \to [1, 2, -2] \to [-2, 2, 1]$$

Similarly, the cycle associated to the cycle associated to $[-1, 2, 2]$ is

$$[-1, 2, 2] \to [2, 2, -1] \to [-1, 2, 2]$$

Thus, a complete set of reduced representatives of $C_p^+(12)$ is given by $[-2, 2, 1]$.

Now, 12 is the fundamental discriminant of the field $\mathbf{Q}(\sqrt{3})$. So, here $F = 1$. As before, we compute the ideals associated to the form classes above, to find that $[-2, 2, 1]$ corresponds to the ideal $[2, 1 - \sqrt{3}]$ and $[-1, 2, 2]$ corresponds to the ideal $[1, 1 - \sqrt{3}]$. Also, $\mathcal{O}_\mathcal{K}$ has no element of norm -1, since the equation $a^2 - 3b^2 = -1$ has no integer solutions. (To see this, consider both sides modo 4, a^2 and b^2 may be 0 or 1 (mod 4)). So, the Picard Group (here, the ideal class group) of $\mathcal{O}_K$ is the trivial group. Thus, the class number of the field $\mathbf{Q}(\sqrt{3})$ is 1.

5.3 Class numbers

The Class Number Problem: We are interested in the following questions:

1. Do there exist infinitely many $d \equiv 0, 1 \pmod 4$ such that $h_f(d) = 1$? (Class number one problem)
2. More generally, do there exist infinitely many $d \equiv 0, 1 \pmod 4$ such that $h_f(d) = n$ for given $n \geq 1$? Can an efficient way to find them be given?
3. What is the asymptotic behaviour of $h_f(d)$ with $d \equiv 0, 1 \pmod 4$?

Gauss's conjectures:

1. $h(d) \to \infty$ as $d \to -\infty$
2. Class number = 1 for d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163. There are no other negative discriminants with class number one. (This has been proven, and is known as the Baker-Heegner-Stark theorem [5])
3. There are infinitely many positive discriminants with class number 1 (Open problem).

Class number problem for negative d

Theorem 5.3.1 (Baker-Heegner-Stark [5])**.** *For $d < 0$, we have $h_f(d) = 1 \Leftrightarrow d = -1, -2, -3, -4, -7, -11, -19, -43, -67, -163$.*

5.3.1 Units, automorphisms, Pell's equation

Theorem 5.3.2. *Let d be a form discriminant and $g \in Form_p^+(d)$, the group of all equivalence classes of positive definite forms of discriminant d, if $d < 0$ and of all indefinite forms if $d > 0$. Let us write $d = F^2 d_K$ with d_K a fundamental discriminant of a quadratic field K, $F \geq 1$. Let $\mathcal{O}$ be the order of K of conductor F. Then, there is an isomorphism between $Aut(g)$ and $\mathcal{O}^*$.*

Determining the group of units turns out to be equivalent to solving Pell's equations $x^2 - ny^2 = 1$.

Proposition 5.3.1 (Units in Imaginary Quadratic Fields)**.** *The group of units $\mathcal{O}^*$ of an $\mathcal{O}$ of an imaginary quadratic field is given by*

$$\mathcal{O}^* \cong \begin{cases} \mathbf{Z}/4\mathbf{Z} & \text{if } d = -1, F = 1 \\ \mathbf{Z}/6\mathbf{Z} & \text{if } d = -3, F = 1, \\ \mathbf{Z}/2\mathbf{Z} & \text{otherwise} \end{cases}$$

Proposition 5.3.2 (Units in Real Quadratic Fields)**.** *The group of units $\mathcal{O}^*$ of an order $\mathcal{O}$ of a real quadratic field is given by*

$$\mathcal{O}^* \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$$

5.4 On Gauss's Class Number Problems: Some Computations

In this section, we follow the notational convention of Daniel Shanks's 2010 paper, [6], which will serve as a reference. Let $h(\Delta)$ (or simply h, when there is no confusion) denote the class number of a binary quadratic form (or equivalently, quadratic number field) of discriminant $-\Delta$. We use the notation $Au^2 + Buv + Cv^2$ for a form.

We distinguish between the discriminant $-\Delta = -4AC + B^2$ of the form $Au^2 + Buv + Cv^2$ and the *determinant* $-D$, used in Gauss's (equivalent) formulation, given by $D = AC - B^2$, of the form $Au^2 + 2Buv + Cv^2$.

Lemma 5.4.1. *If $\Delta = 8k + 3$ $(k > 0)$, then we have*

$$h(-4\Delta) = 3h(-\Delta)$$

Lemma 5.4.2. *If $\Delta = 8k - 1$ $(k > 0)$, then we have*

$$h(-4\Delta) = h(-\Delta)$$

Fact: If the determinant $-D = 1, 2$ or 4, the class number is 1.

Proposition 5.4.1 (Shanks, 2010 [6])**.** *If $-D = 4k + 1$, $4k + 2$, $4k + 4$ $(k > 0)$, the class number is even.*

Proof. There then exists a form of order 2 (called an **ambiguous form**) $f = (A, 2B, C)$ distinct from the principal form I, namely:

$$f = (2, 2, 2k+1), \text{ for } -D = 4k+1$$
$$f = (2^s, 0, 2k+1), \text{ for } -D = 2^s(2k+1)$$
$$f = (4, 4, 2^{s-2}+1), \text{ for } -D = 2^s \ (s > 2)$$

Since $f^2 = I = (1, 0, -D)$ under composition, there is a subgroup of order 2. □

Proposition 5.4.2 (Shanks, 2010 [6]). *If $-D = 8k+3$ ($k > 0$), the class number is divisible by 3.*

Proof. We have $f = (4, 2, 2k+1) \neq I$ satisfying $F^3 = I$, so there is a subgroup of order 3. □

Proposition 5.4.3 (Shanks, 2010 [6]). *For a class number $h = 6n \pm 1$, $n > 0$, we must have $-D = 8k-1$.*

Proof. Propositions 5.4.1 and 5.4.2 rule out the possibilities of $-D = 8k+1$, $-D = 8k+2$, $-D = 8k+3$, $-D = 8k+4$, and thus also $-D = 8k+5$ and $-D = 8k+6$. $-D = 8k$ is not possible since D is square-free. So, the only remaining possibility is $-D = 8k-1$ (or equivalently $-D = 8k+7$). □

We wish to look at forms with class number $6n \pm 1$, so we may restrict our study to negative discriminants $\Delta = 8k-1$ with $h(1-8k) = 6n \pm 1$ (since $\Delta = 32k-4 = 4(8k-1)$, $8k-1 \equiv 3 \pmod 4$, and $h(-\Delta) = h(-4\Delta)$, and $\Delta = 4D$).

One quadratic form is then $F = (2, 1, k)$, and by composition, its h^{th} power is the principal form

$$F^h = (1, 1, 2k)$$

Since h represents 2, we have

$$2^h = u^2 + uv + 2kv^2$$

or

$$2^{h+2} = (2u+v)^2 + \Delta v^2$$

Here, $v \neq 0$, since h is odd. Thus, the only possible values of Δ are given by

$$\Delta = \frac{2^{h+2} - (2u+v)^2}{v^2}$$

which are finite in number.

If h is a prime greater than 3, we also have $(2u+v)$ and v odd. To see this, note that any one of $2u+v$ and v being even forces the other of these terms to be even, as well, from equation 5.1. Now,

$$2^h = u^2 + uv + 2kv^2$$
$$\Rightarrow 2^{h-2} = \left(\frac{u}{2}\right)^2 + \left(\frac{u}{2}\right)\left(\frac{v}{2}\right) + 2k\left(\frac{v}{2}\right)^2$$

So, there exists a representation of 2^{h-2} by $(1, 1, 2k)$,

$$2^{h-2} = u'^2 + u'v' + 2kv'^2$$

This is a contradiction because F is a primitive root of the cyclic class group (recall that h is prime), and thus the smallest power of 2 represented by any form class is 2^h. Therefore, v must be odd (or equivalently, $(2u+v)$ and v must be odd).

Example: $h = 5$
Setting $v = 1$, we get, from equation 5.4,

$$\begin{aligned} 127 &= 128 - 1 \\ 119 &= 128 - 9 \\ 103 &= 128 - 25 \\ 70 &= 128 - 49 \\ 47 &= 128 - 81 \\ 7 &= 128 - 121 \end{aligned}$$

We find that $\Delta = 119$ has class number 10, and $\Delta = 7$ has class number 1 (by construction, any h dividing 5 must also appear on this list, because any element F of such a class group would also satisfy $F^h = (1, 1, 2k)$, while the rest of the numbers on the above list have class number 5. From computations with binary quadratic forms, we find that there are four form classes, so the above list is comprehensive. Note that it was unnecessary to vary v here, which may not always be the case.

5.4.1 Class Number 13 and Some Techniques

We have looked at the cases where the class number equals to primes 5 or 7 ($6n \pm 1$). We now look at the case $h = 13 = 6 \cdot 2 + 1$, which was not discussed by Gauss. We have

$$\Delta v^2 = 2^{15} - (2u+v)^2 = 32768 - (2u+v)^2$$

We need to test only those Δ that are prime powers, because for others, the class number is even (a proof of this fact can be found in Section 1 of Chapter 7) Aside from $v = 1$, any other v must have 2 as a quadratic residue for every prime divisor p of v

$(2 \cdot 2^{14} \equiv (2u+v)^2 \pmod{p} \Rightarrow 2 \equiv \left(\frac{(2u+v)^2}{2^7}\right)^2 \pmod{p}$, $p \mid v$, $p \neq 2$, since v is odd).

Let p denote a prime divisor of v. Now, 2 is a quadratic residue mod p if and only if

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$$

The possible values of p are 7, 17, and so on.

If $p = 17$, $2u + v = 2u + 17 \pmod{289}$, so $\Delta v^2 = 2^{15} - (2u+v)^2$

$$\begin{aligned} (2u+v)^2 &\equiv 2^{15} \pmod{17^2} \\ &\equiv 32768 \pmod{17^2} \\ &\equiv 111 \pmod{289} \\ &\equiv 400 \pmod{289} \end{aligned}$$

u	Δ
18	631
67	263
24	607
73	191

So, $289 \mid (2u+v)^2 - 20^2$, or 17^2 divides $(2u+v-20)(2u+v+20)$. If 17 divides $2u+v-20$, then 17 doesn't divide $(2u+v+20)$, so we must have

$$2u + v \equiv \pm 20 \pmod{1)7^2}$$

But

$$(2u+17)^2 = (289 \pm 20)2 \geq (269)^2$$

So,

$$\Delta v^2 = 2^{15} - (2u+v)^2 = -39593 < 0$$

So, v yields only negative Δ. Similarly, $v > 17$ yields negative Δ, or, at best, positive Δ that are clearly "too small" for $h = 13$ (note that one needs a considerably large discriminant to have class number 13).

If $p = 7$, (and $v = 7$, since we are only considering v less than 17),

$$2u + v \equiv \pm 6 \pmod{7^2}$$

So, $2u \equiv -1 \pmod{7^2}$ or $2u \equiv -13 \pmod{17^2}$. This gives the following possibilities.

It may be verified that these four Δ's are prime and indeed have $h = 13$.

The remaining candidates are those with $v = 1$ i.e.

$$\Delta = 32768 - (2u + 1)^2$$

$(2^{15} = 32768)$

These cases may be eliminated or sieved out by separately considering the cases $2u + 1 < 128 = 2^7$ and $2u + 1 > 128$ and calculating the possible quadratic form classes.

Here, $-D = 727$ and $-D = 2143$ arise from the $\Delta < 2^{14}$ or $2u + 1 > 2^7$ case.

Chapter 6

Splitting of Prime Ideals in Field Extensions

6.1 Introduction

Let A be a Dedekind domain with field of fractions K, L be a finite extension of K, and B be the integral closure of A in L.

Fact: If L/K is a finite separable extension, then B is a finitely generated A-module. If A is a Dedekind domain, so is B. This has been proven in Chapter 1.

[7] and [8] are references for this chapter.

Definition 6.1.1. Let P be a nonzero prime ideal of A and β be a nonzero prime ideal of B, If $\beta \supseteq PB$, write $\beta|P$, i.e. β divides P, or β is above P.

We may decompose PB as

$$PB = \prod_{\beta|P} \beta^{e_\beta}$$

where e_β (or $e_{\beta/P}$) is the **ramification index** of P in β.

Proposition 6.1.1. *β divides P if and only if $\beta \cap A = P$.*

Proof. If $\beta \cap A = P$, then it is clear that $\beta \supseteq PB$, i.e. β divides P. Conversely, let β divide P. Then, $\beta \cap A$ is a prime ideal of A (because β is prime) that contains P, and thus must equal P, since A is a Dedekind domain and every prime ideal is thus maximal. □

Proposition 6.1.2. *For each β dividing P, residue field B/β is a finite extension field of A/P.*

Proof. We may consider the composition of the natural inclusion of A in B with the projection map of B onto B/β, i.e.

$$A \to B \longrightarrow B/\beta$$

The kernel of this map is $\beta \cap A = P$. Thus, there is an induced injection of A/P into B/β. Moreover, since we know that B is a finitely generated A-module, it follows that B/β is a finitely generated A/P-module (i.e. vector space), as well. In other words, it is a finite extension field of A/P. □

Note that we may replace β in the above argument by the ideal PB in B to obtain that B/PB is a finitely generated A/P-algebra, in particular, a finitely-generated vector space over A/P.

