Primes of the Form $x^2 + ny^2$

Steven Charlton

27 April 2012

Declaration

This piece of work is a result of my own work except where it forms an assessment based on group project work. In the case of a group project, the work has been prepared in collaboration with other members of the group. Material from the work of others not involved in the project has been acknowledged and quotations and paraphrases suitably indicated.

Abstract

In this report we investigate the theory necessary to determine which primes a binary quadratic form represents. We explore the theory of binary quadratic forms, and how questions about which integers they represent can be studied using quadratic fields and algebraic number theory. Using class field theory we find increasingly general abstract criteria that can determine whether or not a certain prime is represented by a given binary quadratic form. Applying Dedekind's Theorem we make these abstract criteria very concrete in a variety of examples.

Contents

Chapter 0

Introduction

In a letter to Marin Mersenne, dated December 25, 1640, Pierre de Fermat announced his theorem on when a prime is expressible as the sum of two squares. He claimed that for a prime p:

$$p = x^2 + y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1 \pmod 4$$

Fourteen years later, in a letter to Blaise Pascal, he added two similar results:

$$p = x^2 + 2y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1, 3 \pmod 8$$
$$p = x^2 + 3y^2 \Leftrightarrow p = 3, \text{ or } p \equiv 1 \pmod 3$$

Obtaining complete proofs for Fermat's claims required a full forty years of work and effort on Leonhard Euler's part, and led him to conjectures about the behaviour in other cases. These results naturally raise the question of what happens for x^2+ny^2, or more generally for an arbitrary binary quadratic form.

We introduce the notion of a binary quadratic form $ax^2 + bxy + cy^2$, and its discriminant $D = b^2 - 4ac$. This leads to an easy condition which determines whether a prime p is represented by *some* binary quadratic form of discriminant D:

Theorem 0.1. *An odd prime $p \nmid D$ is represented by some binary quadratic form of discriminant D if and only if $\left(\frac{D}{p}\right) = 1$.*

We define an equivalence relation on the set of all binary quadratic forms, such that equivalent forms represent the same integers and have the same discriminant. This causes the set of binary quadratic forms of discriminant D to break up into a finite number of equivalence classes. This class number and a representative of each equivalence class can be determined algorithmically using the theory of reduced forms.

When the class number is exactly 1, every form of discriminant D is equivalent, and so they all representative the same integers. The condition above is therefore sufficient to determine which primes a form of discriminant D represents. This leads immediately to proofs of Fermat's claims, and further extensions to other discriminants with class number 1.

When there is more than one class of forms of discriminant D, we need some way to separate them. The key idea here, due to Lagrange, is to look at the values each form represents in $(\mathbb{Z}/D\mathbb{Z})^*$. By grouping the forms which represent the same values together we are lead to the notion of a genus of quadratic forms.

The primes that a genus of forms represents can be described explicitly in terms of congruence conditions modulo D. This gives a condition for p to be represented by *some* form in a given genus:

Theorem 0.2. *Suppose a genus of quadratic forms of discriminant D represents the values H in $(\mathbb{Z}/D\mathbb{Z})^*$. Then an odd prime $p \nmid D$ is represented by a form of this genus if and only if $[p] \in H$.*

If there is exactly one form in a genus, then this condition describes precisely what primes it represents. From this we can generate further criteria in a variety of cases. If two forms are in the same genus, then they also represent the same values in $(\mathbb{Z}/m\mathbb{Z})^*$, for any m, and so cannot be separated by congruence conditions. Then there is more than one form in a genus, more advanced techniques are needed to generate criteria.

For this we approach the study of binary quadratic forms from an algebraic number theory point of view. For fundamental discriminants we establish the correspondence between quadratic forms and narrow ideal classes in a quadratic field. The correspondence extends to a relationship between the representations of an integer m by a binary quadratic form and the existence of ideals with norm m in the corresponding class of the class group:

Proposition 0.3. *A positive integer m is represented by the quadratic form $f(x, y)$ corresponding to the narrow ideal class of $\mathfrak{a}$ if and only if there is an integral ideal of norm m in the same narrow ideal class as $\mathfrak{a}$.*

The splitting of the prime (p) in $\mathbb{Q}(\sqrt{d})$ easily tells us whether or not there is an ideal of norm p in the quadratic field. The problem now is to determine which ideal class this ideal lies in, and so determine which form represents p. From class field theory we begin to answer this question in certain cases.

We introduce the Hilbert class field L of a number field K, which is defined as the maximal unramified abelian extension of K. The Artin map of the extension L/K gives a map from the group of fractional ideals $\mathcal{I}(K)$ of K to the Galois group $\mathrm{Gal}(L/K)$ of the extension L/K. The kernel of this map is the group of principal fractional ideals $\mathcal{P}(K)$, and so establishes an isomorphism from the class group $\mathcal{C}(K)$ of K to the Galois group $\mathrm{Gal}(L/K)$ of the extension L/K.

Properties of the Artin symbol used to define the Artin map then give a condition for a prime ideal $\mathfrak{p}$ of K to be principal:

Proposition 0.4. *A prime ideal $\mathfrak{p}$ of K is principal if and only if it splits completely in L, the Hilbert class field of K.*

When the narrow class group and the class group of a quadratic field $K = \mathbb{Q}(\sqrt{d})$ are isomorphic, we have a correspondence between quadratic forms and ideal classes in the class group $\mathcal{C}(K)$. This holds for all imaginary quadratic fields, and some real quadratic fields. As we have a way to tell when a prime ideal is principal, we use this to give an abstract condition for the quadratic form corresponding to the principal ideal class (either $x^2 - dy^2$ or $x^2 + xy + \frac{1-d}{4}y^2$ depending on the field) to represent a prime:

Theorem 0.5. *Suppose the narrow class group and the class group are isomorphic in the quadratic field $K = \mathbb{Q}(\sqrt{d})$, and let $q(x, y)$ be the quadratic form corresponding to the principal ideal class. Let L be the Hilbert class field of K. For a prime p not dividing the discriminant Δ_K, we have:*

$$p \text{ is represented by } q(x, y) \Leftrightarrow (p) \text{ splits completely in } L$$

By determining the polynomial which generates the Hilbert class field we can use Dedekind's Theorem on the factorisation of a prime ideal in an extension to make this into an explicit criterion:

Theorem 0.6. *Suppose the narrow class group and the class group of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ are isomorphic. Let $q(x, y)$ be the quadratic form corresponding to the principal ideal class*

in K. Then there is a polynomial $f(x)$ of degree $h(K) = h(\Delta_K)$ such that for p an odd prime not dividing Δ_K or the discriminant of $f(x)$, we have:

$$p \text{ is represented by } q(x,y) \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

This polynomial can be taken to be the minimal polynomial of the algebraic integer α for which $L = K(\alpha)$ is the Hilbert class field of K.

To generalise this to the remaining real quadratic fields we define the narrow class field. The narrow class field L of a number field K is the maximal abelian extension of K unramified at the finite primes. The Artin map of this extension gives an isomorphism from the narrow class group $\mathcal{C}^+(K)$ of K to the Galois group $\mathrm{Gal}(L/K)$ of the extension L/K.

Properties of the Artin symbol imply that a prime ideal $\mathfrak{p}$ of K is a totally positive principal fractional ideal if and only if it splits completely in the narrow class field L. With this we find a condition for a prime p to be represented by the form corresponding to the totally positive principal fractional ideal class:

Theorem 0.7. *Let $q(x,y)$ be the quadratic form corresponding to the totally positive principal ideal class in K. Then there is a polynomial $f(x)$ of degree $h^+(K) = h^+(\Delta_K)$ such that for p an odd prime not dividing Δ_K or the discriminant of $f(x)$, we have:*

$$p \text{ is represented by } q(x,y) \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

This polynomial can be taken to be the minimal polynomial of the algebraic integer α for which $L = K(\alpha)$ is the narrow class field of K.

By looking at class fields corresponding to subgroups of the class group or the narrow class group we generalise these results even further. For every subgroup H of the narrow class group there is a class field L which detects when the class of a prime ideal $\mathfrak{p}$ lies in this subgroup. This leads to criteria which determine when certain subsets of quadratic forms represent a given prime p:

Theorem 0.8. *Let the subset of forms $\{q_i(x,y)\}$ correspond to the subgroup H of the narrow class group of the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Then there is a polynomial $f(x)$ of degree $h^+(K)/|H| = h^+(\Delta_K)/|H|$ such that for p an odd prime not dividing Δ_K or the discriminant of $f(x)$, we have:*

$$p \text{ is represented by some } q_i(x,y) \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

This polynomial can be taken to be the minimal polynomial of the algebraic integer α for which $M = K(\alpha)$ is the fixed field L^H of the narrow class field, that is the class field corresponding to the subgroup H.

Using an inclusion-exclusion style principle we can sometimes extract from this result further criteria which determine when certain non-principal quadratic forms represent a given prime.

Part I

Quadratic Forms

Chapter 1

Number Fields and Galois Theory

In this chapter we review some of the essential concepts from number theory that will be used throughout this report. We also study the interaction between number theory and Galois theory, the effect this has on prime decomposition in an extension. Finally we introduce the narrow class group of a number field which will be used to link quadratic forms and quadratic fields.

The results on fields and Galois theory mainly come from Stewart [24]. For number fields and prime decomposition we will use Marcus [18] with interludes from Stewart and Tall [25]. The results we need on the narrow class group come from Cox [7].

1.1 Fields and Galois Theory

We will make frequent use of field extensions in the form of number fields and residue field extensions. The goal of Class Field theory is to classify all abelian extensions of a number field, and class fields will aid us when investigating which primes a binary quadratic form represents.

Definition 1.1. A field F is said to be an extension of the field E is E is a subfield of F. We speak of the extension F over E, and write this as F/E. We call E the base field.

We can view a field extension F of E as a vector space over E, as in Theorem 6.1 of Stewart [24, p. 67], and its later generalisation. This means that F has an E-basis, and a dimension as an E-vector space.

Definition 1.2. The degree of the extension F/E is the dimension $\dim_E F$ of F as an E-vector space, and is denoted by $[F : E]$. We call the extension F/E a finite degree field extension, or just a finite extension, if $[F : E]$ is finite.

We usually construct field extensions F/E by adjoining a root of an irreducible polynomial $f(t)$ to the base field E. Formally this is carried out by modding the polynomial ring $E[t]$ out by the maximal ideal (f), as in Theorem 5.12 of Stewart [24, p. 62].

Example 1.3. Adjoining a root α of the polynomial $x^3 - x - 1$ to $\mathbb{Q}$ gives an extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. Since the polynomial is irreducible over $\mathbb{Q}$, a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$ is given by $\{1, \alpha, \alpha^2\}$. This means the extension is finite of degree 3.

Since we will be working with number fields and suchlike the extensions we will deal with will usually be finite.

A useful result is how the degrees of two consecutive field extensions relate to the degree of the overall extension. A sequence of consecutive field extensions is usually referred to as a tower

of fields, and so we have the aptly named Tower Theorem which is Theorem 6.4 in Stewart [24, p. 68].