In the case where $A = \mathbf{Z}$, $K = \mathbf{Q}$, and L is a finite number field, A/P has the form $\mathbf{F}_p$, the finite field with p elements, and thus $L/\mathcal{O}_L$ is also a finite field (with order a power of p).

Definition 6.1.2. The degree $[B/\beta : A/P]$ is called the inertial degree of β over P in B and is denoted f_β or $f_{\beta/P}$.

$$f_\beta := [B/\beta : A/P]$$

Proposition 6.1.3. *Suppose that we have $PB = \prod_{i=1}^{g} P_i^{e_i}$. Then, we have*

$$\sum_i e_i f_i = n = [B/PB : A/P]$$

Proof. Consider the chain of ideals

$$B \supseteq P_1 \supseteq P_1^2 \ldots \supseteq P_1^{e_1} \supseteq P_1^{e_1} P_2 \supseteq \ \ldots \ \supseteq \ P_1^{e_1} P_2^{e_2} \supseteq \ldots \supseteq P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}$$

Since the factorization of ideals into prime ideals in a Dedekind domain is unique, there can be no ideals between consecutive terms in the sequence, since any such intermediate ideal would contain, thus divide, PB. The quotient of any two consecutive terms is given by $\beta/\beta P_i$, and is a vector space over the field B/P_i since it is annihilated by P_i. Moreover, since this vector space has no nontrivial proper subspace as discussed above, it must have dimension one.

So, $[\beta : \beta P_i] = [B : P_i] = f_i$. Therefore, by the multiplicative property of indices, and using the fact that there are exactly e_i consecutive quotients, each of dimension f_i for each i, we have

$$[B : PB] = [B : P_i][P_i/P_i^2] \ldots [P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g - 1} : PB] = \sum_{i=1}^{g} e_i f_i$$

We now prove the second equality under the assumption that B is a free A-module of rank n. In particular, this covers the case where L is a number field. The general case can be proven by an extension of this argument through localization.

If $\{x_1, ..., x_n\}$ is a basis for B over A, we can reduce mod PB to produce a basis for B/PB over A/P. We need to prove only linear independence. Suppose $\sum_{i=1}^{n}(ai + P)(xi + PB) = 0$ in B/PB. Then, $\sum_{i=1}^{n} a_i x_i \in PB$, and so it can be written as $\sum_j b_j y_j$ with $b_j \in B$, $y_j P$. But, $b_j = \sum_k c_{jk} x_k$ with $c_{jk} \in A$, we have $a_k = \sum_j c_{jk} y_j \in P$ for all k. Thus, the $xi + PB$ are linearly independent and form a basis of B/PB over A/PB. The proof is now complete. □

Proposition 6.1.4. *If $\sigma \in G = Aut(L/K)$, then $\sigma(B) = B$. If Q is a prime ideal of B, then so is $\sigma(Q)$. Moreover, if Q lies above the nonzero prime ideal P of A, then so does $\sigma(Q)$. Thus, G acts on the set of prime ideals lying above P.*

Proof. If $x \in B$, then $\sigma(x) \in B$ (apply σ to an equation of integral dependence). Thus $\sigma(B) \subseteq B$. But, $\sigma^{-1}(B)$ is also contained in B (since σ was an arbitrary element of the Galois group). Hence, $B = \sigma(\sigma^{-1}(B)) \subseteq \sigma(B)$. If $PB = \prod_i Q^{e_i}$, then apply σ to both sides to get $PB = \prod_i \sigma(Q_i)^{e_i}$. Since σ preserves all algebraic relations, it is easily verified that the $\sigma(Q_i)$ must be prime ideals. Moreover, σ, being a K-automorphism, fixes every element of A (and thus of P). Therefore $Q \cap A = P \Rightarrow \sigma(Q \cap A) = P \Rightarrow \sigma(Q) \cap A = P$. By the definition of a group action, $Aut(L/K)$ acts on the set of prime ideals lying above in P. □

Proposition 6.1.5. *Let A, B, K, L be as defined at the beginning of the chapter. Suppose L/K is Galois. Then, $Gal(L/K)$ acts transitively on the set of prime ideals β of B which divide a given prime ideal P of A.*

Proof. Let Q_1 and Q_2 be prime ideals lying above P. We have to prove that there exists some $\sigma \in Gal(L/K)$ such that $\sigma(Q_1) = Q_2$. Assume that this is not true. Then, the ideals Q_2 and $\sigma(Q_1)$ are maximal and distinct, so $Q_2 \nsubseteq \sigma(Q_1)$ for each $\sigma \in Gal(L/K)$. The Prime Avoidance Lemma says that if an ideal of a commutative ring is contained in a finite union of prime ideals, then it must be contained in one of these prime ideals. Thus, there exists an element $x \in Q_2$ such that x doesn't lie in any of the $\sigma(Q_1)$'s.

Computing the norm of x relative to L/K, we have $N(x) = \prod_{\sigma \in G}(x)$ (since the extension is Galois). But, one of the σ's is the identity, Q_1 is an ideal, and $\sigma(x) \in B$ for all σ. Thus, $N(x) \in Q_2$. But, $N(x) \in A$ by the Galois theory discussed in a previous section. So, $N(x) \in Q_2 \cap A = P = Q_1 \cap A$. $N(x) = \prod_{\sigma \in G}(x) \in Q_1$, thus one of the $\sigma^{-1}(x)$ lies in Q_1, implying that $x \in \sigma(Q_1)$ as well, which is a contradiction. Therefore, we must have $Q_2 = \sigma(Q_1)$ for some $\sigma \in Gal(L/K)$. □

Corollary 6.1.1. *Let L/K be a Galois extension and $n = [L : K]$ and let P be a nonzero ideal of A. The integers $e_{\beta/P}$ and $f_{\beta/P}$ depend only on P. Denote them by e and f. Let g be the number of prime ideals of B that divide P. Then, by the previous proposition, $n = efg$. This is called the* ***efg formula****.*

Proof. Let $PB = \prod_{i=1}^{g} P_i^{e_i}$. We know that β divides P if and only if it is one of the P_i's. Take $1 \leq j \neq k$ lying between 1 and g. By the previous proposition, there exists $\sigma \in Gal(L/K)$ such that $\sigma(P_j) = P_k$. Apply σ to both sides of $PB = \prod_{i=1}^{g} P_i^{e_i}$ to get $PB = \prod_{i=1}^{g} \sigma(P_i)^{e_i}$. (Here, $\sigma(PB) = PB$, because it is (finitely) generated by the generators of P in A, which are fixed by σ, and because $\sigma(B) = B : PB = \sigma\sigma^{-1}(PB) \subseteq \sigma(PB) \subseteq PB$)

On the right hand side, the power of P_j dividing PB is e_k, and the power of P_k dividing PB is e_j. By uniqueness of prime factorization, we must have $e_j = e_k$. Since j and k were arbitrary, we have $e_j = e_k$ for all indices j and k.

We also have $f_i = [B/P_i : A/P]$. Consider $j \neq i$. Without loss of generality, $f_j \leq f_i$. If $\{x_1 + P_i, x_2 + P_i, \ldots x_{f_i} + P_i\}$ is a basis (as a vector space) of B/P_i over A/P, then the set $\{\sigma(x_1) + P_j, \sigma(x_2) + P_j, \ldots \sigma(x_n) + P_j\} \subseteq P_j$ is claimed to form a basis of B/P_j over A/P. To prove this, it is sufficient to show linear independence (because $f_j \leq f_i$).

Assume a linear dependence relation

$$\sum_i (a_i + P)(\sigma(x_i) + P_j) = 0 \ \ in \ \ B/P_j$$

$$\Rightarrow \sum_i \sigma(a_i x_i) \in P_j \Rightarrow \sigma(\sum_i a_i x_i) \in P_j$$

$$\Rightarrow \sum_i a_i x_i \in \sigma^{-1}(P_j) = P_i$$

By linear independence in B/P_i, we have $a_i \in P_i \cap A = P$, and thus the set $\{\sigma(x_1) + P_j, \sigma(x_2) + P_j, \ldots \sigma(x_n) + P_j\}$ is linearly independent. Thus, $f_j \geq f_i$, and hence $f_j = f_i$. Since i and j were arbitrary, we must have f_β independent of β. Denoting the common values of the e_i's by e and the f_i's by f, and from a previous proposition, we have $efg = n = [L : K]$. □

Definition 6.1.3. Given a Galois extension L/K, we say that a prime ideal P of A is **ramified** when $e_P > 1$.

Definition 6.1.4. If $e_P = 1$, we say that P is **unramified**.

Definition 6.1.5. If $e = f = 1$, we say that P **splits completely** in L.

Definition 6.1.6. Let L/K be a finite Galois extension of number fields, and β be a prime ideal of $\mathcal{O}_K$. Define D_β, the Decomposition Group of β to be

$$D_\beta = \{\sigma \in Gal(L/K) \mid \sigma(\beta) = \beta\}$$

Each $\sigma \in D_\beta$ induces an automorphism $\bar{\sigma}$ on $l := \frac{\mathcal{O}_L}{\beta}$ whose fixed field is $k = \frac{\mathcal{O}_K}{P}$ where $P = \beta \bigcap \mathcal{O}_K$. Moreover, the map $\sigma \to \bar{\sigma}$ is naturally a group homomorphism.

Definition 6.1.7 (Inertia Group)**.** The kernel $I = I_D$ of the above homomorphism, is called the inertia group of Q.

The inertia group is a normal subgroup of the decomposition group, as it is the kernel of a homomorphism. It is given explicitly by

$$I = \{\sigma \in D : \sigma(x) + Q = x + Q, \forall\ x \in B\} = \{\sigma \in D : \sigma(x)x \in Q, \forall\ x \in B\}$$

Theorem 6.1.1. *Assume that the extension $(B/Q)/(A/P)$ is separable. Let D denote the decomposition group of Q. Then, $l : k = B/Q : A/P$ is a Galois extension. Moreover, the natural homomorphism $\sigma \to \bar{\sigma}$ of D to $Gal[(B/Q)/(A/P)]$, which has been defined above, is surjective with kernel I. Therefore, $Gal[(B/Q)/(A/P)] \cong D/I$.*

Proof. The field extension $(B/Q)/(A/P)$ is separable is finite and separable. By the primitive element theorem, it must be a simple extension. Let $\bar{x}$ be a primitive element of B/Q over A/P. Let $x \in B$ be a representative of $\bar{x}$. Let $h(X) = X^r + a_{r1}X^{r1} + \ldots + a_0$ be the minimal polynomial of x over F_D. The coefficients a_i belong to $A_D = B \cap F_D$ since each of them lies in a finitely generated module

of B (using the fact that x is primitive, which in turn must be a finitely generated module of A (thus they are all integral over A, and must lie in B). The roots of h are all of the form $\sigma(x)$, $\sigma \in D$. (We are working in the extension L/K_D, with Galois group D.) If we reduce the coefficients of $hmodP_D$, the resulting polynomial $h(X)$ has coefficients in A/P. The roots of h are of the form $\sigma(x)$, $\sigma \in D$ (because x is a primitive element). Since $\sigma \in D$ means that $\sigma(Q) = Q$, all conjugates of x over A/P lie in B/Q. By the basic theory of splitting fields, B/Q is a Galois extension of A/P.

Therefore, every conjugate $\bar{x}$ over A/P is of the form $\sigma(\bar{x})$, every A/P-automorphism of B/Q (necessarily determined by its action on x), is of the form $\bar{\sigma}$ where $\sigma \in D$. By the definition of the inertial group, $\bar{\sigma}$ is trivial iff $\sigma \in I$. Thus, the map $\sigma \to \bar{\sigma}$ is surjective and has kernel I. □

Proposition 6.1.6. *For Q dividing P and all other notations as before, the decomposition group D_Q has order $e_P f_P$.*

Proof. By the orbit-stabilizer theorem applied to the action of G on the set of primes Q dividing P, the size of the orbit of Q is the index of the stabilizer subgroup D_Q. Since the action is transitive, there is only one orbit of size g. So, $g = [G : D_Q] = |G|/|D_Q|$, hence $|D_Q| = n/g = efg/g = ef$, independent of Q.

Note also that distinct conjugates of Q determine distinct cosets of D_Q, since

$$\sigma_1 D = \sigma_2 D \Leftrightarrow \sigma_2^{-1}\sigma_1 \in D_Q \Leftrightarrow \sigma_1(Q) = \sigma_2(Q)$$

□

Corollary 6.1.2. *The order of I is e. Thus the prime ideal P does not ramify if and only if the inertia group of every prime ideal Q lying over P is trivial.*

Proof. By definition of relative degree, the order of $Gal[(B/Q)/(A/P)]$ is f. By the previous proposition, the order of D is ef. Thus by the isomorphism in the previous theorem, the order of I must be e. □

Definition 6.1.8 (Decomposition and Inertial Fields)**.** The decomposition field F_D is defined to be the fixed field of the decomposition group D_Q, and the inertial field F_I is defined to be the fixed field of the inertial group I_Q.

Consider the extension $F_{D_Q} \subseteq L$ with Galois group D_Q (this holds since L/K is a Galois extension). Let $A_{D_Q} = B \cap F_{D_Q}$ be the integral closure of A in F_{D_Q}. Let P_D be the prime ideal $Q \cap A_{D_Q}$. Q is the only prime factor of $P_D B$, because all primes in the factorization are conjugate, and $\sigma(Q) = Q$ for all $\sigma \in D$, by definition of D.

Proposition 6.1.7. *Fix a prime ideal Q dividing P and denote D_Q by D, e_P by e and f_P by f. Let $P_D B = Q^{e'}$ and $f' = [B/Q : A_D/P_D]$. Then $e' = e$ and $f' = f$. Moreover, $A/P \cong A_D/P_D$.*

Proof. Observe that $e'f' = [L : K_D] = |D| = ef$. Now, $A/P \subseteq A_D/P_D \subseteq B/Q$, so $f' \leq f$. Also, $PA_D \subseteq Q \cap F_D = P_D$, so P_D divides PA_D, hence $P_D B$ divides $PA_D B = PB$. Consequently, $e' \leq e$, and this forces $e' = e$ and $f' = f$. Thus, the dimension of B/Q over A_D/P_D is the same as the dimension of B/Q over A/P. Since A/P can be regarded as a subfield of A_D/P_D, the proof is complete. □

In the basic $AKLB$ setup, with L/K a Galois extension, we now assume that K and L are number fields.

Definition 6.1.9 (Frobenius Element/Automorphism)**.** Let L/K be a finite Galois extension of number fields. Let β be a prime ideal of $\mathcal{O}_L$ and $P = \beta \bigcap \mathcal{O}_K$. Assume P which does not ramify in L (i.e. $e_P = 1$). Then, $l = \frac{\mathcal{O}_L}{\beta}$ is a finite extension of the field $k = \mathcal{O}_K/P$ of q elements (q is a power of some rational prime).

Now, $e_{\beta/P} = 1$, so $I_\beta = \{1\}$. Thus,

$$D_\beta \cong Gal(l/k) \quad \left(k = \frac{\mathcal{O}_K}{P}\right)$$

Since $k = \mathbf{F}_q = Gal(l/k)$ is cyclic and generated by the map $I \to I^q$. Denote by σ_q the corresponding element in $D_\beta \subset Gal(L/K)$. Call σ the Frobenius automorphism related to the extension L/K.

We use the notation $\left[\frac{L/K}{Q}\right]$ for the Frobenius automorphism.

Proposition 6.1.8. *If $\tau \in G$, then $\left[\frac{L/K}{\tau(Q)}\right] = \tau \left(\left[\frac{L/K}{Q}\right]\right) \tau^{-1}$*

Proof. If $x \in B$, then $\left[\frac{L/K}{Q}\right] \tau^{-1} x \equiv \tau^1 x^q = \tau^1 x^q \pmod{Q}$. Apply τ to both sides to conclude that $\tau \left(\left[\frac{L/K}{Q}\right]\right) \tau^{-1}$ satisfies the defining equation for $\left[\frac{L/K}{\tau(Q)}\right]$. Since the Frobenius is uniquely determined by its defining equation, the result follows. □

Lemma 6.1.1. *Let L/K, β, P be as before. Then, the Frobenius automorphism is the unique element $\sigma \in Gal(L/K)$ such that $\forall\ \alpha \in \mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{\mathbf{N}(P)} \pmod{\beta}$$

where $\mathbf{N}(P) = |\mathcal{O}_K : P| = q$.

Corollary 6.1.3. *If L/K is abelian, then $\left[\frac{L/K}{Q}\right]$ depends only on P, and we write the Frobenius automorphism as $\left(\frac{L/K}{P}\right)$ and sometimes call it the* Artin symbol.

6.2 The Chebotarev Density Theorem

The Chebotarev density theorem gives a statistical description of the splitting of primes in a given Galois extension K of the field $\mathbf{Q}$. In general, a prime integer (more precisely, the principal ideal generated by it) will factor into several prime ideals in $\mathcal{O}_K$. For a given prime, only finitely may splitting patterns may occur. The full description of splitting of every p in a general Galois extension is an unsolved problem. The Chebotarev Density Theorem states that the frequency of occurrence of a given pattern for all primes less than or equal to N (for some large integer N) tends to a given limit as N goes to infinity.

In the special case in which K is a Galois extension of $\mathbf{Q}$ of degree n, the primes that completely split in K have density $1/N$ among all primes. Primes may be

assigned an invariant called the Frobenius element, a representative of a well-defined conjugacy class in the Galois group $Gal(K/\mathbf{Q})$. The asymptotic distribution of these invariants is uniforms over the group, so that a conjugacy class with k elements occurs with frequency asymptotic to k/n.

In this section, we use the notation $\Delta(f)$ for the discriminant of the form f. Proofs of unproven results may be found in the references [19], [2], and [16].

Definition 6.2.1 (Dirichlet/Analytic Density)**.** A set S of prime numbers has Dirichlet density δ if

$$\left(\sum_{p\in S}\frac{1}{p^s}\right)\left(\sum_{p \text{ prime}}\frac{1}{p^s}\right)^{-1} \to \delta$$

as s decreases to 1.

Definition 6.2.2 (Natural Density)**.** A set S of prime numbers has natural density δ if

$$\frac{\#\{p \le x : p \in S\}}{\#\{p \le x : p \text{ prime}\}} \to \delta \text{ as } x \to \infty$$

In general, let f be a polynomial with integer coefficients and leading coefficient 1. Let n denote the degree of f. Suppose that $\Delta(f) :\neq 0$. Then, f has distinct zeroes α_1, α_2, ..., α_n in a suitable extension field of $\mathbf{Q}$.

Let $K = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$, and G be the Galois group of f over the field extension $K/\mathbf{Q}$. Each $\sigma \in G$ permutes α_1, ..., α_n and is determined completely by its action on them. Thus G lies inside S_n.
Write $\sigma \in G$ as a product of disjoint cycles (including those of length 1), to obtain a cycle patern of σ, i.e. a partition n_1, ..., n_t of n. where the n_i are the lengths of the individual cycles constituting that of σ.

If p doesn't divide the discriminant $\Delta(f)$ of the form f, we can write f modulo p as a product of distinct irreducible factors over $\mathbf{F}_p$. The degrees of these irreducible factors form the decomposition type of f modulo p, which is also a partition of n.

Theorem 6.2.1 (Frobenius)**.** *The density of the set of primes p for which f has a given decomposition type $n_1 n_2 \ldots n_t$ exists, and it is equal to $1/|G|$ times the number of $\sigma \in G$ with cycle pattern $n_1 n_2 \ldots n_t$, where G is the Galois group of f.*

Thus, the density of the set of primes for which f splits into linear factors (corresponding to the identity permutation) is $1/|G|$.

Definition 6.2.3 (Frobenius Substitution of p)**.** There is a natural association between a prime not dividing $\Delta(f)$ and an element $\sigma_p \in G$, such that the decomposition of f modo p is the same as the cycle type of σ_p. Here, σ_p is the Frobenius symbol of p, and is well-defined only up to conjugacy in G.

Recall that the Frobenius map (or here, also, the Artin map), as described in the previous section, is an automorphism of the field $\overline{\mathbf{F}_\mathbf{p}}$ of characteristic p, and the Frobenius substitution σ_p is an automorphism of the field k of characteristic 0. To relate the two fields, we develop a way of taking elements of $K = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ modulo p so that the zeroes of $(f \pmod p)$ can be regarded as (zeroes of f) $\pmod p$.

Let f be a polynomial with integer coefficients. We are interested in the frequency of each factorization pattern of f modo each prime p (except in the cases where a double factor occurs, i.e. when p divides the discriminant of f.

In case of an abelian extension (i.e. the Galois group is abelian) $K \subset L$, we have an Artin symbol $A(p) \in Gal(L/K)$ for primes p not dividing $\Delta_{L/K}$, with the unique property that for all $\alpha \in \mathcal{O}_L$,

$$A(P)(\alpha) \equiv \alpha^{\#\frac{\mathcal{O}_K}{P}} \pmod{P}\mathcal{O}_L$$

This element $A(P)$ is often called the Frobenius at P.

If we drop the abelian condition and only require the extension to be Galois, then the definition of the Artin map depends on the choice of the prime Q lying over the prime $P = (p)$. Upon this choice, when p not dividing $\Delta_{L/K}$, there is a unique $Frob_Q \in G$ such that for all $\alpha \in \mathcal{O}_L$,

$$Frob_Q(\alpha) \equiv \alpha^{\#\frac{\mathcal{O}_K}{P}} \pmod{Q}$$

This really does depend on the choice of Q. Given another choice Q'/P, there is an element $\sigma \in Gal(L/K)$ such that $Q' = \sigma(Q)$ and we see that

$$Frob_{Q'} = \sigma Frob_Q \sigma^{-1}$$

since

$$\begin{aligned}\sigma Frob_Q \sigma^{-1}((\alpha)) &= \sigma(\sigma^{-1}(\alpha)^{\#\mathcal{O}_K/P})) \pmod{Q} \\ &= \sigma(\sigma^{-1}(\alpha^{\#\mathcal{O}_K/P})) \pmod{Q} \\ &= \alpha^{\#\mathcal{O}_K/P} \pmod{Q}\end{aligned}$$

In this case, we must treat not just the elements themselves but the entire conjugacy class.

Definition 6.2.4. Define the Frobenius symbol of P in L/K to be the conjugacy class $\{Frob_Q : Q \mid P\}$.

$Frob_P$ is also denoted by σ_P.

For an abelian group, this set contains a single element.

The Frobenius element restricts well to subfields of fields. If $K \subset L$, $L \subset M$ are Galois extensions of fields, then $\sigma_P \in Gal(M/K)$ maps by restriction to $\sigma_P \in Gal(L/K)$.

Knowledge of σ_P allows us to control the decomposition of P in every subfield. Given a subextension $K \subset E \subset L$ not necessarily Galois, write

$$P\mathcal{O}_E = \prod_{Q|P} Q$$

If P is unramified, the decomposition of P is given by the sequence of residue class degrees $f(Q/P)$. The Frobenius symbol tells us what they are.
Let $E = L^H$ be the fixed field under the subgroup H of the group G.

Fact: The decomposition type of P in $\mathcal{O}_E$ (the "factorization pattern", which is a partition of the degree $[E : K]$) is equal to the cycle structure of σ_P acting on G/H where $E = L^H$.

Note that G/H is a set of $[E : K]$ cosets. It comes with the action of G, hence a cycle structure of σ on this set. Note that this cycle structure only depends on the conjugacy class of σ_P.

Let $E = K(\alpha)$ and $f \in \mathcal{O}[x]$ be the minimal polynomial of α and assume that p does not divide $\Delta(f)$. We have two factorization patterns to consider:

- the factorization pattern of $f \pmod p$ in $\frac{\mathcal{O}_K}{P}$[X]
- the cycle structure of the Frobenius symbol

Since α generates E over K, for any τ, $\tau\alpha = \alpha \Leftrightarrow \tau \in H$ & $\tau_1\alpha = \tau_2\alpha \Leftrightarrow \tau_1 H = \tau_2 H$. So, instead of the cycle structure on G/H, we may instead consider the cycle on the K-conjugates of α in L.

By concatenating, we can take the product of any distinct irreducible polynomials. We still have the fact that the factorization pattern of f modo p is the same as the cycle of σ_P acting on the set of roots of f.

Theorem 6.2.2 (Chebotarev Density Theorem)**.** *Let $K \subset L$ be Galois, and let $C \subset G = Gal(L/K)$ be a conjugacy class. Then, $\{P$: P is a prime of K, p doesn't divide divide $\Delta_{L/K}$, $\sigma_P \in C\}$ has density $\frac{|C|}{|G|}$. In particular, this ratio is always ¿0, so there always exist such primes. Every element of the Galois group is the Frobenius element of some prime.*

Let S be the set of primes of K. We have already defined the notions of natural and analytic density of primes. If the natural density exists, it is equal to the analytic density. The converse is not true. The Chebotarev density theorem is true with both notions of density.

The theorem goes both ways. If the densities are known, we can get information about the Galois group. If the Galois group is known, we can predict the densities that occur by computing the set of conjugacy classes of the group.

Applying this theorem to the Abelian case, combine the Chebotarev denisty theorem with classification of abelian extensions that comes from Galois theory.

$$\mathbf{Q}(\zeta_m) \supset \mathbf{Q}$$

$$G \cong (\frac{\mathbf{Z}}{m\mathbf{Z}})^*$$

by the isomorphism

$$\sigma_P \leftrightarrow (p \pmod m)$$

For any $a \pmod m \in (\frac{\mathbf{Z}}{m\mathbf{Z}})^*$, Chebotarev density theorem then implies that $\{p : p \equiv a \pmod m\}$ has density $\frac{1}{\phi(m)}$, a statement that is a bit stronger than the Dirichlet theorem on primes in arithmetic progressions.

6.3 Ramification in Number Fields

We first describe the theory that holds in a general number field K and then look, in particular, at quadratic number fields.