Theorem 1.4 (Tower Theorem)**.** *Let $K \subset L \subset M$ is a tower of fields, then the degrees of the extensions are related by:*

$$[M : K] = [M : L][L : K]$$

Example 1.5. A tower of fields is given by $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$. We can see that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] = 3$, and $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Using the Tower Theorem we calculate:

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 3 \cdot 2 = 6$$

Another useful construct is the composite of two fields:

Definition 1.6. Let E and F be two subfields of $\mathbb{C}$. The composite EF is the smallest subfield of $\mathbb{C}$ containing E and F.

Now we review some concepts from Galois Theory. In order to define a Galois extension abstractly we need the notion of a normal and a separable extension. Since we will be working over $\mathbb{C}$, separability comes automatically, see Section 9.3 of Stewart [24, pp. 112-114] so we make the following definitions:

Definition 1.7. An extension L/K is called normal if every irreducible polynomial $f \in K[x]$ which has at least one root in L splits in L. Equivalently every embedding σ of L in $\mathbb{C}$ which fixes K pointwise satisfies $\sigma(L) = L$.

Definition 1.8. Working over $\mathbb{C}$, a normal extension L/K is Galois and we define the Galois group $\mathrm{Gal}(L/K)$ of L/K to be set of automorphisms of L fixing K pointwise. It follows that $|\mathrm{Gal}(L/K)| = [L : K]$.

We may say an extension is cyclic if it is Galois with cyclic Galois group, and similarly an extension is abelian if it is Galois with abelian Galois group.

As shown in Proposition 3.20 of Milne [22, p. 39], if L and M are two abelian extensions of K, then the composite LM is also an abelian extension of K.

Definition 1.9. If L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and H is a subgroup of G, we define the fixed field of H to be:

$$L^H = \{\alpha \in L \mid \sigma(\alpha) = \sigma \text{ for all } \sigma \in H\}$$

The Fundamental Theorem of Galois Theory establishes the existence of a Galois connection between the subgroups of $\mathrm{Gal}(L/K)$ and the intermediate fields of L/K. Specifically we have

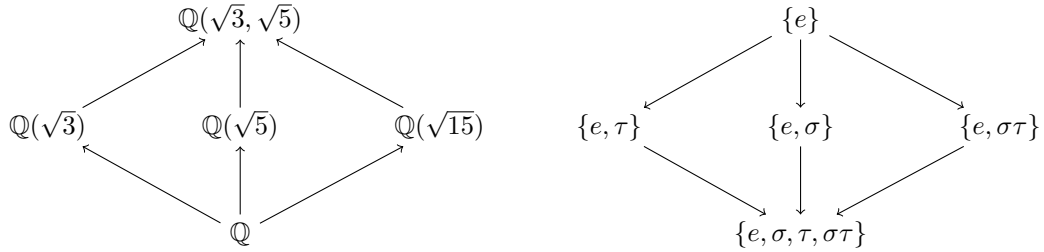
Theorem 1.10 (Fundamental Theorem of Galois Theory)**.** *If L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, then mappings:*

$$\{ \textit{ Fields } K \subset F \subset L \} \longleftrightarrow \{ \textit{ Groups } H < G \}$$

defined by sending a field $F \mapsto \mathrm{Gal}(L/F)$ and a group $H \mapsto L^H$ are mutual inverses, and set up an order-reversing one-to-one correspondence, called the Galois correspondence, between the intermediate fields of L/K and the subgroups of $\mathrm{Gal}(L/K)$.

Proof. See Chapter 12 and Theorem 12.1 in Stewart [24, pp. 133-136]. □

Example 1.11. The extension $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}$ is Galois, with $\mathrm{Gal}(L/K) = \{e,\sigma,\tau,\sigma\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $\sigma\colon \sqrt{3} \mapsto -\sqrt{3}$, and $\tau\colon \sqrt{5} \mapsto -\sqrt{5}$. The Galois correspondence set up the following correspondence between subgroups and subfields:



We also need a few results about finite fields and their Galois theory. A treatment of finite fields is given in Chapter 20 of Stewart [24, pp. 227–232], the main result of which is:

Theorem 1.12. *If F is a finite field, then F contains a unique subfield $\mathbb{Z}_p$, for some prime p (called the characteristic), and $|F| = p^n$, where $n = [F : \mathbb{Z}_p]$. For each $q = p^n$, with p prime, there exists up to isomorphism precisely one field with q elements, called the Galois Field $\mathbb{F}_q$.*

The main result on the Galois Theory of finite fields is the following from Hasse [12, p. 41]:

Theorem 1.13. *If $\mathbb{F}_r/\mathbb{F}_q$ is an extension of finite fields, then it is Galois with cyclic Galois group canonically generated by the Frobenius automorphism* $\mathrm{Frob} : x \mapsto x^q$.

1.2 Number Fields

Definition 1.14. A number field K is a finite extension of $\mathbb{Q}$.

Definition 1.15. An element $\alpha \in \mathbb{C}$ is called an algebraic integer if α is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

A combination of Theorem 1 and Theorem 2 in Marcus [18, pp.14–16] give various equivalent criterion for α to be an algebraic integer, some of which may easier to apply:

Theorem 1.16. *The following are equivalent for $\alpha \in \mathbb{C}$:*

i) α is an algebraic integer,
ii) The monic minimal polynomial of α over $\mathbb{Q}$ has integer coefficients,
iii) The additive group of the ring $\mathbb{Z}[\alpha]$ is finite generated,
iv) α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group.

An important corollary of this Theorem is that the sum and product of two algebraic integers are again algebraic integers, and so the algebraic integers in $\mathbb{C}$ form a ring. The method of the proof in fact gives a procedure to compute the polynomials they satisfy. We will denote the algebraic integers by $\mathbb{A}$. We can then make the following definition:

Definition 1.17. The ring of integers $\mathcal{O}_K$ of a number field K is the set of all algebraic integers in K. Being the intersection of two rings $\mathcal{O}_K = \mathbb{A} \cap K$, the ring of integers is indeed a ring. We call the elements of $\mathcal{O}_K$ the integers of K.

Example 1.18. i) Consider the number field $K = \mathbb{Q}(\sqrt{2})$. Both 1 and $\sqrt{2}$ are algebraic integers, since they are roots of the monic polynomials $x-1$, and x^2-2 respectively. Therefore any element of the form $a + b\sqrt{2}$, with $a, b \in \mathbb{Z}$, is an algebraic integer. By analysing the minimal polynomial of $r + s\sqrt{2} \in K$, as in Section 3.7 of Cohn [6, pp. 45-47], it follows that these are all the algebraic integers in $\mathbb{Q}(\sqrt{2})$. Hence $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$.

ii) Now take $K = \mathbb{Q}(\sqrt{-3})$. In this case $\frac{1+\sqrt{-3}}{2}$ is an algebraic integer as it is a root of the monic polynomal $x^2 - x - 1$. As above, analysing the minimal polynomial of $r + s\sqrt{2} \in K$ shows that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

iii) A more complicated example with a number field higher degree is given in Example 2.23 of Stewart and Tall [25, pp. 55–56], where the ring of integers of $K = \mathbb{Q}(\sqrt[3]{175})$ is shown to be $\mathbb{Z}\langle 1, \sqrt[3]{175}, \sqrt[3]{245}\rangle$. The example goes on to prove that integers cannot be written as $\mathbb{Z}[\theta]$, for any $\theta \in K$.

Quadratic fields, those with degree 2 over $\mathbb{Q}$, will be at the forefront of our attention. We will use their connection with quadratic forms to study what integers a quadratic form represents.

Definition 1.19. A quadratic field is a number field K with $[K : \mathbb{Q}] = 2$. As stated in Fröhlich and Taylor [10, p. 175], the quadratic fields correspond bijectively to the square-free integers $d \neq 1$, via $d \mapsto \mathbb{Q}(\sqrt{d})$.

The more general analysis in Section 3.7 of Cohn [6, pp. 45-47] establishes the following description of the ring of integers in any quadratic field:

Proposition 1.20. *The integers in the quadratic field $K = \mathbb{Q}(\sqrt{d})$ are given by:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{otherwise} \end{cases}$$

The analysis presented there is specific to the case of a quadratic number field, and relies on ad-hod methods of analysing the minimal polynomial. A more general and systematic method arises once the discriminant of a system has been defined, as explained in Section 2.6 of Stewart and Tall [25, pp. 51–57]

1.3 The Norm and The Discriminant

A number field K can be embedded in $\mathbb{C}$ in many ways. The Simple Extension Theorem, Theorem 2.2 in Stewart and Tall [25, pp. 36–37] guarantees that we can write any number field K as $K = \mathbb{Q}(\theta)$, where θ if the root of some polynomial $f \in \mathbb{Z}[x]$. Using this, Theorem 2.4 in Stewart and Tall [25, pp. 38-39] gives the following explicit description of the embeddings:

Theorem 1.21. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, then there are exactly n distinct embeddings $\sigma_i \colon K \hookrightarrow \mathbb{C}$, where $\sigma_i(\theta) = \theta_i$ are the (necessarily distinct) zeros of the minimal polynomial of θ.*

The first links between quadratic forms and number fields comes when we define the norm of an element.

Definition 1.22. Let $K = \mathbb{Q}(\theta)$ be a number of degree n with embeddings $\sigma_i \colon K \hookrightarrow \mathbb{C}$, and let $\alpha \in K$. We define the norm of α to be:

$$N(\alpha) = \prod_i \sigma_i(\alpha)$$

Corollaries 1 and 2 to Theorem 4 in Marcus [18, pp. 21–22], and a remark in Stewart and Tall [25, p. 49] establish the following properties of the norm:

Proposition 1.23. *Let K be a number field, and $\alpha, \beta \in K$, then:*
i) The norm $N(\alpha)$ is always rational.
ii) Furthermore, if $\alpha \in \mathcal{O}_K$, then $N(\alpha)$ is in fact a rational integer.
iii) The norm satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$.