Let p be a rational prime number. The ideal generated by p in the ring of integers $\mathcal{O}_K$ of a number field K has a unique factorization in terms of the prime ideals of $\mathcal{O}_K$. We have seen that this factorization looks like $p\mathcal{O} = P_1^{e_{P_1}} P_2^{e_{P_2}} \dots P_g^{e_{P_g}}$, and also that $n = [K : \mathbf{Q}] = \Sigma_{i=1}^{g} e_{P_i} f_{P_i}$, where f_{P_i} denotes the intertial index of P_i, i.e. $f_{P_i} = [\mathcal{O}_K/P_i : \mathbf{Z}/\mathbf{pZ}]$. Also, since the extension $K/\mathbf{Q}$ is Galois, all the e_{P_i}'s and f_{P_i}'s are equal, and we have the formula n = efg.

In general, there is no straightforward method to compute the factorization of $p\mathcal{O}_K$. However, when $\mathcal{O}_K = \mathbf{Z}[\mathcal{O}]$, we can use the following result.

Theorem 6.3.1 (Kummer)**.** *Let K be a number field and $p \in \mathbf{Z}$ be prime. Assume that there exists θ such that $\mathcal{O}_K = \mathbf{Z}[\theta]$, where f is the minimal polynomial of $\mathcal{O}$ and $\overline{f}$ is the reduction of f modulo p. Let*

$$\overline{f}(X) = \prod_{i=1}^{g} \phi_i(X)^{e_i}$$

be the factorization of $f(x)$ in $\mathbf{F}_p[X]$, with the $\phi_i(X)$'s co-prime and irreducible. Set

$$P_i = (p, f_i(\theta)) = p\mathcal{O}_K + f_i(\theta)\mathcal{O}_K$$

where f_i is any lift of ϕ_i to $\mathbf{Z}[X]$, i.e. $\overline{f_i} = \phi_i \pmod p$. Then,

$$p\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g}$$

is the factorization of $p\mathcal{O}_K$ in $\mathcal{O}_K$.

Proof. Note that

$$\frac{\mathcal{O}_K}{p\mathcal{O}_K} = \frac{\mathbf{Z}[\mathcal{O}]}{p\mathbf{Z}[\mathcal{O}]} \simeq \frac{\mathbf{Z}[X]/f(X)}{p(\mathbf{Z}[X]/f(X))} \simeq \frac{\mathbf{Z}[X]}{(p, f(X))} \simeq \frac{\mathbf{F}_p[X]}{(\overline{f}(X))})$$

where $\overline{f} = f \pmod p$.

Let $A := \frac{\mathbf{F}_p[X]}{(\overline{f}(X))})$

If $\psi(X) \in \mathbf{F}_p[X]$, $\psi(X) \pmod{\overline{\ }} f(X) \in A$ and $g \in \mathbf{Z}[X]$ such that $\overline{g} = \psi$, then its preimage is given by $g(\mathcal{O})$ (i.e. the inverse of the isomorphism $\frac{\mathbf{Z}[\mathcal{O}]}{p\mathbf{Z}[\mathcal{O}]} \simeq \frac{\mathbf{F}_p[X]}{(\overline{f}(X))}$) is evaluation at $\mathcal{O}$).

By the Chinese Remainder Theorem, we have

$$A = \frac{\mathbf{F}_p[X]}{(\overline{f}(X)))} \simeq \prod_{i=1}^{g} \frac{\mathbf{F}_p[X]}{\phi_i(X)^{e_i}}$$

Since by assumption, the ideal $\overline{f}(X)$ has a prime factorization given by $\overline{f}(X) = \prod_{i=1}^{g} (\phi_i(X))^{e_i}$.

We are now ready to understand the structure of prime ideals of both $\frac{\mathcal{O}_K}{p\mathcal{O}_K}$ and A, thanks to which we will prove that $P_i = (p, f_i(\mathcal{O}))$ is prime, that any prime divisor of $p\mathcal{O}_K$ is actually one of the P_i, that the powers e_i appearing in the factorization of $\overline{f}$ are bigger than or equal to the ramification index e_{P_i} of P_i. Then, invoke the result that $n = \sum_{i=1} e_i f_i$ to show that $e_i = e_{P_i}$.

Since

$$A = \frac{\mathbf{F}_p[X]}{(\overline{f}(X)))} \simeq \prod_{i=1}^{g} \frac{\mathbf{F}_p[X]}{\phi_i(X)^{e_i}},$$

the maximal ideals of A are given by $(\phi_i(X))^{e_i}$, and the degree of the extension $\frac{A}{\phi_i(X)A}$ over $\mathbf{F}_p$ is the degree of ϕ_i.

Since $A \simeq \frac{\mathcal{O}_K}{p\mathcal{O}_K}$, we get that the maximal ideals of $\frac{\mathcal{O}_K}{p\mathcal{O}_K}$ are the ideals generated by $f_i(\mathcal{O}) \pmod p)\mathcal{O}_K$. Consider the projection

$$\pi : \mathcal{O}_K \to \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$

We have

$$\begin{aligned}
\pi(\overline{P_i}) &= \pi(p\mathcal{O}_K + f_i(\mathcal{O})\mathcal{O}_K) \\
&= f_i(\mathcal{O})\mathcal{O}_K \pmod{p\mathcal{O}_K} \\
&= \phi_i(\mathcal{O})\mathcal{O}_K \pmod{p\mathcal{O}_K}
\end{aligned}$$

We have seen that $f_i(\mathcal{O})\mathcal{O}_K$ are maximal ideals in $\frac{\mathcal{O}}{p\mathcal{O}}$, and are thus prime.

Therefore, P_i, being the pre-image of a prime ideal under the above projection, is a prime ideal. Furthermore, since $P_i \supset p\mathcal{O}_K$, $P_i | p\mathcal{O}_K$ and the inertial degree is equal to the degree of the polynomial ϕ_i.

$$\begin{aligned}
f_{P_i} &= \left[\frac{\mathcal{O}_K}{P_i} : \mathbf{F}_p\right] \\
&= \left[\frac{\mathcal{O}_K/p\mathcal{O}_K}{\pi(P_i)} : \mathbf{F}_p\right] \\
&= \left[\frac{\mathcal{O}_K/p\mathcal{O}_K}{f_i(\mathcal{O}) \pmod{p\mathcal{O}_K}} : \mathbf{F}_p\right] \\
&= \left[\frac{A}{(\phi_i(X))A} : \mathbf{F}_p\right] \\
&= \deg \phi_i
\end{aligned}$$

Now, every prime ideal P in the factorization of $p\mathcal{O}_K$ is one of the P_i, since the image of P by π is a maximal ideal of $\mathcal{O}_K/p\mathcal{O}_K$.

We are left to look at e_{P_i}, the ramification index of P_i. The ideal ${\phi_i}^{e_i}A$ of A belongs to $\frac{\mathcal{O}_K}{p\mathcal{O}_K}$ via the isomorphism $\frac{\mathcal{O}_K}{p\mathcal{O}_K} \simeq A$ and its preimage in $\mathcal{O}_K$ by π^{-1} contains ${P_i}^{e_i}$.

In $\frac{\mathcal{O}_K}{p\mathcal{O}_K}$, we have

$$\mathcal{O}_K = \cap_{i=1}^{g} \phi_i(\mathcal{O})^{e_i}$$

i.e.

$$\begin{aligned} p\mathcal{O}_K &= \pi^{-1}(\mathcal{O}_K) \\ &= \cap_{i=1}^{g} \pi^{-1}(\phi_i^{e_i} A) \supset \cap_{i=1}^{g} P_i^{e_i} \\ &= \prod_{i=1}^{g} P_i^{e_i} \end{aligned}$$

Thus, $\prod_{i=1}^{g} P_i^{e_i}$ is divided by $p\mathcal{O}_K = \prod_{i=1}^{g} P_i^{e_{P_i}}$, and so $e_i \geq e_{P_i}$.

$$n = [K : \mathbf{Q}] = \sum_{i=1}^{g} e_{P_i} f_{P_i} \leq \sum_{i=1}^{g} e_i \deg(\phi_i) = \dim_{\mathbf{F}_p}(A) = \dim_{\mathbf{F}_p} \frac{\mathbf{Z}^n}{p\mathbf{Z}^n} = n$$

Thus, $e_{P_i} = e_i$. □

Thus, we have a concrete method to compute the factorization of $p\mathcal{O}_K$ for a prime p:

1. Choose a prime $p \in \mathbf{Z}$
2. Let f be the minimal polynomial of θ where $\mathcal{O}_K = \mathbf{Z}[\theta]$
3. Let $\bar{f} = \prod_{i=1}^{g} \phi_i(X)^{e_i}$ be the factorization of $\overline{f} = f \pmod{p}$
4. Lift each ϕ_i to a polynomial $f_i \in \mathbf{Z}[X]$
5. Compute $P_i = (p, f_i(\theta))$ by evaluating f_i at θ
6. We have $p\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g}$

Recall the following definition.

Definition 6.3.1. A prime p is called inert if $p\mathcal{O}_K$ is prime, i.e. $g = 1, e = 1, f = n$, and is called totally ramified if $e = n, g = 1, f = 1$.

In general, the following theorem holds.

Theorem 6.3.2. *Let K be a number field. If a prime p is ramified, it divides the discriminant d_K.*

Proof. Let $\overline{P}$ be a prime ideal dividing $p\mathcal{O}_K$ such that $\overline{P}^2 | p\mathcal{O}_K$ ($\overline{P}$ exists because p is ramified). Write

$$p\mathcal{O}_K = \overline{P} I$$

where I is an ideal divisible by all prime ideals above p.

Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subset \mathcal{O}_K$ be a $\mathbf{Z}$-basis of $\mathcal{O}_K$ and let α be an element of I that does not lie in $p\mathcal{O}_K$ (α exists because $p\mathcal{O} \subset I$ (properly) since $\overline{P}$ divides I). Write

$$\alpha = b_1\alpha_1 + \dots + b_n\alpha_n, \ b_i \in \mathbf{Z}$$

Since $\alpha \notin p\mathcal{O}_K$, there exists b_i such that p doesn't divide b_i, say p doesn't divide b_1
Recall

$$d_K = \det \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

where σ_i are the n embeddings of K into $\mathbf{C}$

Let L be the Galois closure of K. All the conjugates of α belong to L. We also know that α belongs to all the primes of $\mathcal{O}_K$ above p. Similarly, $\alpha \in L \subseteq L$ belongs to all primes β of $\mathcal{O}_L$ lying above p, since $\beta \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ above p and contains α.

Fix a prime β above p in $\mathcal{O}_L$. Then $\sigma_i(\beta)$ is also a prime ideal of $\mathcal{O}_L$ above p ($\sigma_i(\beta) \in L$ since $L/\mathbf{Q}$ is Galois, $\sigma_i(\beta)$ is prime because β is, and $p = \sigma_i(p) \in \sigma_i(\beta)$) Now, $\sigma_i(\alpha) \in \beta, \forall\ \sigma_i$, thus the first column of the matrix involved in computing d_K is in β, we have $d_K \in \beta \cap \mathbf{Z} = p\mathbf{Z}$, as required. The proof of the theorem is now complete. □

Corollary 6.3.1. *There are only finitely many primes that ramify in a given number field.*

6.3.1 Ramification in Quadratic Number Fields

In the case of quadratic fields, e, f and g may take values 1 or 2, and the only possibilities for a prime p are the following.

1. If g = 2, e = f = 1, $p\mathcal{O}_K = P_1P_2$ for some distinct primes P_1, P_2 of $\mathcal{O}_K$. p is a decomposed or split prime.
$$\frac{\mathcal{O}_K}{P_i} \cong \frac{\mathbf{Z}}{p\mathbf{Z}}$$

2. g = 1, e = 2, f = 1 $p\mathcal{O}_K = P^2$, P is a prime ideal of $\mathcal{O}_K$. p is a ramified prime.
$$\frac{\mathcal{O}_K}{P_i} \cong \frac{\mathbf{Z}}{p\mathbf{Z}}$$

3. g = 1, e = 1, f = 2 $p\mathcal{O}_K = P$, where P is a prime ideal of $\mathcal{O}_K$. p is an inertial or inert prime.
$$[\frac{\mathcal{O}_K}{P_i} : \frac{\mathbf{Z}}{p\mathbf{Z}}] = 2$$

Let $(\frac{a}{b})$ denote the Legendre symbol.

Theorem 6.3.3. *Let $K = \mathbf{Q}(\sqrt{m})$ be a quadratic field and p be a rational prime. If $m \equiv 1 \pmod 4$, p is*

- *decomposed if $(\frac{m}{p}) = 1, p \neq 2$ or if $p = 2$, $m \equiv 1 \pmod 8$ 8,*
- *ramified if $p|m$, i.e. $(\frac{m}{p}) = 0$ (here $p \neq 2$)*

- *inert if* $(\frac{m}{p}) = -1$ *if* $p \neq 2$ *or if* $p = 2$ *and* $m \equiv 1 \pmod 8$ *8.*

If $m \equiv 2, 3 \pmod 4$*,* p *is*

- *decomposed if* $(\frac{m}{p}) = 1, p \neq 2$
- *ramified if* $p = 2$ *or* $(\frac{m}{p}) = 0$
- *inert if* $p \neq 2$ *and* $(\frac{m}{p}) = -1$

Proof. CASE-1: $m \equiv 2, 3 \pmod 4$

We have $\mathcal{O}_K = \mathbf{Z}[\sqrt{m}]$

$f(X) = X^2 - m$ is the minimal polynomial of $\mathcal{O} = \sqrt{m}$. By Kummer's theorem, the factorization of $p\mathcal{O}_K$ is determined by the factorization of
$\overline{f}(X) = f(X) \pmod p$

- If $p \mid m$ or $p = 2$, then clearly, $\overline{f}(X) = X^2$ or $(X-1)^2$ [with $(X-1)^2$ occurring in case of these restrictions if and only if p doesn't divide m and $p = 2$) and thus
$$(p)\mathcal{O}_K = Q^2, \ \ , Q = (p, \sqrt{m}) \ \text{or} \ \ Q = (p, 1 - \sqrt{m})$$
By Kummer's theorem, p is ramified.

- If p does not divide m and $p \neq 2$, then $\overline{f}(X) = X^2 - \overline{m}$ is either irreducible in $\frac{\mathbf{Z}}{p\mathbf{Z}}[X]$ or has two distinct roots in $\frac{\mathbf{Z}}{p\mathbf{Z}}$.

  - If $\overline{f}(X)$ is irreducible, then p is inert, since it has only one prime ideal (with power 1) in its factorization.
  - If $\overline{f}(X)$ is reducible,

$$X^2 - m = (X + a)(X + b) \pmod p = X^2 + (a + b)X + ab \pmod p$$
$$\Rightarrow b = -a \pmod p, ab = -m \pmod p$$
$$m = a^2 \pmod p$$

    p does not divide a or b since it does not divide m, so m is a square $\pmod p$. Moreover, we must have $b \neq a \pmod p$, else $2b = 0 \pmod p \Rightarrow p \mid b$, a contradiction. By Kummer's theorem, p is split into two distinct prime ideal factors.

We have proven the $m \equiv 2, 3 \pmod 4$ case in the theorem.

CASE-2: $m \equiv 1 \pmod 4$

We have $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{m}}{2}]$

$f(X) = X^2 - X - \frac{m-1}{4}$ is the minimal polynomial of $\frac{1+\sqrt{m}}{2}$ over $\mathbf{Q}$

- If $p = 2$, $\overline{f}(X)$ has a root modulo p if and only if $\frac{m-1}{4} \equiv 0 \pmod 2$, i.e. $m \equiv 1 \pmod 8$
  - In this case, i.e. if $\frac{m-1}{4} \equiv 0 \pmod p 2$, each of the two distinct elements in $\frac{mathbfZ}{2\mathbf{Z}}$ is a root of $\overline{f}(X)$, so p is a split prime.
  - If $p = 2$ and $\frac{m-1}{4} \equiv 1 \pmod 2$, $\overline{f}(X)$ is irreducible, thus p is inert.
- If $p \neq 2$,
  - If the roots $\frac{1 \pm \sqrt{m}}{2}$ of $X^2 - X - \frac{m-1}{4}$ exist in $\frac{\mathbf{Z}}{p\mathbf{Z}}$ (they are necessarily distinct), their sum, $\sqrt{m}$ exists in $\frac{\mathbf{Z}}{p\mathbf{Z}}$ (note that 2 is a unit $\pmod p$). Equivalently, m is a square modulo p, i.e. $(\frac{m}{p}) = 1$. Kummer's theorem shows that p is a split prime.
  - Moreover, $\overline{f}(X)$ has multiple roots in $\frac{\mathbf{Z}}{p\mathbf{Z}}$ if and only if p divides m. Thus, by Kummer's theorem, p is ramified if and only if p divides m, i.e. if and only if $(\frac{m}{p}) = 0$.
  - Thus, in this case, p is inert if and only if $(\frac{m}{p}) = -1$

We have thus completed the proof by showing the $m \equiv 1 \pmod 4$ case in the theorem. □

In particular, looking at the ramified conditions in both the above cases, we have the following result.

Corollary 6.3.2. *Let K be a number field. A rational prime p is ramified in $\mathcal{O}_K$ if and only if p divides the discriminant of K.*

Theorem 6.3.4 (Fermat's Two Square Theorem)**.** *An odd prime p can be expressed as a sum of two squares if and only if $p \equiv 1 \pmod 8$ 4. These primes are also called Pythagorean primes.*

Proof. Take $K = \mathbf{Q}(i)$, so that $\mathcal{O}_K = \mathbf{Z}[i]$. Now, a prime p is the sum of two squares if and only if there exist integers nonzero x and y such that

$$p = x^2 + y^2 = (x + iy)(x - iy)$$

Thus, p must be a decomposed or split prime (it cannot be ramified because that would imply that $x + iy = x - iy \pmod p$ or $2y = 0 \pmod p$ or p divides x, a contradiction to the assumption.) We see in the previous theorem (noting that $m = -1 = 3 \pmod 4$) that this implies that $(\frac{-1}{p}) = 1$ or $(-1)^{\frac{p-1}{2}} = 1$ or $\frac{p-1}{2} = 0 \pmod 2$ or $p = 1 \pmod 4$.

Conversely, suppose that $p \equiv 1 \pmod 4$. By the theorem, p is a decomposed prime in K, i.e. it is not a Gaussian prime. Then, we have $p\mathbf{Z}[i] = P_1 P_2 = ((a + ib)(\gamma)$, where $a + bi$ and γ are Gaussian integers, since $\mathbf{Z}[i]$ is a PID. Since by definition, a Gaussian prime is an element of $\mathbf{Z}[i]$ whose norm is prime, or in other words, a Gaussian integer that is not the product of Gaussian integers of smaller

norm, $a+bi$ and γ are Gaussian integers with norm less than the norm p^2 of p (and hence also of norm > 1). Taking conjugates of both sides we get

$$p = (a - ib)\overline{\gamma}$$

Multiplying these two expressions for p gives

$$p^2 = (a - ib)(a + ib)\gamma\overline{\gamma} = (a^2 + b^2)|\gamma|^2$$

where both $a^2 + b^2$ and $|\gamma|^2$ are greater than 1. But the only such factorization of p^2 is pp, hence $p = a^2 + b^2$.

[Also, this implies that $\gamma = a - ib$, so we have shown that every integral odd prime p is either a Gaussian prime or the product of two conjugate Gaussian primes]

We have proven that p is the sum of two squares, completing the proof of the theorem. □

Corollary 6.3.3. *A positive integer n can be written as a sum of two squares if and only if n has a prime factorization $n = p_1^{e_1} \dots p_n^{e_n}$ (p_i distinct) where e_i is even whenever $p_i \equiv 2$ or $3 \pmod 4$.*

Proof. We may assume that n is non-prime. To prove the corollary, we first claim that if two numbers are each individually a sum of squares, then their product is a sum of squares, as well. By induction, this result holds for any finite number of multiplicands.

Proof of claim:

$$\begin{aligned}&(x_1^2 + y_1^2)(x_2^2 + y_2^2)\\ &= ((x_1x_2)^2 + x_1y_1^2 + y_1x_2^2 + (y_1y_2)^2) + 2x_1x_2y_1y_2 - 2x_1x_2y_1y_2\\ &= (x_1x_2 - y_1y_2)^2 + (x_1y_1 + y_1x_2)^2\end{aligned}$$

Now, assume (without loss of generality) that for $1 \le i \le r$, $p_1 \equiv 2, 3 \pmod 4$, and for $r \le in$, $p_i \equiv 1 \pmod 4$. Then, using Fermat's two square theorem and the previous claim, we may write $p_{r+1} \dots p_n = x^2 + y^2$, and so

$$n = p_1^{e_1} \dots p_r^{e_r}(x^2 + y^2)$$

Now, it is clear that if each of the e_i for $1 \le i \le r$ is even, then $p_1^{e_1} \dots p_r^{e_r}$ is a square, and thus n is a sum of squares, as required. Conversely, if we know that n is a sum of squares, say $n = X^2 + Y^2 = (X + iY)(X - iY)$, write

$$(X + iY)(X - iY) = p_1^{e_1} \dots p_r^{e_r}(x + iy)(x - iy)$$

Case-1: $(x + iy)$ (and thus also $(x - iy)$) is prime. Since it divides the product $(X + iY)(X - iY)$, it must divide one of the two factors, say $(X + iY)$ (without loss of generality). Then, $x - iy$ divides $X - iY$, but taking conjugates shows that $\frac{X+iY}{x+iy} = \frac{X-iY}{x-iy}$, and thus $p_1^{e_1} \dots p_r^{e_r}$ is a square and the corresponding e_i's must be even.

Case-2: $(x + iy)$ is not prime, and thus neither is $(x - iy)$). Then, each of these is the product of the same (seen by taking conjugates) conjugate Gaussian primes. Thus, $(x + iy)(x - iy)$ is a square. Similarly, $(X + iY)(X - iY)$ is a square, as well. Thus, $p_1^{e_1} \dots p_r^{e_r}$ is a square and so each of the e_i's is even.

□

Chapter 7

Factorization of the Class Number

7.1 Class numbers of fields with discriminant having only two odd prime factors

This section states and proves results that are found in [9] and [10].

Theorem 7.1.1. *Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field whose discriminant is divided by at least two distinct primes. Then, the class number of K is even.*

Proof. Pick a prime p that divides d. We know that this condition is equivalent to p being a ramified prime. So, $p\mathcal{O}_K = P^2$ for some prime ideal P of the ring of integers $\mathcal{O}_K$ of K.

Claim: P cannot be a principal ideal.

Proof of claim: If, to the contrary, P is a principal ideal, $p\mathcal{O}_K = (a + b\sqrt{d})$ if $d \equiv 2, 3 \pmod 4$ and $p\mathcal{O}_K = \frac{1}{2}(a + b\sqrt{d})$ if $d \equiv 1 \pmod 4$. Here a and b are integers. So, $p = (a + b\sqrt{d})^2$ or $p = (\frac{1}{2}(a + b\sqrt{d}))^2$. Thus, $p = a^2 + b^2d + 2ab\sqrt{d}$ or $4p = a^2 + b^2d + 2ab\sqrt{d}$. In either case, we must have $a = 0$ or $b = 0$. We must have, respectively, $p = a^2$ or $p = b^2d$, which is not possible, because p is prime, or $4p = a^2$ or $4p = b^2d$, both of which are, again, impossible by similar arguments.

Thus, the class of P is a non-trivial element of the ideal class group. Since $P^2 = p\mathcal{O}_K$, (the class of) P has order 2. By Lagrange's theorem, 2 divides the order of the ideal class group (i.e. the class number), and the proof is complete. □

We now consider imaginary quadratic fields whose discriminant has only two odd prime factors.

Theorem 7.1.2 (Byeon & Lee, [9])**.** *Let $g \geq 2$. Then, there exist infinitely many imaginary quadratic fields whose ideal class group has an element of order $2g$ and whose discriminant has only two prime factors.*

This theorem is proved by showing the existence of infinitely many fields of the form $\mathbf{Q}(\sqrt{n^2 - m^{2g}})$ and $\mathbf{Q}(\sqrt{n^2 - 4m^{2g}})$ whose class number is divisible by n and whose discriminant has only two prime factors. The construction of fields of the form

$\mathbf{Q}(\sqrt{n^2 - m^{2g}})$, in which case the odd prime divisors of d lie in different congruence classes modulo 4, was carried out by Byeon and Lee [9], while Akiko Ito [10] proved the theorem for fields of the form $\mathbf{Q}(\sqrt{n^2 - 4m^{2g}})$, in which case the odd prime divisors of d lie in the same congruence class modulo 4.

Theorem 7.1.3 (Bruden, Kawada, and Wooley, [11]). *Let $\phi(x) \in \mathbf{Z}[x]$ be a polynomial of degree k with positive leading coefficient. Let $S_k(N, \phi)$ denote the number of positive integers n, $1 \leq n \leq N$ for which the equation $2\phi(n) = p + q$ has no solution in primes p and q. Then, there exists an absolute constant $c > 0$ such that $S_k(N, \phi) <<_\phi N^{1-\frac{c}{k}}$ where the last equation means that there exists a constant $c^{'}$ that depends on ϕ and satisfies $S_k(N, \phi) < c^{'} N^{1-\frac{c}{k}}$ for large enough N.*

We now use this theorem first to prove the theorem 7.1.2.

Lemma 7.1.1. *Let $g \geq 2$ and let*

$$\phi(x) = 2(8x + 1)^g \in \mathbf{Z}[x]$$

By the lemma, there exist infinitely many positive integers $m^{'}$ for which the equation

$$2\phi(m^{'}) = 4(8m^{'} + 1)^g = p + q$$

has a solution in odd primes p and q.

Proof. Assume that only finitely many such $m^{'}$ exist. Let $m^{'}$ denote the largest integer for which there exist odd p and q with $2\phi(m^{'} = p + q$. Then, for any $N > m^{'}$,

$$S_k(N, \phi) \geq N - m^{'}$$

But, the lemma implies that $S_k(N, \phi) < c^{'} N^{1-\frac{c}{g}}$, $c > 0$, $g \geq 1$. So, $N - m^{'} < c^{'} N^{1-\frac{c}{g}} \forall\ N > m^{'}$. But, this is a contradiction because the function $N(1 - c^{'} N^{-\frac{c}{g}})$ is strictly increasing and unbounded, as $c, g > 0$, $g \geq 1$]

Thus, the equation 1 has a solution in odd primes p, q for infinitely many $m^{'}$. The congruence $p + q \equiv 4 \pmod 8$ gives the following possibilities:

1. $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$
2. $p \equiv 3 \pmod 8$, $q \equiv 1 \pmod 8$
3. $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$
4. $p \equiv 7 \pmod 8$, $q \equiv 5 \pmod 8$

For $m^{'}$, p, q satisfying equation 1, let $m = 8m^{'} + 1$, $n = \frac{p-q}{2} > 0$. There exist infinitely many distinct positive square-free integers

$$d = 4m^{2g} - n^2 = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2 = pq$$

Consider the ideal factorization in $\mathbf{Q}(\sqrt{-d})$:

$$(4m^{2g}) = (n^2 + d) = (n + \sqrt{-d})(n - \sqrt{-d})$$

$d = 4m^{2g} - n^2 = pq$

(1) to (4) $\Rightarrow pq \equiv 3 \pmod 8 \Rightarrow -d \equiv 5 \pmod 8$ and $n = \frac{p-q}{2}$ is odd.