Example 1.24. i) If $K = \mathbb{Q}(\sqrt{7})$ is a quadratic field, then we can embed $K \hookrightarrow \mathbb{C}$ via $\sigma_1 \colon \sqrt{7} \mapsto \sqrt{7}$ or $\sigma_2 \colon \sqrt{7} \mapsto -\sqrt{7}$. If $x + y\sqrt{7} \in K$, its norm is given by:

$$N(x + y\sqrt{7}) = (x + y\sqrt{7})(x - y\sqrt{7}) = x^2 - 7y^2$$

If we restrict to the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$, then x and y are integers. The question of what values the quadratic form $x^2 - 7y^2$ represents corresponds to the question of what possible norms an integer in $K = \mathbb{Q}(\sqrt{7})$ has.

ii) Similarly if we look at the cubic field $K = \mathbb{Q}(\sqrt[3]{2})$, we can embed $K \hookrightarrow \mathbb{C}$ via $\sigma_i \colon \sqrt[3]{2} \mapsto \sqrt[3]{2}\rho^i$, where $\rho^3 = 1$ is a primitive cube root of 1. The norm of an element $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is given by:

$$\begin{aligned} N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a + b\sqrt[3]{2}\rho + c\sqrt[3]{4}\rho^2)(a + b\sqrt[3]{2}\rho^2 + c\sqrt[3]{4}\rho) \\ &= a^3 + 2b^3 + 4c^3 - 6abc \end{aligned}$$

We will occasionally need to use the discriminant of a number field, particular its property regarding ramification of primes, and as a criterion to determine when we can apply Dedekind's Theorem. Given this we can define the discriminant of a basis of K as follows:

Definition 1.25. Let K be a number field of degree n with embeddings $\sigma_i \colon \mathbb{C} \hookrightarrow K$, and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of K. We define its discriminant to be:

$$\Delta_K(\alpha_1, \ldots, \alpha_n) = \det([\sigma_i(\alpha_j)])^2$$

Section 2.2 and 2.4 of Stewart and Tall [25, pp. 38–41, 45–49] establish some properties of the discriminant:

Proposition 1.26. *If $\{\beta_1, \ldots, \beta_n\}$ is another basis of K, related to the basis $\{\alpha_1, \ldots, \alpha_n\}$ by the change of basis matrix $M = [c_{ij}]$, so $\beta_j = \sum_{i=1}^n c_{ij}\alpha_i$, then:*

$$\Delta_K(\beta_1, \ldots, \beta_n) = (\det(M))^2 \Delta_K(\alpha_1, \ldots, \alpha_n)$$

Proposition 1.27. *If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K, then $\Delta_K(\alpha_1, \ldots, \alpha_n)$ is rational and non-zero. Furthermore if the α_i are integers, then $\Delta_K(\alpha_1, \ldots, \alpha_n)$ is a rational integer.*

Using these results they establish in Theorem 2.16 [25, pp. 46–47] that the ring of integers in any number field has a $\mathbb{Z}$-basis. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is necessarily a basis for K, and such a basis is called a integral basis for K. The discriminant of any integral basis of K takes the same value, and so this leads to the following definition:

Definition 1.28. The discriminant Δ_K of K is defined to be the discriminant of any integral basis $\{\alpha_1, \ldots, \alpha_n\}$ of K.

Example 1.29. i) If $d \equiv 1 \pmod 4$, the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ is given by $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, so $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis. Hence the discriminant of K is given by:

$$\begin{aligned}\Delta_K &= \Delta_K\left(1, \frac{1+\sqrt{d}}{2}\right) \\ &= \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 \\ &= \left(\tfrac{1-\sqrt{d}}{2} - \tfrac{1+\sqrt{d}}{2}\right)^2 \\ &= d\end{aligned}$$

ii) If $d \not\equiv 1 \pmod 4$, the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ is given by $\mathbb{Z}[\sqrt{d}]$, so $\{1, \sqrt{d}\}$ is an integral basis. Hence the discriminant of K is given by:

$$\begin{aligned}\Delta_K &= \Delta_K(1, \sqrt{d}) \\ &= \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 \\ &= (-\sqrt{d} - \sqrt{d})^2 \\ &= 4d\end{aligned}$$

A useful observation is that if $K = \mathbb{Q}(\theta)$ is a number field of discriminant Δ_K, and θ is an algebraic integer, then $\Delta_K \mid \Delta_K(1, \theta, \ldots, \theta^{n-1})$. By finding an integral basis $\{\alpha_1, \ldots, \alpha_n\}$, we can write θ_i as an $\mathbb{Z}$-linear combination of the α_i, so the change of basis matrix M has rational integer entries and rational integer determinant. Hence $\Delta_K(1, \theta, \ldots, \theta^{n-1}) = (\det(M))^2 \Delta_K(\alpha_1, \ldots, \alpha_i) = (\det(M))^2 \Delta_K$, which gives precisely the result.

Theorem 8 in Marcus [18, pp. 26–27] gives the following formula for calculating this:

Proposition 1.30. *If $K = \mathbb{Q}(\theta)$ is a number field, and with θ a root of the monic minimal polynomial $f \in \mathbb{Z}[x]$, then $\Delta_K(1, \theta, \ldots, \theta^{n-1})$ is given by:*

$$\Delta_K(1, \theta, \ldots, \theta^{n-1}) = \pm N(f'(\theta)) = \prod_{i<j} (\theta_i - \theta_j)^2$$

where θ_i are the roots of $f(x)$.

In the proposition above polynomial is monic, hence the expression on the right hand side can be recognised as the discriminant of the polynomial. The discriminant of a polynomial can be computed effectively.

1.4 Primes Ideals and Extensions of Number Field

We now turn our attention to prime ideals in the ring of integers of a number field, and their properties. Recall the definitions of a prime ideal and a maximal ideal.

Definition 1.31. In a commutative ring R, an ideal $I \neq R$ is called prime if has the property: $ab \in I$ implies $a \in I$ or $b \in I$. An ideal $M \neq R$ is called maximal if there are no proper ideals between M and R.

Theorem 14 in Marcus [18, pp. 56–57] establishes that the ring of integer $\mathcal{O}_K$ of a number field K is a so-called Dedekind domain, where the definition of a Dedekind domain is as follows:

Definition 1.32. A Dedekind domain is a integral domain R such that:
i) Every ideal is finitely generated,
ii) Every non-zero prime ideal is a maximal ideal,
iii) R is integrally closed in its field of fractions.

Theorem 16 in Marcus [18, pp. 59–60] then establishes that the ideals in any Dedekind domain factor uniquely into a product of prime ideals. A Corollary obtained during this proof is that if A and B are ideals in a Dedekind domain, then $A \mid B$ if and only if $A \supset B$. Combining these two results, as in the Corollary of Theorem 16, gives the following:

Proposition 1.33. *The ideals in the ring of integers $\mathcal{O}_K$ of a number field K factor uniquely into prime ideals.*

We usually refer to the non-zero prime ideals of $\mathcal{O}_K$ as simply the primes of K. Associated with each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we have a quotient ring $\mathcal{O}_K/\mathfrak{p}$.

Proposition 1.34. *For any prime $\mathfrak{p}$ of K, the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field, this is called the residue field.*

Proof. Since $\mathfrak{p}$ is a maximal ideal, the quotient ring is $\mathcal{O}_K/\mathfrak{p}$ is a field. The proof that more generally $\mathcal{O}_K/I$, where I is a non-zero ideal, is provided by Exercise 5.1 in Cox [7, p. 115]. Let I be a non-zero ideal, we find a non-zero rational integer $m \in I$ as follows. Since $I \neq (0)$, there is some $\alpha \neq 0 \in I$. The minimal polynomial of α is given by $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_0 \neq 0$. Then $a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha \in I$ since I is an ideal.

Now $\mathcal{O}_K/(m)$ is finite: find a $\mathbb{Z}$-basis for $\mathcal{O}_K$, after quotienting by (m), there are only m possibilities for each coefficient, so finitely many possible elements. Since $(m) \subset I$, quotienting by I identifies more elements of $\mathcal{O}_K$, hence $\mathcal{O}_K/I$ is finite. □

Definition 1.35. In a number field K, the quantity $|\mathcal{O}_K/I|$ is the norm of the ideal I, written $N(I)$.

The ideal norm satisfies various properties:
i) The ideal norm is multiplicative: $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.
ii) If (α) is a principal ideal, then $N((\alpha)) = |N(\alpha)|$.
This is part of Theorem 22 in Marcus [18, p. 65–69]

We can now consider how a prime ideal behaves in an extension of number fields. If L/K is an extension of number fields, and $\mathfrak{p}$ is a prime of K, then $\mathcal{O}_K \subset \mathcal{O}_L$ so we can lift $\mathfrak{p}$ to the ideal $\mathfrak{p}\mathcal{O}_L$ of L. We know the ideals in $\mathcal{O}_L$ factorise uniquely we must be able to write:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are primes of L. We make the following definitions:

Definition 1.36. In the situation above, the primes $\mathfrak{P}_i$ are said to be the primes of L above $\mathfrak{p}$, in the extension L/K.

Equivalent criteria for the prime $\mathfrak{P}$ to lie above $\mathfrak{p}$ are given by Theorem 19 in Marcus [18, p. 63], in particular we get the following result:

Proposition 1.37. *Let $\mathfrak{P}$ be a prime of L, and $\mathfrak{p}$ be a prime of K. Then $\mathfrak{P}$ lies above $\mathfrak{p}$ if and only if $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.*

Proof. If $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, then $\mathfrak{p} \subset \mathfrak{P}$, so $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$, and hence $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Conversely if $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, then $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$, so $\mathfrak{P} \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ which contains $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal and $1 \notin \mathfrak{P}$, we must have $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. □

Theorem 20 in Marcus [18, p. 63] then gives:

Proposition 1.38. *In the extension L/K, every prime $\mathfrak{P}$ of L lies over a unique prime of K.*

Proof. By the previous proposition this is equivalent to showing $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime of K. Firstly $\mathfrak{P} \cap \mathcal{O}_K$ is non-empty since $\mathfrak{P}$ contains some non-zero rational integer. Now $1 \notin \mathfrak{P}$, hence $1 \notin \mathfrak{p}$, so $\mathfrak{p} \neq \mathcal{O}_K$. Lastly, we prove $\mathfrak{p}$ is prime. Let $ab \in \mathfrak{p}$, then $ab \in \mathfrak{P}$, so since $\mathfrak{P}$ is prime, $a \in \mathfrak{P}$ or $by \in \mathfrak{P}$. Hence $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. □

Definition 1.39. In the decomposition above, the exponent e_i is called the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$, and we denote it by $e(\mathfrak{P}_i \mid \mathfrak{p}) = e_i$.

From Marcus we have the following observation. If $\mathfrak{P}$ is a prime of L above the prime $\mathfrak{p}$ of K, the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ composed with the quotient map $\mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{P}$ induces a ring homomorphism:

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{P}$$

with kernel $\mathcal{O}_K \cap \mathfrak{P} = \mathfrak{p}$. By the First Isomorphism Theorem, $\mathcal{O}_K/\mathfrak{p}$ is isomorphic to the image of the map in $\mathcal{O}_L/\mathfrak{P}$, hence we get an embedding $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$. This means we have an extension of residue fields. We know the residue fields are finite fields, and so this extension has finite degree.

Definition 1.40. Let $\mathfrak{P}$ be a prime of L above the prime $\mathfrak{p}$ of K. The degree of the residue field extension $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$ is called the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. We denote it by $f(\mathfrak{P} \mid \mathfrak{p})$.

We now state some results on the ramification indices and inertial degrees. From Exercise 10 in Chapter 3 Marcus [18, p. 83] we have the following:

Proposition 1.41. *The ramification indices and inertial degrees are multiplicative in towers, in particular if $K \subset L \subset M$ is a tower of fields, and $\mathfrak{p} \subset \mathfrak{P} \subset \mathfrak{R}$ are primes above each other in the extensions then:*

$$e(\mathfrak{R} \mid \mathfrak{p}) = e(\mathfrak{R} \mid \mathfrak{P})e(\mathfrak{P} \mid \mathfrak{p})$$
$$f(\mathfrak{R} \mid \mathfrak{p}) = f(\mathfrak{R} \mid \mathfrak{P})f(\mathfrak{P} \mid \mathfrak{p})$$

Proof. We get a tower of residue fields $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P} \subset \mathcal{O}_M/\mathfrak{R}$, and the multiplicativity of the inertial degree follows directly from the Tower Theorem.