So, $\frac{n \pm \sqrt{-d}}{2}$ is an algebraic integer ($-d \equiv 1 \pmod 4$). So, we can also consider the ideal factorization in $\mathbf{Q}(\sqrt{-d})$

$$(m)^{2g} = (\frac{n + \sqrt{-d}}{2})(\frac{n - \sqrt{-d}}{2})$$

Claim: $(\frac{n+\sqrt{-d}}{2})$ and $(\frac{n-\sqrt{-d}}{2})$ are coprime ideals.

Proof of claim. If (α) is a common factor, α divides m^{2g} and $\frac{n+\sqrt{-d}}{2} + \frac{n-\sqrt{-d}}{2} = n$. So, α divides $\gcd(m^{2g}, n)$. But, this gcd has to be 1, otherwise $d = 4m^{2g} - n^2$ is not square-free. So, $\alpha = 1$, i.e. there are no common factors. □

Therefore, each of $\frac{n \pm \sqrt{-d}}{2}$ is a $2g$-th power, say

$$\beta^{2g} = \frac{n + \sqrt{-d}}{2}$$

Suppose that the ideal β has order $r < 2g$. Then, $r \mid 2g$ and so $r \leq g$.

$$\begin{aligned} \beta^r &= (\frac{n + \sqrt{-d}}{2})^r \\ &= \frac{u + v\sqrt{-d}}{2} \end{aligned}$$

, $u, v \in \mathbf{Z}^*$. Taking norms,

$$\begin{aligned} \frac{u^2 + dv^2}{4} &= \frac{(n^2 + d)^r}{2^r} \\ &= \frac{(4m^{2g})^r}{4^r} \\ &= (8m^{'} + 1)^{2g} \equiv 1 \pmod 4 \end{aligned}$$

, $\frac{u^2+dv^2}{4} \in \mathbf{Z}$. We have

$$u^2 + dv^2 \equiv u^2 + 3v^2 \equiv 0 \pmod 4$$

So, $u \equiv v \pmod 2$. We also have

$$\frac{n \pm \sqrt{-d}}{2} = (\frac{u + v\sqrt{-d}}{2})^{\frac{2g}{r}},\ g \geq r$$

Taking norms on both sides of $\beta^{2g} = \frac{n+\sqrt{-d}}{2}$, we get

$$\begin{aligned} m^{2g} &= \frac{n^2 + d}{4} \\ &= N(\beta^r)^{\frac{2g}{r}} \\ &= (\frac{u^2 + v^2 d}{4})^{\frac{2g}{r}} \\ &\geq (\frac{1 + d}{4})^2 \end{aligned}$$

i.e. $16m^{2g} \geq (1+d)^2 \Leftrightarrow 4m^g - 1 \geq d$.

But, $d = 4m^{2g} - n^2$.

Thus,

$$4m^g - 1 \geq (2m^g - n)(2m^g + n)$$

If $2m^g - n > 1$, then $2m^g + n \leq \frac{d}{2}$, so $4m^g + 2n \leq d$. But, $4m^g - 1 \geq d$, a contradiction.

If $2m^g - n = 1$, this implies that $2m^g - n = \frac{p+q}{2} - \frac{p-q}{2} = q \neq 1$. Therefore, $r < 2g$ is not possible, and the order of β is exactly $2g$. □

Therefore, we have constructed an infinite family of quadratic fields $\mathbf{Q}(\sqrt{n^2 - 4m^{2g}})$, $(m,n) = 1$, $4m^{2g} > n^2$ whose class numbers are divisible by $2g$ where g is any integer. In this process, we have also proven the following theorem.

Theorem 7.1.4. *For an integer $g > 1$, $\#\{(p,q)|\ p,q$ odd primes, $p \neq q \pmod 4$, $2g|h(-pq)\} = \infty$.*

We now turn focus to the case $p \equiv q \pmod 4$. A proof similar to the above may be outlined to prove an analogous result for this case, as well. In particular, we have the following result.

Theorem 7.1.5 (Ito, 2012 [10])**.** *Let $g > 1$. Then,*
$\#\{(p,q)|\ p,q$ *odd primes,* $p \equiv q \pmod 4$, $2g \mid h(-pq)\} = \infty$.

Proof. This theorem is proved by showing the existence of infinitely many imaginary quadratic fields $\mathbf{Q}(\sqrt{\mathbf{n^2 - m^{2g}}})$, $n^2 - m^{2g} = -pq$, $p \equiv q \pmod 4$, $(m,n) = 1$, $m^{2g} > n^2$. This implies $m^{2g} - n^2 = pq \equiv 1 \pmod 4$, $p \equiv q \pmod 4$.

The theorem of Bruden, Kawada, and Wooley [11] is used again.

Let $n > 1$ and let

$$\phi(x) := (4x+1)^n \in \mathbf{Z}[x]$$

We know that there exist infinitely many positive m' for which $2\phi(m') := 2(4m'+1)^n \equiv 2 \pmod 4$. Thus, p and q satisfy one of:

- $p \equiv q \equiv 1 \pmod 4$
- $p \equiv q \equiv 3 \pmod 4$

Without loss of generality, assume that $p > q$. For m', p, q satisfying equation 1, put $m = 4m' + 1$ and $n = \frac{p-q}{2}$. Here, n is even because $p \equiv q \pmod 4$.

$$m^{2g} - n^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = pq$$

So, there exist infinitely many distinct positive square-free integers $d = m^{2n} - n^2$ with only two odd prime divisors. m is odd and greater than 1, and n is an even integer, $pq \equiv 1 \pmod 4$, so $-d = -pq \equiv 3 \pmod 4$. So, $\mathcal{O}_{\mathbf{Q}(\sqrt{-pq})} = \mathbf{Z}[\sqrt{-pq}]$. We can write

$$(m^{2g}) = (n^2 + pq)) = (n + \sqrt{-pq})(n - \sqrt{-pq})$$

in $\mathbf{Q}(\sqrt{-pq})$. As before, $(n+\sqrt{-pq})$ and $(n-\sqrt{-pq})$ have no common factors, because if they did, such a factor would divide m^{2g}, which is odd, as well as $2n$, and thus would divide the g.c.d. of n and m^{2g}, but this would imply that $d = n^2 - m^{2g}$ is not square-free. So, the ideals have to be co-prime. Thus, $(n+\sqrt{-pq}) = \beta^{2g}$ for some ideal β of $\mathcal{O}_{\mathbf{Q}(\sqrt{-pq})}$.

Suppose that the order of β in the ideal class group is $r < 2g$. Then, $r \mid 2g$, so $r \leq g$. Since $\mathcal{O}_{\mathbf{Q}(\sqrt{-pq})} = \mathbf{Z}[\sqrt{-pq}]$, we have

$$\beta^r = (u + v\sqrt{-pq}),\ u, v \in \mathbf{Z}$$

$$(n+\sqrt{-pq}) = \beta^{2g} = (\beta^r)^{\frac{2g}{r}} = (u+v\sqrt{-pq})^{\frac{2g}{r}}$$

Now, if $u = 0$ or $v = 0$, the above equation doesn't hold, since $n \neq 0$. Moreover, since $\mathbf{Q}(\sqrt{-pq}) \neq \mathbf{Q}(\sqrt{-1}),\ \mathbf{Q}(\sqrt{-3}$, the group of units of $\mathbf{Q}(\sqrt{-pq})$ is $\{\pm 1\}$. Then,

$$n + \sqrt{-pq} = \pm(u+v\sqrt{-pq})^{\frac{2g}{r}}$$

Taking norms on both sides,

$$\begin{aligned} m^{2g} &= n^2 + pq \\ &= N((n+\sqrt{-pq})) \\ &= N(\beta^r)^{\frac{2g}{r}} \\ &= N(u+v\sqrt{-pq})^{\frac{2g}{r}} \\ &= (u^2+v^2pq)^{\frac{2g}{r}} \end{aligned}$$

Since $u^2 \geq 1$, $v^2 \geq 1$, $g/r \geq 1$ hold,

$$\begin{aligned} & m^{2g} = (u^2+v^2pq)^{\frac{2g}{r}} \geq (1+pq)^2 \\ & \Leftrightarrow m^g - 1 \geq pq \end{aligned}$$

But, $m^{2g} - n^2 = pq \Rightarrow (m^g - n)(m^g + n) = pq$.

We have

$$m^g + n = \frac{p+q}{2} + \frac{p-q}{2} = p > 1$$

So, $m^g + n = p$, $m^g - n = q$, but $m^g + n > m^g - 1 \geq pq$, a contradiction. Therefore, the order of β must be equal to $2g$, and the proof of the theorem is complete. □

7.2 The Hilbert Class Field: A Brief Introduction

Definition 7.2.1 (Unramified Field Extension)**.** A field extension $K \subseteq L$ is called unramified if every prime ideal P of $\mathcal{O}_K$ is unramified in $\mathcal{O}_L$.

Definition 7.2.2 (Minkowski's Bound)**.** Let D be the discriminant of a field K, n be the degree of K over $\mathbf{Q}$, and $2r_2 = n - r_1$, $2r_2 = n - r_1$ be the number of complex embeddings where r_1 is the number of real embeddings. Then, by Minkowski's theorem, every class in the ideal class group of K contains an integral ideal of norm not exceeding Minkowski's bound.

Minkowski's constant/bound for the field K is this bound M_K.

We have

$$M_K = \sqrt{|D|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$$

Minkowski's bound implies that there exists a lower bound for the discriminant of a field K given n, r_1 and r_2.

$$\sqrt{|D|} \geq \left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{n/2}\frac{n^n}{n!}$$

For n at least 2, it is easy to show that the lower bound is greater than 1, so we obtain the fact that the discriminant of every number field, other than $\mathbf{Q}$, is non-trivial.

Theorem 7.2.1. *The field of rational numbers has no unramified finite extension.*

Proof. From the above result, no finite extension of $\mathbf{Q}$ has discriminant equal to ± 1, and thus every number field's discriminant is divided by some prime. We know that any prime dividing the discriminant of a number field ramifies in it. Thus, such an extension cannot be unramified. □

On the other hand, fields larger than $\mathbf{Q}$ may have unramified extensions.

Definition 7.2.3 (Relative Discriminant)**.** Let K be a number field and L be a finite extension of K. The relative discriminant $\Delta_{L/K}$ is an ideal of $\mathcal{O}_L$. Let $\{\sigma_i\}$ be the embeddings of K into $\mathbf{C}$ and $\{b_i\}$ be an integral basis of $\mathcal{O}_K$. When $\mathcal{O}_K = \mathbf{Z}[\alpha]$, the discriminant of K is equal to the discriminant of the minimal polynomial of α ($b_i = \alpha^{i-1}$) and the matrix is the Vandermonde matrix associated to $\alpha_i = \sigma_i(\alpha)$ whose determinant is $\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2$), which is also equal to the discriminant of the minimal polynomial of α.

In a tower of fields $L \supseteq K \supseteq F$,

$$\Delta_{L/F} = N_{K/F}(\Delta_{L/K}\Delta_{K/F}^{[L:K]})$$

where N denotes the relative ideal norm, i.e.

$$N_{L/K}(\alpha) = (\prod_{j=1}^{n}\sigma_j(\alpha))^{[L:K(\alpha)]}$$

where $\sigma_j(\alpha)$ are the roots of the minimal polynomial of α over K in some extension field of L.

Theorem 7.2.2. *The extension L/K is ramified in exactly those prime ideals that divide the relative discriminant $\Delta_{L/K}$. Hence, the extension is unramified in all but finitely many prime ideals.*

Definition 7.2.4. The Hilbert class field E of a number field K is the maximal abelian unramified extension of K.

Its degree over K equals the class number of K.

The Galois group of E over K is canonically isomorphic to the ideal class group using the Frobenius elements for prime ideals in K.

If $\mathcal{O}_K$ is a UFD, in particular if $K = \mathbf{Q}$, then $K = E$.

Example. Consider $K = \mathbf{Q}(\sqrt{-15})$ with discriminant -15, and let $L = \mathbf{Q}(\sqrt{-3}, \sqrt{-5})$ with discriminant $225 = -15^2$. L is an everywhere unramified extension of K, since the relative discriminant Δ_L/K equals the unit principal ideal $\mathcal{O}_K$:

$$\begin{aligned}
&\Delta_{L/\mathbf{Q}} = N_{K/\mathbf{Q}}(\Delta_{L/K})\Delta_{K/\mathbf{Q}}^{[L:K]} \\
&\Rightarrow -15^2 = N_{K/\mathbf{Q}}(\Delta_{L/K})(-15^2) \\
&\Rightarrow N_{K/\mathbf{Q}}(\Delta_{L/K}) = 1 \\
&\Rightarrow \Delta_{L/K} = (1) = \mathcal{O}_K
\end{aligned}$$

Thus, L is an everywhere unramified abelian extension of K. The computations using binary quadratic forms as described in a previous section show that K has class number 2. Thus, L is the Hilbert class field, since the $Gal(L/K)$ has order 2.