For the ramification indices we use that each prime of an extension contains a unique prime below it. Factorise the prime $\mathfrak{p}$ as a product of primes in L. The prime $\mathfrak{P}$ above $\mathfrak{p}$ has ramification index $e(\mathfrak{P} \mid \mathfrak{p})$. The prime $\mathfrak{P}$ is the unique prime of L lying below $\mathfrak{R}$, so if we factorise this as a product of primes of M, we get ramification index $e(\mathfrak{R} \mid \mathfrak{P})$. Hence overall the exponent of $\mathfrak{R}$ in the factorisation of $\mathfrak{p}$ is $e(\mathfrak{R} \mid \mathfrak{P})e(\mathfrak{P} \mid \mathfrak{p})$, but by definition this is just the ramification index $e(\mathfrak{R} \mid \mathfrak{p})$. Hence we get the result. □

Theorem 21 in Marcus [18, p. 65–69] gives the following result which relates the ramification indices and inertial degrees in the factorisation of any prime $\mathfrak{p}$:

Proposition 1.42. *Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the primes above $\mathfrak{p}$ in the extension L/K. Let e_i, and f_i be respectively the ramification indices and inertial degrees of $\mathfrak{P}_i$ above $\mathfrak{p}$. We have:*

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

Now I will describe some different types of splitting that can occur when decomposing a prime:

Definition 1.43. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the primes above $\mathfrak{p}$ in the extension L/K. Let e_i, and f_i respectively the ramification indices and inertial degrees of $\mathfrak{P}_i$ above $\mathfrak{p}$. The prime $\mathfrak{p}$ is said to:

i) ramify if any $e_i > 1$.
ii) totally ramify if $g = 1$, $f_1 = 1$, and $e_1 = [L : K]$.
iii) be unramified if every $e_i = 1$
iv) split completely if $g = [L : K]$, every $e_i = 1$ and every $f_i = 1$.
v) remain inert if $\mathfrak{p}\mathcal{O}_L$ is prime in L.

A combination of Theorems 24 and 34 in Marcus [18, pp. 72–73, 112–114] gives us the following:

Theorem 1.44. *A prime p of $\mathbb{Z}$ is ramified the number field K if and only if $p \mid \Delta_K$.*

Theorem 31 in Marcus [18, p. 107] tells when a prime remains unramified in a composite:

Theorem 1.45. *Let K be a number field, and let L and M be two extensions of K. If the prime $\mathfrak{p}$ of K is unramified in both L and in M, then $\mathfrak{p}$ is unramified in the composite LM.*

We can use these results from number theory to study situations what arise from Galois theory. Following Exercise 2.1 in Washington [28, p. 17] we can find the quadratic subfields of the cyclotomic fields.

Example 1.46. From the Galois theory of the cyclotomic fields $L = \mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of 1, with p an odd prime, we know L must contain a unique quadratic subfield. This is because $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ has a unique index 2 subgroup. The Lagrange resolvent method works to find this subfield in simple cases, but does not give a general result.

By studying which primes ramify in L we can determine what the quadratic subfield must be. Marcus [18, p. 27] calculates the discriminant of the polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ generating $L/\mathbb{Q}$ to be $\mathrm{disc}\, f = p^{p-2}$. The discriminant Δ_L of L divides this, and so only the prime p can ramify in L.

Let $K = \mathbb{Q}(\sqrt{d})$, with $d \neq 0, 1$ and d square-free, be the quadratic subfield of L. Its discriminant is given by:

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{otherwise} \end{cases}$$

By the multiplicativity of e in towers, any prime q ramifying in K also ramifies in L. These primes q are exactly the primes dividing Δ_K. From this we see firstly $2 \nmid \Delta_K$, hence $d \equiv 1 \pmod 4$, and $\Delta_K = d$. Secondly, only p can divide Δ_K, hence $d = \pm p^n$, for some n. But $d \neq 1$ is square-free and $d \equiv 1 \pmod 4$ so the only possibility is $d = \pm p$, with the sign chosen so $d \equiv 1 \pmod 4$, that is $d = (-1)^{(p-1)/2} p$.

The field L has a quadratic subfield, but the only possibility is $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$, hence this must be the unique quadratic subfield of L.

In order to do any explicit calculations we need some method to determine how a prime ideal $\mathfrak{p}$ factors in an extension L/K. For this we turn to Dedekind's Theorem, Theorem 27 in Marcus [18, pp. 79-82]

Theorem 1.47 (Dedekind)**.** *Let L/K be an extension so that $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$. Let $h \in \mathcal{O}_K[x]$ be the monic minimal polynomial for α over K. Let $\mathfrak{p}$ be a prime of K such that the $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$, where p is the prime of $\mathbb{Z}$ below $\mathfrak{p}$. Then $h(x)$ factors uniquely into monic irreducible factors modulo $\mathfrak{p}$:*

$$\overline{h} = \overline{h_1}^{e_1} \cdots \overline{h_g}^{e_g}$$

and prime decomposition of $\mathfrak{p}\mathcal{O}_L$ is given by:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_i^{e_i} \cdots \mathfrak{P}_g^{e_g}$$

where $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + h_i(\alpha)\mathcal{O}_L$. Furthermore, the inertial degree is given by $f(\mathfrak{P}_i \mid \mathfrak{p}) = \deg(h_i)$.

As noted by Marcus the condition on p is satisfied whenever $L = \mathbb{Q}(\alpha)$, and $p^2 \nmid \operatorname{disc} f_\alpha$, where $f_\alpha(x)$ is the minimal polynomial for α over $\mathbb{Q}$. We will make use of this theorem later.

As stated in Proposition 5.11 in Cox [7, p. 102], if the polynomial $f(x)$ is separable modulo $\mathfrak{p}$, then the above theorem works and gives the decomposition of $\mathfrak{p}$ in the extension L/K.

1.5 Quadratic Fields and the Legendre Symbol

Here we will review the Legendre symbol and what it tells us about the decomposition of a prime in a quadratic field.

Definition 1.48. Let p be an odd prime. An integer a is said to be a quadratic residue modulo p if it is a perfect square modulo p. The Legendre symbol records this, and is defined to be:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is square modulo } p \\ -1 & \text{if } a \text{ is non-square modulo } p \end{cases}$$

It is completely multiplicative in the top argument:

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

and is periodic with period p in its top argument. If $a \equiv b \pmod{p}$, then:

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

An extremely important property the Legendre symbol satisfies is the law of quadratic reciprocity:

Theorem 1.49 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Proof. See Theorem A.20 in Stewart and Tall [25, pp. 286–288]. Later on we will indicate how class field theory can be used to prove and generalise quadratic reciprocity. □

Two supplements to this law tell us the values of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$:

Proposition 1.50 (Supplements to Quadratic Reciprocity)**.** *Let p be an odd prime. Then:*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Proof. See Proposition A.19 in Stewart and Tall [25, p. 286]. □

Using these we can determine the values of any Legendre symbol, and as we will need to do later, determine modulo which primes a given integer is square.

Example 1.51. i) To compute $\left(\frac{98765}{127}\right)$ we can proceed as follows:

$$\begin{aligned}
\left(\frac{98765}{127}\right) &= \left(\frac{86}{127}\right) \\
&= \left(\frac{2}{127}\right)\left(\frac{43}{127}\right) \\
&= (-1)^{(127^2-1)/8}\left(\frac{43}{127}\right) \\
&= \left(\frac{43}{127}\right) \\
&= \left(\frac{127}{43}\right)(-1)^{(127-1)(43-1)/4} \\
&= -\left(\frac{127}{43}\right) \\
&= -\left(\frac{-2}{43}\right) \\
&= -\left(\frac{2}{43}\right)\left(\frac{-1}{43}\right) \\
&= -(-1)^{(43^2-1)/8)}(-1)^{(43-1)/2} \\
&= -(-1)\cdot(-1) \\
&= -1
\end{aligned}$$

And so we conclude 98765 is not a square modulo 127.

ii) Something we will need to do later is calculate which primes an integer is square modulo. Modulo which primes is 6 a square? Equivalently we are asking when is $\left(\frac{6}{p}\right) = 1$. We can proceed as follows:

$$\left(\frac{6}{p}\right) = 1 \text{ if and only if } \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1 \text{ or } \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$$

To begin with we compute $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)(3-1)/4} = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$. This tells us $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{-1}{p}\right)$. Now let us determine when this takes values 1 or -1. For $\left(\frac{3}{p}\right) = 1$ we need $\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) = 1$ or $\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) = -1$. By the definition of the Legendre symbol we have $\left(\frac{p}{3}\right) = 1$ means p is a non-zero square modulo 3. The squares modulo 3 are 0 and 1, so we must have

$p \equiv 1 \pmod 3$. We also have $\left(\frac{-1}{p}\right) = 1$ means $p \equiv 1 \pmod 4$. So overall we have $p \equiv 1 \pmod 4$. On the other hand $\left(\frac{p}{3}\right) = -1$ means $p \equiv 2$, and $\left(\frac{-1}{p}\right) = -1$ means $p \equiv 3 \pmod 4$. Overall this is $p \equiv 11 \pmod{12}$. Hence $\left(\frac{3}{p}\right) = 1$ is equivalent to $p \equiv 1, 11 \pmod{12}$. Similarly $\left(\frac{3}{p}\right) = -1$ is equivalent to $p \equiv 5, 7 \pmod{12}$.

Now we can determine when $\left(\frac{6}{p}\right) = 1$. We have $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = 1$, so $p \equiv 1, 11 \pmod{12}$ and $p \equiv 1, 7 \pmod 8$. By the Chinese Remainder Theorem these congruences are equivalent to $p \equiv 1, 23 \pmod{24}$. On the other hand $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = -1$ means $p \equiv 5, 7 \pmod{12}$ and $p \equiv 3, 5 \pmod 8$, which is equivalent to $p \equiv 5, 19 \pmod{24}$.

Hence $\left(\frac{6}{p}\right) = 1$ if and only if $p \equiv 1, 5, 19, 23 \pmod{24}$.

The value of the Legendre symbol can be used to determine how the prime p decomposes in a quadratic field $K = \mathbb{Q}(\sqrt{d})$.

As Marcus [18, p. 74] notes, the formula $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}] = 2$ shows that there are only three possible ways in which the prime p can decompose:

$$
\begin{aligned}
&p\mathcal{O}_K \text{ is prime, that is } g = 1,\ e_1 = 1, \text{ and } f_1 = 2, \text{ or} \\
&p\mathcal{O}_K = \mathfrak{p}^2, \text{ so } g = 1,\ e_1 = 2, \text{ and } f_1 = 1, \text{ or} \\
&p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \text{ so } g = 2, \text{ and } e_i = f_i = 1
\end{aligned}
$$

The explicit decomposition of a prime p is in the quadratic field K well known and proven in Theorem 25 of Marcus [18, pp. 74–75]. What we need to draw from that Theorem is the following result:

Proposition 1.52. *The decomposition of an odd prime p in the quadratic field $\mathbb{Q}(\sqrt{d})$ is determined by the value of the Legendre symbol:*

i) If $\left(\frac{d}{p}\right) = 0$, then $p\mathcal{O}_K = \mathfrak{p}^2$ and so p ramifies.

ii) If $\left(\frac{d}{p}\right) = -1$, then $p\mathcal{O}_K$ is prime and so p is inert.

iii) If $\left(\frac{d}{p}\right) = 1$, then $p\mathcal{O}_L = \mathfrak{p}\widetilde{\mathfrak{p}}$ with $\mathfrak{p} \neq \widetilde{\mathfrak{p}}$ and so p splits (completely).

Here $\widetilde{\cdot}$ is the non-trivial automorphism of $\mathbb{Q}(\sqrt{d})$.

1.6 Primes in Galois Extensions

Now let us suppose that we are dealing with an arbitrary Galois extension. What effect does this have on the decomposition of primes and how does the arithmetic the number field interact with Galois theory?

We begin with a proposition on how prime ideals behave under the action of the Galois group:

Proposition 1.53. *Let L/K be a Galois, then the Galois group $\mathrm{Gal}(L/K)$ acts on the primes of L above a prime $\mathfrak{p}$ of K.*

Proof. As the Galois group acts on elements of L, it extends to an action on subsets of L. We first show that the Galois group takes an ideal of $\mathcal{O}_L$ to an ideal of $\mathcal{O}_L$, then establish it takes prime ideals to prime ideals, and finally that they both lie above $\mathfrak{p}$.

Let $\sigma \in \mathrm{Gal}(L/K)$. First observe that $\sigma(\mathcal{O}_L) = \sigma(\mathbb{A} \cap L) = \sigma(\mathbb{A}) \cap \sigma(L) = \mathbb{A} \cap L = \mathcal{O}_L$, since for any algebraic integer $\alpha \in \mathbb{A}$, $\sigma(\alpha)$ satisfies the same minimal polynomial hence is an algebraic integer. So a subset of $\mathcal{O}_L$ goes to a subset of $\mathcal{O}_L$.

Let I be an ideal of $\mathcal{O}_L$, then we show $\sigma(I)$ is an ideal of $\mathcal{O}_L$. Let $a, b \in \sigma(I)$, and take $r \in \mathcal{O}_L$. Then $\sigma^{-1}(a), \sigma^{-1}(b) \in I$, and $\sigma^{-1}(r) \in \mathcal{O}_L$. As I is an ideal we have: $\sigma^{-1}(a - b) =$

$\sigma^{-1}(a) - \sigma^{-1}(b) \in I$, and $\sigma^{-1}(ar) = \sigma^{-1}(a)\sigma^{-1}(r) \in I$. This implies $a - b \in \sigma(I)$ and $ar \in \sigma(I)$, hence $\sigma(I)$ is an ideal.

By a similar argument $\sigma(\mathfrak{P})$ is prime. Let $ab \in \sigma(\mathfrak{P})$, then $\sigma^{-1}(ab) = \sigma^{-1}(a)\sigma^{-1}(b) \in \mathfrak{P}$. Since $\mathfrak{P}$ is prime, we have $\sigma^{-1}(a) \in \mathfrak{P}$ or $\sigma^{-1}(b) \in \mathfrak{P}$. This implies $a \in \sigma(\mathfrak{P})$ or $b \in \sigma(\mathfrak{P})$, hence $\sigma(\mathfrak{P})$ is prime.

Lastly we find $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{p}) = \mathfrak{p}$, since σ fixes K pointwise. Hence $\sigma(\mathfrak{P})$ is a prime above $\mathfrak{p}$. □

An important feature of this action is that it is transitive, a fixed prime $\mathfrak{P}$ can be sent to any other prime above $\mathfrak{p}$. This tells us what the orbit of each prime $\mathfrak{P}$, and so allows us to use the Orbit-Stabilizer Theorem to gain insight into how the prime ideals behave in extensions.

Theorem 1.54. *The action of the Galois group on the primes of L above a prime $\mathfrak{p}$ of K is transitive. That is give primes $\mathfrak{P}$ and $\mathfrak{P}'$ of L above $\mathfrak{p}$, then there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Proof. A proof of this is given as Theorem 24 in Marcus [18, pp. 70-71], but uses the relative norm of an element. Since I have not introduced this, and won't use it elsewhere I will rephrase the proof to avoid it.

Suppose that the action isn't transitive, that is $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$ for any $\sigma \in \mathrm{Gal}(L/K)$.

By the previous proposition, we know the Galois group acts on the primes above $\mathfrak{p}$, so $\sigma(\mathfrak{P})$ is always a prime above $\mathfrak{p}$. Since primes are all coprime, the Chinese Remainder Theorem tells us we can pick an element $x \in \mathcal{O}_L$ such that:

$$\begin{cases} x \equiv 0 \pmod{\mathfrak{P}'} \\ x \equiv 1 \pmod{\sigma(\mathfrak{P})} \text{ for } \sigma \in \mathrm{Gal}(L/K) \end{cases}$$

Now consider the following product:

$$y \coloneqq \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

If we act by any $\tau \in \mathrm{Gal}(L/K)$, the order of the factors in the product is just permuted hence $\tau(y) = y$. But this means y is fixed under all elements of $\mathrm{Gal}(L/K)$, hence $y \in L^{\mathrm{Gal}(L/K)} = K$. Each factor is also an algebraic integer, so furthermore $y \in \mathbb{A}$. Hence $y \in K \cap \mathbb{A} = \mathcal{O}_K$.

We also have that $y \in \mathfrak{P}'$, since one of the factors is in $\mathfrak{P}'$, specifically when σ is the identity automorphism $\sigma(x) = x \in \mathfrak{P}'$. So overall we have that $y \in \mathcal{O}_K \cap \mathfrak{P}' = \mathfrak{p}$. But now since $\mathfrak{P} \mid \mathfrak{p}$, we have $\mathfrak{P} \supset \mathfrak{p}$, and hence $y \in \mathfrak{P}$.

By permuting the factors of the product, we may write y as a product over σ^{-1}. So on one hand we have $x \notin \sigma(\mathfrak{P})$, for any $\sigma \in \mathrm{Gal}(L/K)$, hence $\sigma^{-1}(x) \notin \mathfrak{P}$. And on the other hand we have $y \in \mathfrak{P}$, hence some $\sigma^{-1}(x) \in \mathfrak{P}$. This is a contradiction.

Hence the assumption that the action isn't transitive is wrong, and so the Galois group acts transitively on the primes of L above a prime $\mathfrak{p}$ of K as required. □

From this theorem we get the following corollaries which place very strong restrictions on how a prime can decompose in a Galois extension:

Corollary 1.55. *In a Galois extension L/K the ramification indices and inertial degrees of any two primes $\mathfrak{P}_1$, $\mathfrak{P}_2$ of L above a prime $\mathfrak{p}$ of K are the same. That is $e(\mathfrak{P}_1 \mid \mathfrak{p}) = e(\mathfrak{P}_2 \mid \mathfrak{p})$, and $f(\mathfrak{P}_1 \mid \mathfrak{p}) = f(\mathfrak{P}_2 \mid \mathfrak{p})$. We may then denote these quantities simply by $e = e(\mathfrak{p})$, and $f = f(\mathfrak{p})$ respectively.*

Proof. Since the Galois group acts transitively on the primes above $\mathfrak{p}$ we can find $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

Decompose $\mathfrak{p}\mathcal{O}_L$ as a product of prime of L:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

Now act by σ on both sides. On the left hand side we have $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$. On the right hand side σ permutes the primes, and so we get:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \sigma(\mathfrak{P}_i)^{e_i}$$

Since $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$, comparing the two factorisations gives, by uniqueness of prime factorisation, that $e_2 = e_1$. Since the primes were chosen arbitrarily, the ramification index of every prime $\mathfrak{P}_i$ above $\mathfrak{p}$ must be the same.

To prove the inertial degrees are equal we need to establish an isomorphism between $\mathcal{O}_L/\mathfrak{P}_1$ and $\mathcal{O}_L/\mathfrak{P}_2$. The isomorphism comes from considering the homomorphism obtained by applying the isomorphism σ^{-1} to $\mathcal{O}_L$ and modding by $\mathfrak{P}_1$:

$$\mathcal{O}_L \xrightarrow{\sigma^{-1}} \mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{P}_1$$

The kernel of this composition is $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$, and by the First Isomorphism Theorem we obtain $\mathcal{O}_L/\mathfrak{P}_2 \cong \mathcal{O}_L/\mathfrak{P}_1$. Then the result follows since:

$$f(\mathfrak{P}_1 \mid \mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P}_1 : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{P}_2 : \mathcal{O}_K/\mathfrak{p}] = f(\mathfrak{P}_2 \mid \mathfrak{p})$$ □

Corollary 1.56. *If $\mathfrak{p}$ is a prime of K, and the g primes of L above $\mathfrak{p}$ in the Galois extension L/K have ramification index e and inertial degree f, the formula from Proposition 1.42 becomes simply:*

$$efg = [L : K]$$

Proof. In the previous formula we have $e_i = e$, and $f_i = f$, hence:

$$[L : K] = \sum_{i=1}^{g} e_i f_i = \sum_{i=1}^{g} ef = efg$$ □

In a Galois extension L/K the conditions for the various types of splitting simplify. If $\mathfrak{p}$ is a prime of K, and the ramification index and inertial degree of any prime $\mathfrak{P}$ above $\mathfrak{p}$ is given by e and f respectively, then $\mathfrak{p}$ is said to:

i) ramify if $e > 1$.
ii) be unramified if $e = 1$.
iii) split completely if $e = 1$ and $f = 1$.

The link between number fields and Galois theory, coupled with Dedekind's Theorem force very strict behaviour on the polynomials generating Galois extensions.

Example 1.57. i) The splitting field of the polynomial $x^3 - 2$ is $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$, where $\rho^3 = 1$. This means $K/\mathbb{Q}$ is Galois, and it is generated by the polynomial $f(x) = x^6 + 108$.

Since $K/\mathbb{Q}$ is Galois, the results above say that the inertia degree and ramification index of any prime $\mathfrak{p}$ above a prime p of $\mathbb{Q}$ is the same. Dedekind's Theorem gives the decomposition of

p in terms of the factorisation of $f(x)$ modulo p, at least for primes $p \nmid \operatorname{disc}(f) = -2^{16} \cdot 3^{21}$, the ramification indices given by the degrees of the factors. Hence when reducing modulo p each factor *must* have the same degree.

Looking modulo various primes demonstrates this:

p	Factorisation of $f(x) \pmod p$
5	$(x^2+4x+2)(x^2+x+2)(x^2+2)$
7	$(x^3+5)(x^3+2)$
11	$(x^2+10x+4)(x^2+x+4)(x^2+4)$
13	$(x^3+3)(x^3+10)$
31	$(x+28)(x+15)(x+18)(x+13)(x+3)(x+16)$
47	$(x^2+7)(x^2+16x+7)(x^2+31x+7)$

ii) Conversely if a polynomial factors modulo p into factors of different degrees, than the extension *cannot* be Galois. The irreducible polynomial $f(x) = x^3 + x + 1$ has discriminant -31, and modulo $p = 2$ it has irreducible factorisation:

$$f(x) \equiv (x+2)(x^2+x+2) \pmod 2$$

Since it has irreducible factors of different degrees, the extension $\mathbb{Q}(\alpha)$, where α is a root of $f(x)$ is not a Galois extension.

Later on, after we have developed some more theory we can explore more elaborate examples relating number fields and the factorisation of polynomials modulo p.