7.2.1 Properties of the Hilbert Class Field

1. E is a finite Galois extension of K with $[E : K] = h_K$, the class number of K
2. The ideal class group of K is isomorphic to the Galois grop of E/K.
3. Every ideal of $\mathcal{O}_K$ is a principal ideal of the ring extension $\mathcal{O}_E$
4. Every prime ideal P of $\mathcal{O}_K$ decomposes into the product of $\frac{h_K}{f}$ prime ideals in $\mathcal{O}_E$, where f is the order of $[P]$ in the ideal class group of $\mathcal{O}_K$.

In fact, E is the unique field satisfying 1, 2, and 4.

7.3 Unramified Extensions of Quadratic Number Fields

This section is based mainly on two papers by Koji Uchida, [12], and [15].

Theorem 7.3.1 (Hensel's Lemma)**.** *Assume K is a field complete with respect to a normalised discrete valuation ν. Suppose, furthermore, that $\mathcal{O}_K$ is the ring of integers of K (i.e. all elements of K with non-negative valuation), let $\pi \in K$ be such that $\nu(\pi) = 1$ and let $k = \mathcal{O}_K/\pi$ denote the residue field. Let $f(X) \in \mathcal{O}_K[X]$ be a polynomial with coefficients in $\mathcal{O}_K$. If the reduction $\overline{f}(X) \in k[X]$ has a simple root (i.e. there exists $x_0 \in k$ such that $\overline{f}(x_0) = 0$ and $\overline{f'}(x_0) \neq 0$, then there exists a unique $a \in \mathcal{O}_K$ such that $f(a) = 0$ and the reduction $\overline{a}$ equals x_0 in k.*

Theorem 7.3.2 (Uchida, 1969 [12]). *Let K be an algebraic number field of finite degree. Let a and b be integers of K, i.e. $a, b \in \mathcal{O}_K$. Let L denote the minimal splitting field of a polynomial*

$$f(X) = X^n - aX + b$$

i.e., $L = K(\alpha_1, \ldots \alpha_n)$, where α_1, ..., α_n are the roots of $f(X) = 0$. Let

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

be the discriminant of $f(X)$. If $(n1)a$ and nb are relatively prime, L is unramified over $K(\sqrt{D})$.

Proof. Let β be any finite prime of L, and let $P = \beta \cap K$. Let G be the Galois group of L over K. Then, G is a permutation group of $\{\alpha_1, \ldots, \alpha_n\}$. Let H be the subgroup of G consisting of the even permutations. H corresponds to the fixed field $K(\sqrt{D})$. We show that H meets the inertia group of β trivially. First we consider the factorization of $f(X) \pmod p$. From $f(X) = X^n - aX + b$ and $f'(X) = nX^{n-1} - a$, it follows that

$$Xf'(X) - nf(X) = (n-1)aX - nb$$

As $((n-l)a, nb) = 1$, the above expression does not vanish $\pmod p$. So $(nl)aX - nb$ is divisible by the gcd of $f(X)$ and $f'(X) \pmod p$. If $f(X)$ and $f'(X) \pmod p$, it must equal to the gcd since it is of degree one. Therefore $f(X)$ is factorized as

$$f(X) \equiv \overline{f_1(X)} \ldots \overline{f_r(X)} \pmod p$$

if f has only simple roots $\pmod p$ and

$$f(X) \equiv ((n-1)aX - nb)^2 \overline{g_2(X)} \ldots \overline{g_s(X)} \pmod p$$

if $f(X)$ has non-simple roots $\pmod p$.

In the above each $f_r(X)$ is irreducible $\pmod p$ and $\overline{f_i(X)} \neq \overline{f_j(X)})$ for $i \neq j$. Each $\overline{g_j(X)}$, $2 \leq j \leq s$ is irreducible and $\overline{g_i(X)} \neq \overline{g_j(X)})$ for $i \neq j$, and also $g_i(X) \neq (n-1)aX - nb \pmod p, \forall\, i$.

By Hensel's lemma, $f(X)$ is factorized in the in the completion of K with respect to the norm given rise to by prime ideal P, the local field k_P in the form

$$f(X) \equiv f_1(X) \ldots f_r(X)$$

or

$$f(X) \equiv \ g_1(X) \ldots g_s(X)$$

as according to whether f has only simple roots or not, respectively.

Here, $f_i(X) = \overline{f_i}(X) \pmod p$, $g_j(X) = \overline{g_i}(X) \pmod p$ for $i \geq 2$ and $g_1(X) \equiv (n-1)aX - nb \pmod p$.

L_β is obtained from K_P, by adjoining the roots of $f(X) = 0$. The roots of $f_i(X)$ or $g_j(X)$, $j \geq 2$, generate unramified extensions of K. So, if f has only simple

roots, K_β is unramified over k_P. If $f(X)$ has non-simple roots $\pmod p$ and if L_β is ramified over K_P, $g_i(X)$ is irreducible of degree 2 and the inertia group is generated by the transposition of the roots of $g_1(X) = 0$. So it meets with H trivially (since H contains only even permutations), and thus β is unramified over K (H is the Galois group of the extension $L/K(\sqrt{D})$, and the order of the inertial group is e, the ramification index). As β was arbitrary, L is unramified over $K(\sqrt{D})$. □

Theorem 7.3.3 (Uchida, 1969 [12])**.** *Let K be an algebraic number field of finite degree. Let a and b be integers of K, i.e. $a, b \in \mathcal{O}_K$. Let L denote the minimal splitting field of a polynomial*

$$f(X) = X^n - aX + b$$

i.e., $L = K(\alpha_1, \ldots \alpha_n)$, where α_1, …, α_n are the roots of $f(X) = 0$. If $(n-1)a$ and nb are relatively prime, any prime ideal of L has the ramification index 1 or 2 over K.

Proof. We have seen from the previous theorem that any prime of L is unramified over $K(\sqrt{D})$, where D is the discriminant of f. We know that ramification indices are multiplicative over field extensions. Since the ramification index of a prime in $K(\sqrt{D})$ over K can be either 1 or 2 (from the efg formula), the result follows. □

Corollary 7.3.1. *Let $K = \mathbf{Q}$ be the field of rational numbers. Let $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$ be the discriminant of $f(X) = 0$. Assume that any prime number that appears in the factorization of D, appears odd number of times. Then, $L = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ is unramified over $\mathbf{Q}(\sqrt{D})$.*

Proof. Every prime number that is ramified in $L/\mathbf{Q}$ appears in D. By assumption, it is ramified in $\mathbf{Q}(\sqrt{D})/\mathbf{Q}$, since it appears odd number of times in D. Thus, by the multiplicative property of ramification indices, such a prime is unramified in $L/\mathbf{Q}(\sqrt{D})$, as required. □

Lemma 7.3.1 ([13], Theorem 13.3)**.** *If a primitive permutation group contains a transposition, it is a symmetric group.*

Proposition 7.3.1. *If $n = l$ is a prime and if $f(X)$ is irreducible over $\mathbf{Q}$ with discriminant D and splitting field K, the Galois group of K over $\mathbf{Q}$ is a symmetric group S_l. Therefore, K is an unramified extension of $\mathbf{Q}(\sqrt{D})$ with Galois group A_l.*

Proof. As we have seen in the proof of Theorem 7.1.4, the inertia group of a prime β contains a transposition if β is ramified. As the field $\mathbf{Q}$ has no unramified extension, there exist primes of K ramified over $\mathbf{Q}$. Therefore, the Galois group of K over $\mathbf{Q}$ contains a transposition. As any transitive group of prime degree is primitive [[13], Theorem 8.3], so the Galois group of K over $\mathbf{Q}$ is primitive, and by lemma 7.1.1, it is a symmetric group. □

Proposition 7.3.2. *Let $P(x)$ be a polynomial in $k[x]$ for a field k. The equation $P(x) = 0$ has a root α generating a degree d extension K of k if and only if $P(x)$ has a degree d irreducible factor $f(x)$ in $k[x]$.*

Proof. Let α be a root of $P(x) = 0$ generating a degree d extension $k(\alpha) = k[\alpha]$ over k. Let $M(x)$ be the minimal polynomial for α over k. Let

$$P = Q \cdot M + R$$

in $k[x]$ with $\deg R < \deg M$. Then, evaluating these polynomials at α, $R(\alpha) = 0$, but the minimality of the degree of M with this property assures that $R = 0$. That is, M divides P. On the other hand, for an irreducible (monic, without loss of generality) $M(x)$ dividing $P(x)$, the quotient $K = \frac{k[x]}{<M(x)>}$ is a field containing (a canonical copy of) k, and the image α of x in that extension is a root of $M(x) = 0$. Letting $P = Q \cdot M$, $P() = Q() \cdot M(\alpha) = Q(\alpha) \cdot 0 = 0$, showing that $P(x) = 0$ has root α. □

Theorem 7.3.4 (Uchida, 1969 [12])**.** *The polynomials $f(X) = X^n - X + 1$ for $n = 5, 6, 7$ ($a = b = 1$) satisfy the condition of Corollary 7.1.1. The Galois groups of $f(X) = 0$ are symmetric groups. Thus, there exists an unramified extension of the quadratic field $\mathbf{Q}(\sqrt{D})$ with the alternating groups A_5, A_6, A_7 or symmetric groups S_5, S_6, S_7 as Galois groups.*

Proof. First consider the general case $f(X) = X^n - aX + b$. Then, the discriminant D of f may be expressed in terms of its roots α_i as before. The product of all the α_i's is equal to b.

1. $D = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\alpha_i)$ and

$$\begin{aligned}\prod_i f' &= \prod_i (n\alpha_i^{n-1} - a) \\ &= \prod_i \frac{n\alpha_i^n - a\alpha_i}{\prod_i \alpha_i} \\ &= \prod_i n\frac{(a\alpha_i - b) - a\alpha_i}{\prod_i \alpha_i} \\ &= \frac{\prod_{i=1}^n ((n-1)a\alpha_i - nb)}{\prod_i \alpha_i} \\ &= n^n b^{n-1} - (n-1)^{n-1}a^n\end{aligned}$$

   Let D_5, D_6, D_7 be the discriminants corresponding to n = 5, 6, 7. Here, we have a = 1 = b. So,

$$D_5 = 5^5 - 4^4 = 19 \times 151$$

$$D_6 = 5^5 - 6^6 = -101 \times 431$$

$$D_7 = 6^6 - 7^7 = -776887, \textit{ a prime}$$

   So, for n = 5, 6, and 7, any prime appearing in the factorization of the discriminant D_n of the polynomial $f(X) = X^n - aX + b$, appears odd number of times. Thus, by Corollary 7.1.1, $L = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ is unramified over $\mathbf{Q}(\sqrt{D})$.

2. Now, we find the Galois groups of these equations. If n = 5, f is irreducible modulo 5. (Since $\frac{\mathbf{Z}}{5\mathbf{Z}}$ is cyclic of order 5, there are no roots. It can be checked manually that there are not quadratic irreducible factors.) If n = 7, f is irreducible modulo 7. (Since $\frac{\mathbf{Z}}{7\mathbf{Z}}$ is cyclic of order 7, there are no roots. It can be checked manually that there are not quadratic and cubic irreducible factors.)

   Thus, using the following lemma, f is irreducible over $\mathbf{Z}$ for n = 5, 7.

   Lemma 7.3.2. *If $f(T) \in \mathbf{Z}[T]$ is monic and there is a prime p such that $f(T)$ is irreducible in $\frac{\mathbf{Z}}{pZ}[T]$ then $f(T)$ is irreducible in $\mathbf{Q}[T]$.*

   If n = 6, f is irreducible mod 2.

   Now, when n is a prime number, a transitive permutation group of n letters is a symmetric group if it contains a transposition. We have

$$x^5 \equiv (X^2 - X + 1)(X^3 + x^2 + 1) \pmod 2$$

$$X^7 - X + 1 \equiv (X^2 - X + 1)(X^5 + X^4 - X^3 - X + 1) \pmod 3$$

   Since quadratic polynomials occur in the factorizations, the Galois groups contain transpositions (and are n-transitive). Thus, they are symmetric groups. We are left with the case n = 6. We have

$$X^6 - X + 1 \equiv (X + 1)(X^2 + X - 1)(X^3 + X^2 + X - 1) \pmod 3$$

$$X^6 - X + 1 \equiv (X - 2)(X^5 + 2X^4 - 3X^3 + X^2 + 2X + 3) \pmod 7$$

   Now, $X^5 + 2x^4 - 3X^3 + X^2 + 2X + 3$ is irreducible modulo 7. To see this, we use Proposition 7.1.2.