Finally introduce the decomposition and inertia group of a prime ideal, which will make an appearance later when we study class field theory. Let L/K be a Galois extension with Galois group $G = \operatorname{Gal}(L/K)$, and let $\mathfrak{P}$ be a prime above $\mathfrak{p}$.

Definition 1.58. i) The decomposition group of $\mathfrak{P}$ is $D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$.
ii) The inertia group of $\mathfrak{P}$ is $I_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(x) \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in \mathcal{O}_L\}$.

Both of these are subgroups of the Galois group. In fact the decomposition group $D_{\mathfrak{P}}$ is just the stabiliser of $\mathfrak{P}$ under the action of the Galois group. Since we know the action is transitive we know the orbit, and we can use the Orbit-Stabilizer Theorem to give:

Proposition 1.59. *The size of the decomposition group is $|D_{\mathfrak{P}}| = ef$, where e and f is the ramification index and inertia degree of the prime $\mathfrak{P}$.*

Proof. There are g primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ above $\mathfrak{p}$, hence the orbit of $\mathfrak{P}$ has size g. The quantities are related by $efg = [L:K] = |G|$, where $G = \operatorname{Gal}(L/K)$ is the Galois group of L/K. Hence by the Orbit-Stabilizer Theorem:

$$efg = |G| = |D_{\mathfrak{P}}|\,|G(\mathfrak{P})| = |D_{\mathfrak{P}}|\,g$$

Cancelling g from both sides gives $|D_{\mathfrak{P}}| = ef$. □

Following Marcus [18, p. 99], we can show the elements of $D_{\mathfrak{P}}$ naturally induce automorphisms of the residue field. Let $\sigma \in D_{\mathfrak{P}}$, σ restricts to an isomorphism from $\mathcal{O}_L$ to itself, and so consider the composite homomorphism:

$$\mathcal{O}_L \xrightarrow{\sigma} \mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{P}$$

The kernel of this map is given by $\sigma^{-1}(\mathfrak{P})$ which is just $\mathfrak{P}$, by definition of the decomposition group. Hence the map factors through the quotient $\mathcal{O}_L/\mathfrak{P}$, giving a commutative diagram:

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

The induced map $\overline{\sigma}$ fixes $\mathcal{O}_K/\mathfrak{p}$ pointwise since σ fixes K pointwise, and hence $\overline{\sigma}$ is in the Galois group $\widetilde{G}$ of the extension $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$. Placing a copy of the diagram for the map τ, next to the diagram for σ shows that the composition in $D_{\mathfrak{P}}$ gives composition of the induced maps, and hence we get a group homomorphism $D_{\mathfrak{P}} \to \widetilde{G}$.

If the induced map $\overline{\sigma}$ is the identity, then we must have $[\sigma(\alpha)] = [\alpha]$ in the quotient $\mathcal{O}_L/\mathfrak{P}$. But this says precisely $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$. Hence the kernel of the map $D_{\mathfrak{p}} \to \widetilde{G}$ is precisely the inertial group $I_{\mathfrak{P}}$.

As proven in Corollary 1 to Theorem 28 in Marcus [18, p. 101], this map is actually surjective, and so using the First Isomorphism Theorem we get an isomorphism:

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \widetilde{G}$$

From this we obtain the following results:

Corollary 1.60. *The inertia group $I_{\mathfrak{P}}$ has order f.*

Proof. The Galois group $\widetilde{G}$ of the residue field extension has order f, and hence

$$|D_{\mathfrak{P}}| \,/\, |I_{\mathfrak{P}}| = |\widetilde{G}| = f$$

Since $D_{\mathfrak{P}}$ has order ef, the inertia group $I_{\mathfrak{P}}$ must have order e. □

Corollary 1.61. *The quotient $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is cyclic.*

Proof. We know the Galois group of an extension of finite fields is cyclic. □

Using this we can explore another example of how the number theory and Galois theory force a particular structure on the factorisation of a polynomial modulo p. The motivation for this example comes from Exercise 6 in Chapter 5 of Janusz [14, p. 139]

Example 1.62. There exists a polynomial $f(x)$, such that $f(x)$ is irreducible over $\mathbb{Q}$, but is reducible modulo every prime p. In other words $f(x)$ is irreducible, but the reduction modulo p test would never show this.

Proof. Consider the polynomial $f(x) = x^4 - 10x^2 + 1$, which is the generating polynomial of the degree 4 Galois extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. Since it generates the extension it must be irreducible. We see the discriminant of $f(x)$ is $2^{14}3^2$, and so primes $p \neq 2, 3$ are unramified in the extension. Modulo 2 and 3 the polynomial $f(x)$ is reducible:

$$\begin{aligned} x^4 + 10x^2 + 1 &\equiv x^4 + 1 = (x+1)^4 \pmod{2}, \text{ and} \\ x^4 + 10x^2 + 1 &\equiv x^4 - x^2 + 1 = (x^2+1)^2 \pmod{3}. \end{aligned}$$

This is more generally true: a polynomial is reducible modulo any prime p which divide its discriminant: modulo p the discriminant is 0, so the polynomial has multiple roots. This means

$\gcd(\overline{f}, \overline{f'})$ is non-trivial, and as always can be written as a linear combination of $\overline{f}, \overline{f'}$. So $\overline{f}$ has a non-trivial factor.

Now if p is any other prime, Dedekind's theorem tell us how (p) factors in K, and this corresponds to how the polynomial $f(x)$ factors modulo p. For any prime $\mathfrak{P}$ above p, we know $D_{\mathfrak{P}} \cong \widetilde{G}$, and so is cyclic. But the Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so the largest cyclic subgroup has order 2. Thus we have $|D_{\mathfrak{P}}| = ef \leq 2$, and so $g = \frac{[K:\mathbb{Q}]}{ef} \geq 2$. This means the prime p cannot remain inert, and so must split. But this means the polynomial $f(x)$ must split modulo p, and so is reducible.

This shows two things: firstly that $f(x) = x^4 - 10x^2 + 1$ is reducible modulo every prime p as claimed, and secondly (after we check that (2) and (3) ramify, and in particular split) that no prime (p) remains inert in the extension $K/\mathbb{Q}$. □

There was nothing particularly special about the extension $K/\mathbb{Q}$ above, other than it *wasn't* cyclic. The above argument would give exactly the same conclusion for the generating polynomial of any non-cyclic Galois extension, and so we can generate wealth of such examples. For a more detailed look this, see the article by Guralnick, Schacher, and Sonn [11].

We can also extract from it the following general proposition:

Proposition 1.63. *If L/K is a non-cyclic Galois extension of number fields, then no prime $\mathfrak{p}$ of K can remain inert in L.*

Proof. If $\mathfrak{p}$ remains inert in the extension, then we know $e = g = 1$, and so we calculate $f = [L : K]$. This means $D_{\mathfrak{P}} = \mathrm{Gal}(L/K)$. But since $e = 1$ and so $I_{\mathfrak{P}}$ is trivial, we have the isomorphism $D_{\mathfrak{P}} \cong D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \widetilde{G}$, where $\widetilde{G}$ is the Galois group of the residue field extension. We know $\widetilde{G}$ is cyclic, so this tells us that $D_{\mathfrak{P}}$ is cyclic, and hence $\mathrm{Gal}(L/K)$ is cyclic, but we assumed it isn't. So we have a contradiction. Hence no prime $\mathfrak{p}$ of K can remain inert in L. □

1.7 Class Groups

In this section we will review the class group of a number field, and introduce the narrow class group.

Definition 1.64. A fractional ideal of a number field K is a finitely generated $\mathcal{O}_K$-submodule of K. Every fractional ideal can be written as λI, for some $\lambda \in K^*$, and some ideal I of $\mathcal{O}_K$.

By Theorem 2 in Section 1.6 of Lang [16, p. 18], the non-zero fractional ideals of a number field form a group under multiplication. Moreover a fractional ideal $\mathfrak{a}$ factors uniquely as a product of prime of K:

$$\mathfrak{a} = \prod_{i=1}^{g} \mathfrak{p}_i^{r_i}$$

We denote the group of non-zero fractional ideals by $\mathcal{I}(K)$. We define two important subgroups of the fractional ideals as follows:

Definition 1.65. A fractional ideal of the form (α), for $\alpha \in K^*$, is called a principal fractional ideal. The subgroup of principal fractional ideals is denoted by $\mathcal{P}(K)$.

Definition 1.66. An element $\alpha \in K$ is called totally positive if $\sigma(\alpha) > 0$, for every real embedding $\sigma \colon K \hookrightarrow \mathbb{R}$. By extension a principal fractional ideal (α) is called totally positive if it is generated by some totally positive α. The subgroup of totally positive principal fractional ideals is denoted by $\mathcal{P}^+(K)$.

If the number field K has no real embeddings, then $\sigma(\alpha) > 0$ is vacuously true. This holds in particular if K is an imaginary field, and so every principal fractional ideal is totally positive. In real quadratic fields this is not always the case.

Example 1.67. Consider the real quadratic field $K = \mathbb{Q}(\sqrt{2})$. In this case we can show every principal fractional ideal is totally positive. We can embed $K \hookrightarrow \mathbb{R}$ in two way, either via $\sigma_1 \colon \sqrt{2} \mapsto \sqrt{2}$, or via $\sigma_2 \colon \sqrt{2} \mapsto -\sqrt{2}$.

Let (α) be a principal fractional ideal. The fundamental unit of K is $u = 1 + \sqrt{2}$, which as norm $N(u) = -1$. Equivalently this means $\sigma_1(u)\sigma_2(u) = -1$, so $\sigma_1(u)$ and $\sigma_2(u)$ have opposite signs. If $\sigma_1(\alpha)$ and $\sigma_2(\alpha)$ have different signs, then $\sigma_1(u\alpha)$ and $\sigma_2(u\alpha)$ have the same sign. If the signs are negative than $\sigma_1(-u\alpha)$ and $\sigma_2(-u\alpha)$ have positive sign. Multiplying the generator of an ideal by units does not change the ideal, so $(\alpha) = (\pm u\alpha)$, and in this latter representation we see the ideal is totally positive.

The same analysis works whenever the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$ has negative norm. In this case the group of totally positive principal fractional agrees with the group of principal fractional ideals. Things are more interesting when the fundamental unit has positive norm.

Example 1.68. The fundamental unit of the real quadratic field $K = \mathbb{Q}(\sqrt{6})$ is $u = 5 + 2\sqrt{6}$, of norm -1. The same trick as above does not work, and in fact not all principal ideals are totally positive. Consider, say, the ideal $\mathfrak{a} = (2 + \sqrt{6})$ generated $\alpha = 2 + \sqrt{6}$. The norm of the generator is $N(\alpha) = 4 - 6 = -2$, and so α has different signs under the embeddings $\sigma_1 \colon \sqrt{6} \mapsto \sqrt{6}$, and $\sigma_2 \colon \sqrt{6} \mapsto -\sqrt{6}$. Any other generator of the ideal $\mathfrak{a}$ is associate to α, so is of the form $\pm u^n \alpha$, but this too has norm $N(\pm u^n \alpha) = -1$. So $\mathfrak{a}$ is *not* totally positive.

We then define following class groups of a number field:

Definition 1.69. The class group of a number field K is the quotient group $\mathcal{I}(K)/\mathcal{P}(K)$, and it is denoted by $\mathcal{C}(K)$. The size of $\mathcal{C}(K)$ is the class number of K, denoted by $h(K)$.

Definition 1.70. The narrow class group of a number field K is the quotient group $\mathcal{I}(K)/\mathcal{P}^+(K)$, and it is denoted by $\mathcal{C}^+(K)$. The size of $\mathcal{C}^+(K)$ is the narrow class number of K, denoted by $h^+(K)$.

Both of these groups are finite, so the class numbers are always finite. This is proven more generally using class field theory. For an imaginary quadratic field the class group and the narrow class group agree. In a real quadratic number field we can give a simpler description of the totally positive principal ideals:

Proposition 1.71. *Let K be a real quadratic number field. An ideal $I = (\alpha)$ is totally positive if and only if it has a generator of positive norm.*

Proof. If I is generated by an element α of positive norm, then $\sigma_1(\alpha)\sigma_2(\alpha) > 0$, where σ_1, σ_2 are the real embeddings of K. In this case $\sigma_1(\alpha)$ and $\sigma_2(\alpha)$ have the same sign, and so one of α or $-\alpha$ is totally positive. They generate the same ideal, hence the ideal I is totally positive.

If I is totally positive, then it is generated by an element α with $\sigma_1(\alpha) > 0$ and $\sigma_2(\alpha) > 0$. The norm of α is $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) > 0$, so α is of positive norm. □

For a real quadratic field K, we can relate the sizes of the class group and the narrow class group. Following Exercise 7.23 in Cox [7, pp. 155–156] we obtain the result:

Proposition 1.72. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with fundamental unit u. Then:*

$$\frac{h^+(K)}{h(K)} = \begin{cases} 1 & \text{if } N(u) = -1 \\ 2 & \text{if } N(u) = 1 \end{cases}$$

Proof. The composition of the identity map on $\mathcal{I}(K)$ followed by the projection to $\mathcal{C}(K)$ induces a group homomorphism with kernel $\mathcal{P}(K)$. Since $\mathcal{P}^+(K) \subset \mathcal{P}(K)$, this map factors through the quotient $\mathcal{I}(K)/\mathcal{P}^+(K)$, and hence induces a surjective map $\mathcal{C}^+(K) \twoheadrightarrow \mathcal{C}(K)$ fitting into the commutative diagram:

$$\begin{array}{ccc} \mathcal{I}(K) & \longrightarrow & \mathcal{I}(K) \\ \downarrow & & \downarrow \\ \mathcal{C}^+(K) = \mathcal{I}(K)/\mathcal{P}^+(K) & \twoheadrightarrow & \mathcal{C}(K) = \mathcal{I}(K)/\mathcal{P}(K) \end{array}$$

The kernel of the induced map is $\mathcal{P}(K)/\mathcal{P}^+(K)$.

Next we show that $\mathcal{P}(K) = \mathcal{P}^+(K) \cup \sqrt{d}\mathcal{P}^+(K)$. Since the principal fractional ideals form a group each factor on the right hand side is a principal fractional ideal, hence we get the inclusion $\mathcal{P}(K) \supset \mathcal{P}^+(K) \cup \sqrt{d}\mathcal{P}^+(K)$. On the other hand, given a principal fractional ideal (α), one of α or $\alpha/\sqrt{d}$ has positive norm since $N(\sqrt{d}) = -d < 0$. This means one of (α) or $(\alpha/\sqrt{d})$ is totally positive, hence we get the other inclusion. Taking the quotient shows that $\mathcal{P}(K)/\mathcal{P}^+(K) = \{[(1)], [(\sqrt{d})]\}$, so the kernel has size 1 or 2.

If the kernel of the induced map has size 1, then $[(1)] = [(\sqrt{d})]$ and so $I = (\sqrt{d})$ is totally positive. Hence we can find a generator α of I with positive norm. Any other generator is associate to $\sqrt{d}$, and so $\alpha = \pm u^n\sqrt{d}$. Taking norms shows that $N(u^n) = -1$, hence $N(u) = -1$, and the fundamental unit has negative norm. Conversely if the fundamental unit has negative norm, we can find a generator of $(\sqrt{d})$ which is totally positive, hence $[(1)] = [(\sqrt{d})]$, and the kernel of the induced map has size 1.

We concluded:

$$\frac{|\mathcal{C}^+(K)|}{|\mathcal{C}(K)|} = \left|\mathcal{P}(K)/\mathcal{P}^+(K)\right| = \begin{cases} 1 & \text{if } N(u) = -1 \\ 2 & \text{if } N(u) = 1 \end{cases}$$

□

We can now compute the narrow class numbers of some real quadratic fields once we know the class numbers.

Example 1.73. i) The real quadratic field $K = \mathbb{Q}(\sqrt{6})$ has class number $h(K) = 1$. Its fundamental unit is $u = 5 + 2\sqrt{6}$, which has norm $N(u) = 1$. So $h^+(K) = 2h(K) = 1$.

ii) The real quadratic field $K = \mathbb{Q}(\sqrt{10})$ has class number $h(K) = 2$. Its fundamental unit is $u = 3 + \sqrt{10}$, which has norm $N(u) = -1$. So $h^+(K) = h(K) = 2$.

Chapter 2

Binary Quadratic Forms

The primary focus of this report is to find criteria for when a prime is represented by the quadratic form $x^2 + ny^2$. To this end we will spend some time studying quadratic forms and the theory surrounding them. The basic results in this chapter will allow us to give a proof of Fermat's claims and take some small steps beyond them.

The basic definitions and results on binary quadratic forms are from Cox [7]. For equivalence of forms we work from Flath [8]. Finiteness of the class number comes from Cohen [4], and the correspondence between forms and ideals comes from Fröhlich and Taylor [10]. After this we return to Cox [7] to study the primes a form represents.

2.1 Definition of a Quadratic Form

We already have something of an idea what a quadratic form is, but we should give a formal definition, and explain some related terminology.

Definition 2.1. A quadratic form is a degree 2 homogeneous polynomial in some number of variables. The prefix n-ary tell us that it is in n variables, so a binary quadratic form is a quadratic form in two variables.

Example 2.2. i) The polynomial $x^2 + y^2$ is a binary quadratic form. Any binary quadratic form has the form $ax^2+bxy+cy^2$, where a, b, c are some coefficients. Taking $a = 1$, $b = 0$, and $c = n \in \mathbb{Z}$, gives us the quadratic form $x^2 + ny^2$ which is the focus of this report. The coefficients do not have to be integers, so $(\mathrm{e} + \sqrt{2})x^2 + \mathrm{i}xy + \pi y^2$ is a perfectly fine binary quadratic form

ii) An example of a ternary quadratic form is $x^2 + 2y^2 + 3z^2 + 5xy + 2xz$, and an example of a quaternary quadratic form is $x^2 + 2y^2 + 5z^2 + 5w^2$.

Remark 2.3. It will sometimes be useful to write and think of the binary quadatic form $ax^2 + bxy + cy^2$ as a matrix product:

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

where the matrix $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ is called the matrix of the form, or sometimes the Gram matrix.

Whilst in general there are no restrictions on what the coefficients can be, the most interesting and useful case for us and number theory is when they are integers. Whether or not the coefficients are coprime strongly affects the behaviour of the form, and what values it can represent.

Definition 2.4. A quadratic form is called integral if all the coefficients are integers. An integral quadratic form is called primitive if the coefficients are coprime.

Remark 2.5. The definition of what constitutes an integral quadratic form is the source of some confusion and controversy. Historically the convention adopted by Gauss was that a form is integral if its matrix is integral, and so the off-diagonal coefficients are even. Nowadays the convention is that the coefficients of the form are integers, and so the matrix can have half-integer off-diagonal entries.

Definition 2.6. We say that an integral binary quadratic form $f(x, y)$ represents the integer m if $m = f(x, y)$ has a solution with $x, y \in \mathbb{Z}$.

Example 2.7. i) The quadratic form $f(x, y) = x^2 + 5y^2$ represents $m = 0, 1, 4, 5, 6, \ldots$, since each of :

$$\begin{aligned} 0 &= f(0,0) = 0^2 + 5 \cdot 0^2 \\ 1 &= f(1,0) = 1^2 + 5 \cdot 0^2 \\ 4 &= f(2,0) = 2^2 + 5 \cdot 0^2 \\ 5 &= f(0,1) = 0^2 + 5 \cdot 1^2 \\ 6 &= f(1,1) = 1^2 + 5 \cdot 1^2 \end{aligned}$$

is a solution in integers to $m = f(x, y)$.

However $f(x, y)$ does not represent 2, or 3. If we try to solve $2 = x^2 + 5y^2$, with $x, y \in \mathbb{Z}$, we need firstly $y = 0$ otherwise the result will already be too large. Then this gives $2 = x^2$, but since $\sqrt{2}$ is irrational there is no solution with $x \in \mathbb{Z}$. Similarly $3 = x^2 + 5y^2$ cannot be solved in integers.

ii) It is more difficult to determine whether or not an integer is represented by a quadratic form like $g(x, y) = x^2 - 2y^2$, since there aren't any obvious bounds on the size x and y beyond which no solution is possible. We can make some headway with small values using a combination of luck, good guesses and experimentation, but this does not work generally. Being able to find a criterion which will give a definitive answer in a finite time is *much* more useful in this case.

We see that $g(x, y) = x^2 - 2y^2$ represents $m = 0, 1, 2, 4, 7, \ldots$, since each of:

$$\begin{aligned} 0 &= f(0,0) = 0^2 - 2 \cdot 0^2 \\ 1 &= f(1,0) = 1^2 - 2 \cdot 0^2 \\ 2 &= f(3,2) = 3^2 - 2 \cdot 2^2 \\ 4 &= f(2,0) = 2^2 - 2 \cdot 0^2 \\ 7 &= f(3,1) = 3^2 - 2 \cdot 1^2 \end{aligned}$$

is a solution in integers to $m = g(x, y)$. Try as we might, the form doesn't seem to represent 3, 5, or 6. Unlike above, checking all possibilities is not possible, and so a proof does not come as easily.

In light of this we can restate the first goal of this report as finding which primes the binary quadratic form $x^2 + ny^2$ represents.

If the integral binary quadratic form we are studying is not primitive, then every integer represented by the form is divisible by the greatest common divisor d of the coefficients. In particular, if the form represents the prime p, then $d \mid p$, and so $d = p$. From this we see that if d is not prime, the form does not represent any primes. However if d is prime, the only prime which the form might represent is $d = p$ itself.

Primes Represented by Non-Primitive Forms

i) What primes does $q(x, y) = 3x^2 + 18y^2$ represent? Since the form is not primitive, and the gcd of the coefficients is $d = 3$, the only prime the form can represent is $p = 3$. We see easily that $3 = q(1, 0)$ is represented by $q(x, y)$.

ii) What primes does $r(x, y) = 4x^2 + 4xy + 6y^2$ represent? The gcd of the coefficients is $d = 2$, so the only prime which $r(x, y)$ can represent is $p = 2$. By completing the square we can write $r(x, y)$ as $r(x, y) = 4(x + \frac{y}{2})^2 + 5y^2$. From this we see that $r(x, y)$ cannot represent 2: we need $y = 0$ firstly, and then $x = 0$ to prevent the result being too large, but $r(0, 0) = 0 \neq 2$.

iii) What primes does $s(x, y) = 9x^2 - 3y^2$ represent? The gcd of the coefficients is $d = 3$, so the only prime which $s(x, y)$ can represent is $p = 3$. On dividing through, the question becomes whether $3x^2 - y^2$ represents $m = 1$, or equivalently whether $x^2 - 3y^2$ represents $m = -1$? As it turns out it doesn't: by recognising $x^2 - 3y^2$ as the norm form on $\mathbb{Q}(\sqrt{3})$ this says $x + y\sqrt{3}$ is a unit of norm -1. The fundamental unit $u = 2 + \sqrt{3}$ has norm $N(u) = 1$, so there are no units of negative norm. We begin to see connections between quadratic forms and quadratic fields!