   If $X^5+2x^4-3X^3+X^2+2X+3$ was reducible modulo 7, it would have a root in $\frac{\mathbf{Z}}{7\mathbf{Z}}$ (for a linear factor) or in a quadratic extension field of $\frac{\mathbf{Z}}{7\mathbf{Z}}$ (for a quadratic factor). In either case, this factor would divide both X^6-X+1 and $X^{49}-X$. But, these polynomials have no common factors except $X-2$, which does not divide $X^5+2x^4-3X^3+X^2+2X+3$ modulo 7. So, $X^5+2x^4-3X^3+X^2+2X+3$ is irreducible, and the Galois group is a symmetric group by a result in [14], cited in [12].

3. We have shown that $L = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ is an unramified extension of $\mathbf{Q}$ with Galois group S_n, for n = 5, 6, 7. Now, $L/Q(\sqrt{D})$ is an unramified field extension (because $Q(\sqrt{D})/\mathbf{Q}$ is ramified, and ramification indices are multiplicative) with Galois group of order $\frac{|S_n|}{2}$. But, the only permutation group with this order is A_n. Thus, L is an unramified extension of $Q(\sqrt{D})$ with Galois group A_n, n = 5, 6, 7.

   Let p be a prime number which does not appear in the factorization of D. Then, each $L(\sqrt{p})/Q(\sqrt{pD})$ is unramified and its Galois group is a symmetric group.

□

Theorem 7.3.5 (Uchida, 1969 [12]). *There exist infinitely many real quadratic field with class numbers divisible by 3.*

Proof. If a cubic irreducible equation $X^3 - aX + b = 0$ ($a,\ b \in \mathbf{Z}$) satisfies the condition of Theorem 7.1.5, and if K denotes its splitting field, the Galois group of $K/\mathbf{Q}$ is a symmetric group of three letters. Let $D = 4a^3 - 27b^2$ be the discriminant of the given equation. Then $K/\mathbf{Q}(\sqrt{D})$ is an unramified abelian extension. So, the degree of the extension $K/\mathbf{Q}(\sqrt{D})$ divides the degree of the Hilbert class field over $\mathbf{Q}(\sqrt{D})$. Now, the Hilbert class field over $\mathbf{Q}(\sqrt{D})$ has order is divisible by the order of the Galois group $K/\mathbf{Q}(\sqrt{D})$, which is 3 (by multiplicative property of degrees of field extensions). Since the class group is isomorphic to this Galois group (as discussed in section 2 of this chapter), the class number of $\mathbf{Q}(\sqrt{D})$ is divisible by 3.

Therefore, it is enough to prove there exist infinitely many different $Q(\sqrt{D})$ with positive D. If we assume that $a \geq 2$, $a \equiv 1 \pmod 3$, and $b = 1$, then $X^3 - aX + l$ is irreducible and satisfies the condition of Theorem 7.1.1 and has a positive discriminant $4a^3 - 27 = D > 0$. Then clearly, if $p \neq 2, 3$ is a prime number, p divides D for some a if and only if 4 is a cubic residue mod p. If $p = 2 \pmod 3$, any number is a cubic residue. So, there exists $a_1 > 2$ such that $p \mid 4a_1^3 - 27$. As the equation

$$a_1 + rp \equiv 1 \pmod 3$$

has an integral solution r, we may assume that $a_1 \equiv 1 \pmod 3$ If $4a_1^3 - 27$ is divisible by p^2, we replace a_1 by $a = a_1 + 3p$. Then, $4a^3 - 27$ is divisible by p but not by p^2. So, p is ramified in $\mathbf{Q}(\sqrt{D})/\mathbf{Q}$. As there exist infinitely many p satisfying the above condition ($p = 2 \pmod 3$), there exist infinitely many different $\mathbf{Q}(\sqrt{\mathbf{D}})$, with D positive and the discriminant of some irreducible monic cubic equation. □

Theorem 7.3.6 (Uchida, 1970 [15]). *Let $n \geq 3$ be an integer, and A_n be an alternating group of degree n. Then there exist infinitely many quadratic number fields which have unramified Galois extensions with Galois groups A_n.*

Proof. We find pairs of rational integers (a, b) such that $((n-1)a, nb) = 1$ and the equations $f(X) = X^n - aX + b = 0$ which have symmetric groups S_n as Galois groups. Now, we show that there exist pairs of integers (a, b) satisfying the conditions of Theorem 7.1.4. Let l be a prime number such that

$$l \equiv 1 \pmod{(n-1)}$$

holds. If b is divisible by 1, then

$$X^n - ax + b \equiv X(X^{n-1} - a) \pmod l$$

holds. As $\mathbf{Z}/l\mathbf{Z}$ contains all the $(n-1)$-st roots of unity, $X^{n-1} - a$ is irreducible mod 1 if a is a primitive root mod 1. Then, $X^n - aX + b$ has irreducible factors of degree 1 and degree $n - 1$, if it is reducible over $\mathbf{Q}$. But, it has no factor of degree 1 if a is sufficiently large. Then $X^n - aX + b$ is irreducible over $\mathbf{Q}$, and its Galois group is primitive by the factorization $X^n - ax + b \equiv X(X^{n-1} - a) \pmod l$. We can choose a and b as $((n-1)a, nb) = 1$. Then, all the conditions of Theorem 7.1.1 are satisfied.

Now let p be any prime number such that $(p, ln(n-1)) = 1$, where l is fixed as above. We show that there exists a pair (a, b) such that $D = D(a, b) = pD_0$, $(p, D_0) = 1$ and that satisfies the above conditions. Then we have infinitely many different $Q(\sqrt{D})$. D is calculated as

$$\begin{aligned} D = \prod_{i<j}(\alpha_i - \alpha_j)^2 =& (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\alpha_i) \\ =& (-1)^{\frac{n(n-1)}{2}} \prod_i (n\alpha_i^{n-1} - a) \\ =& (-1)^{\frac{n(n-1)}{2}} \prod_i \frac{n\alpha_i^n - a\alpha_i}{\prod_i \alpha_i} \\ =& \prod_i n\frac{(a\alpha_i - b) - a\alpha_i}{\prod_i \alpha_i} \\ =& \frac{\prod_{i=1}^n ((n-1)a\alpha_i - nb)}{\prod_i \alpha_i} \\ =& n^n b^{n-1} - (n-1)^{n-1}a^n \end{aligned}$$

Let b be a multiple of l such that $b \equiv n-1 \pmod{p}$ and $(b, n-1) = 1$. As $(p, n) = 1$, we have a sufficiently large integer a_1 such that $a_l \equiv n \pmod{p}$, $(a_l, nb) = 1$ and a_1 is a primitive root mod 1. Then $D_1 = D(a_1, b)$ is divisible by p. If D_1 is divisible by p_2, we replace a_1 by

$$a = a_1 + nblp$$

Then $D = D(a, b)$ is divisible by p, but not divisible by p^2. This completes the proof. □

Corollary 7.3.2 (Uchida, 1969 [12]). *Let G be a finite group. Then, there exists an algebraic number field k which has an unramified extension with Galois group G. If G is of order N, k is taken as $[k : \mathbf{Q}] \leq 2(n-1)!$*

Proof. Let K be a Galois extension of $\mathbf{Q}$ with Galois group S_n, which is unramified over $\mathbf{Q}(\sqrt{D})$. Let q be a prime number such that $(q, D) = 1$. Then, $K(\sqrt{q})$ is unramified over $\mathbf{Q}(\sqrt{D})$ and its Galois group is a symmetric group S_n. So, G can be considered as a subgroup of S_n. If k denotes the subfield of $K(\sqrt{q})$ corresponding to G, k satisfies the conditions of this corollary, as required. □

Corollary 7.3.3 (Uchida, 1970 [15]). *Let F be an algebraic number field of finite degree. Let a and b be indeterminates. Then, the equation*

$$X^n - aX + b$$

has the Galois group S_n over $F(a, b)$.

Proof. We may assume that F is normal over $\mathbf{Q}$. Let (a_0, b_0) be a pair of rational integers such that the Galois group of $X^n - a_0X + b_0$ is a symmetric group S_n. Let $D_0 = D(a_0, b_0)$ be its discriminant. By the proof of Theorem 7.1.8, (a_0, b_0) can be chosen such that $\mathbf{Q}(\sqrt{D})$ is not included in F. Then, the Galois group of $X^n - aX + b$ over F is also S_n. So the Galois group of $X^n - aX + b$ over $F(a, b)$ is also S_n. □

Bibliography

[1] Ş. Alaca and K. S. Williams, *Introductory algebraic number theory*. Cambridge University Press Cambridge, 2004.

[2] W. Stein, "Introduction to algebraic number theory," *Unpublished manuscript*, 2005.

[3] T. W. Hungerford, *Algebra*. Springer-Verlag New York, 1974.

[4] C. Perret-Gentil, "The correspondence between binary quadratic forms and quadratic fields," Master's thesis, Ecole Polytechnique federale de Lausanne, Section de Mathematiques, 2012.

[5] B. J. Birch, "Heegner points: The beginnings," 2004.

[6] D. Shanks, "On gauss's class number problems," 2010.

[7] S. Lang, *Algebraic number theory*, vol. 110. Springer Science & Business Media, 2013.

[8] K. Conrad, "Galois theory at work: Concrete examples."

[9] D. Byeon and S. Lee, "Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors," *Proc. Japan Acad. Ser. A Math. Sci.*, vol. 84, pp. 8–10, 01 2008.

[10] A. ITO, "On the divisibility of class numbers of imaginary quadratic fields whose discriminant has only two odd prime factors (functions in number theory and their probabilistic aspects)," *RIMS Kokyuroku Bessatsu*, vol. B34, 8 2012.

[11] J. Brudern, K. Kawada, and T. D. Wooley, "Additive representation in thin sequences, vii: Restricted moments of the number of representations," *Tsukuba J. Math.*, vol. 32, pp. 383–406, 12 2008.

[12] K. Uchida, "Unramified extensions of quadratic number fields, i," *Tohoku Math. J. (2)*, vol. 22, no. 1, pp. 138–141, 1970.

[13] H. Wielandt, *Finite permutation groups*. Academic Press, 1964.

[14] O. Ore, "Review: B. l. van der waerden, moderne algebra," *Bull. Amer. Math. Soc.*, vol. 44, p. 320, 05 1938.

[15] K. Uchida, "Unramified extensions of quadratic number fields, ii," *Tohoku Math. J. (2)*, vol. 22, no. 2, pp. 220–224, 1970.

[16] Z. I. Borevich and I. R. Shafarevich, *Number theory / by Z. I. Borevich and I. R. Shafarevich. Translated by Newcomb Greenleaf for Scripta Technica, translators, New York*. Academic Press New York, 1966.

[17] N. C. Ankeny and S. Chowla, "On the divisibility of the class number of quadratic fields.," *Pacific J. Math.*, vol. 5, no. 3, pp. 321–324, 1955.

[18] F. Oggier, "Introduction to algebraic number theory."

[19] P. L. Clark, "8430 handout 5: Chebotarev density; global class field theory."

[20] J. Kaplan, "Binary quadratic forms, genus theory, and primes of the form $p = x^2 + ny^2$," 2014.

[21] K. Smith, "The collision of quadratic fields, binary quadratic forms, and modular forms," 2011.

[22] K. Conrad, "Galois groups as permutation groups."

[23] H. M. Stark, "A complete determination of the complex quadratic fields of class-number one.," *Michigan Math. J.*, vol. 14, pp. 1–27, 04 1967.

[24] R. L. Shepherd, *Binary quadratic forms and genus theory*. The University of North Carolina at Greensboro, 2013.

[25] L. Zeng, "A note on finitely generated z-module and algebraic integers," in *2015 International Conference on Education Reform and Modern Management*, Atlantis Press, 2015.

[26] B. Osserman, "Math 254a: Dedekind domains ii."

[27] B. Osserman, "Math 254a: The hilbert class field."

[28] S. Hussein, "Valuation theory."

[29] S. V. Neel, "Binary quadratic forms and the ideal class group," 2012.

[30] Y. Yamamoto, "On unramified galois extensions of quadratic number fields," *Osaka Journal of Mathematics*, vol. 7, no. 1, pp. 57–76, 1970.

[31] B. Sury, "Frobenius and his density theorem for primes," *Resonance*, vol. 8, no. 12, pp. 33–41, 2003.

[32] R. B. Ash, "A course in algebraic number theory."

[33] H. Cohn, *Advanced number theory*. Courier Corporation, 1962.

[34] C. Shantian, "Binary quadratic forms reduction theory and genus theory."

[35] K. Conrad, "Ideal factorization."

[36] C. S. Rajan, "An algebraic chebotarev density theorem."

[37] D. A. Cox, "Primes of the form x^ 2+ ny^ 2," 1997.

[38] P. Stevenhagen and H. W. Lenstra, "Chebotarëv and his density theorem," *The Mathematical Intelligencer*, vol. 18, no. 2, pp. 26–37, 1996.

[39] H. Lenstra, "The chebotarev density theorem," *URL: http://math. berkeley. edu/jvoight/notes/oberwolfach/Lenstra-Chebotarev. pdf*, 2006.

[40] L. Lingle, "Intro to class field theory and the chebotarev theorem," 2014.

[41] M. F. Lim, "On the divisibility of class numbers and discriminants of imaginary quadratic fields," *arXiv preprint arXiv:1601.05180*, 2016.

[42] A. Hoque and K. Chakraborty, "Divisibility of class numbers of certain families of quadratic fields," *arXiv preprint arXiv:1712.07338*, 2017.