Later on we will see that the criterion we generate work for all but a finite set of excluded primes. The above result have precisely this form for non-primitive forms: for $p \neq d$, the quadratic form does not represent p. So we have answered the question to the same level as we will in the primitive case. For this reason we will make the assumption that all quadratic forms are primitive from now on.

2.2 The Discriminant of a Quadratic Form

We will now introduce the discriminant of a quadratic form. The discriminant gives us a rough measure of what types of integers a form can represent. By looking at the forms of a fixed discriminant D, we can begin to introduce more sophisticated techniques to determine which primes a form can represent.

Definition 2.8. The discriminant of the binary quadratic form $ax^2 + bxy + cy^2$ is defined to be $D = b^2 - 4ac$. We may write $D(f)$ to represent the discriminant of the form f.

Remark 2.9. If the form $f(x, y) = ax^2 + bxy + cy^2$ has matrix $M = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, then the discriminant of the form is related to the matrix by $D = -4 \det M$. The discriminant of the form is also just the discriminant of the quadratic polynomial $ax^2 + bx + c$ obtained by setting $y = 1$.

Proposition 2.10. *The discriminant satisfies $D \equiv 0, 1 \pmod 4$, and any integer $N \equiv 0, 1 \pmod 4$ occurs as a discriminant.*

Proof. Looking at the definition of the discriminant $D = b^2 - 4ac$ modulo 4 gives $D \equiv b^2 \pmod 4$. We know the squares modulo 4 are $0, 1$, so $D \equiv 0, 1 \pmod 4$.

Now given $N \equiv 0, 1 \pmod 4$, we will write down a quadratic form with discriminant N. If $N \equiv 0 \pmod 4$, let $b = 0$, otherwise $N \equiv 1 \pmod 4$, so take $b = 1$. Then $N - b^2 \equiv 0 \pmod 4$, so write $N = b^2 - 4d$. Take $a = d$, and $c = 1$. Then by construction $ax^2 + bxy + cy^2 = dx^2 + bxy + y^2$ is a primitive (since $\gcd(a, b, c) = \gcd(d, 1) = 1$) integral binary quadratic form with discriminant $D = b^2 - 4ac = b^2 - 4d = N$. □

We will often refer to the discriminants $D \equiv 0 \pmod 4$ as the even discriminants, and the discriminants $D \equiv 1 \pmod 4$ as the odd discriminants, as would be expected.

The discriminant is a perfect square if and only if the binary quadratic form is reducible, that is it factors as the product of linear polynomials. Dividing the quadratic form $f(x, y)$ through by y^2 gives us a quadratic polynomial in $\frac{x}{y}$ with the same discriminant D. If this discriminant is a perfect square, the polynomial has rational roots, and so factors over $\mathbb{Z}$ by the Gauss Lemma. We can then multiple through by a y in each factor to get a factorisation of the original quadratic form.

If the form is reducible, the question of what primes the form represents can be dealt with much more easily than in general; to represent a prime p one of the factors must be 1 and the other must be p itself.

Primes Represented by Reducible Forms

i) What primes does the quadratic form $q(x, y) = x^2 - 4y^2$ represent? Since $q(x, y)$ has discriminant $D = 0^2 - 4 \cdot (-4) \cdot 1 = 16$, a perfect square, the form is reducible. We factor $q(x, y)$ as $q(x, y) = (x - 2y)(x + 2y)$. So if $q(x, y)$ represent the prime p, we must have (after flipping the sign of x or y as necessary), that:

$$\begin{cases} 1 = x + 2y \\ p = x - 2y \end{cases}$$

Solving these equations for x and y gives that:

$$\begin{cases} x = \frac{1}{2}(1 + p) \\ y = \frac{1}{4}(1 - p) \end{cases}$$

There is an integer solution if and only if $1 + p \equiv 0 \pmod 2$ and $1 - p \equiv 0 \pmod 4$. We can rewrite this as just $p \equiv 1 \pmod 4$. So a prime p is represented by $x^2 - 4y^2$ if and only if $p \equiv 1 \pmod 4$.

ii) What primes does the quadratic form $r(x, y) = 2x^2 - xy - 3y^2$ represent? Since $r(x, y)$ has discriminant $D = (-1)^2 - 4 \cdot 2 \cdot (-3) = 25$, a perfect square, the form is reducible. We can factor $r(x, y)$ as $r(x, y) = (x + y)(2x - 3y)$. So if $r(x, y)$ represents the prime p, we must have (after flipping the sign of x and y if necessary), that:

$$\begin{cases} 1 = x + y \\ p = 2x - 3y \end{cases} \text{ or } \begin{cases} 1 = 2x - 3y \\ p = x + y \end{cases}$$

Solving for x and y gives that:

$$\begin{cases} x = \frac{1}{5}(3 + p) \\ y = \frac{1}{5}(2 - p) \end{cases} \text{ or } \begin{cases} x = \frac{1}{5}(1 + 3p) \\ y = \frac{1}{5}(2p - 1) \end{cases}$$

There is an integer solution if and only if $3 + p \equiv 0 \pmod 5$ and $2 - p \equiv 0 \pmod 5$, or $1 + 3p \equiv 0 \pmod 5$ and $2p - 1 \equiv 0 \pmod 5$. These conditions are simply if and only if $p \equiv 2 \pmod 5$, or $p \equiv 3 \pmod 5$. So a prime p is represented by $r(x, y) = 2x^2 - xy - 3y^2$ if and only if $p \equiv 2, 3 \pmod 5$.

We can completely answer the question of which primes a reducible binary quadratic form represents, and so we may assume without loss of generality that the discriminant of a quadratic form is not a perfect square so the form is irreducible.

The sign of the discriminant identifies what types of integers the quadratic form can represent, and splits quadratic forms into two sets which behave very differently.

Definition 2.11. A quadratic form is called positive-definite if, other than 0, it only represents positive values; is called negative-definite if it only represents negative values; and is called indefinite if it represents both positive, and negative values.

Proposition 2.12. *The binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant D, with D non-square, is:*

i) positive-definite if $D < 0$, and $a > 0$;
ii) negative-definite if $D < 0$, and $a < 0$;
iii) indefinite if $D > 0$.

Proof. Since D is not a square, we know $a \neq 0$. Now we make use of the identity found in Flath [8, p. 56], which says:

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

If $D > 0$, the right hand side takes positive and negative values hence $f(x, y)$ is indefinite: at $x = 1, y = 0$ we get $f(1, 0) = a$, and at $x = -b, y = 2a$, we get $f(-b, 2a) = -Da$. If $D < 0$ then for any (x, y) sign of the right hand side corresponds to the sign of a, and hence $f(x, y)$ is positive- or negative-definite according to whether a is positive or negative. □

Since the primes of $\mathbb{Z}$ are by definition positive, no negative-definite form can represent a prime number, so we may exclude them from our investigation. Furthermore by negating a negative-definite form we obtain a corresponding positive-definite form which represents the corresponding positive integers, so we only need study positive-definite forms, rather than both positive- and negative-definite forms.

Often we will have to analyse the situation for positive-definite forms and indefinite forms separately since they have very disparate behaviour. We will see later that binary quadratic forms link to quadratic fields and their ideals, with the indefinite forms linking to the real quadratic fields. The presence of infinitely many units in real quadratic fields leads to them being less 'well-behaved' than imaginary quadratic fields, and this transfers to the binary quadratic forms.

2.3 Equivalence of Quadratic Forms

As with all mathematical objects, we want to define a notion of equivalence between binary quadratic forms. We want some way to identify that certain forms are for all intents and purposes the same. In particular we would intuitively like equivalent forms to have the same discriminant, and to represent the same integers.

Following Flath [8, pp. 56–58] we will define a group action of $\mathrm{SL}(2, \mathbb{Z})$ on the set of all binary quadratic forms, and use to this define the equivalence classes of forms as orbits under $\mathrm{SL}(2, \mathbb{Z})$.

Definition 2.13. For a form $f(x, y) = ax^2 + bxy + cy^2$, and a matrix $A = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$, we define the operation:

$$(A \cdot f)(x, y) = f(px + ry, qx + sy)$$

So in matrix notation, if the matrix of $f(x, y)$ is M, we have:

$$(A \cdot f)(x, y) = \begin{pmatrix} x & y \end{pmatrix} AMA^\top \begin{pmatrix} x \\ y \end{pmatrix}$$

Lemma 2.14. *The operation $A \cdot f$ above defines an action of* $\mathrm{SL}(2,\mathbb{Z})$ *on the set of all binary quadratic forms.*

Proof. We have $I \cdot f = f$, since $IMI^\top = M$. We also have $B \cdot (A \cdot f) = (BA) \cdot f$ since $B(AMA^\top)B^\top = (BA)M(BA)^\top$. □

From this and properties of a group action we can make the following definition of equivalence which is then automatically an equivalence relation:

Definition 2.15. Two forms $f(x,y)$ and $g(x,y)$ are said to be equivalent if there is $A \in \mathrm{SL}(2,\mathbb{Z})$ such that $A \cdot f = g$. The orbits under $\mathrm{SL}(2,\mathbb{Z})$ give the equivalence classes of forms, the classes of forms which are all equivalent.

Remark 2.16. On the set of binary quadratic forms there are at least *three* notions of equivalence, one defined by the above action of $\mathrm{SL}(2,\mathbb{Z})$, which is usually called proper equivalence; and another define by the obvious action of $\mathrm{GL}(2,\mathbb{Z})$ which is just called equivalence. As Zagier [29, p. 62] warns there is also a signed equivalence, where $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ acts by $\left(\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \cdot f\right)(x,y) = \det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) f(px + ry, qx + sy)$.

Signed equivalence is no good for our purposes since signed-equivalent forms don't represent the same integers. For example the forms $x^2 - 3y^2$ and $-x^2 + 3y^2$ are signed-equivalent via $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$. Since the fundamental unit of $\mathbb{Q}(\sqrt{3})$ is $u = 2 + \sqrt{3}$, of norm 1, the form $x^2 - 3y^2$ cannot represent -1, and yet clearly $-x^2 + 3y^2$ does. An even more blatant example occurs if we look at the forms $x^2 + y^2$ and $-x^2 - y^2$. They, too, are signed-equivalent via $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, yet one is positive definite and the other is negative definite! We do not want this.

Since $\mathrm{SL}(2,\mathbb{Z})$-equivalence has stronger links to quadratic number fields, it is the one we will make most use of and so when we speak of equivalence we will mean $\mathrm{SL}(2,\mathbb{Z})$-equivalence.

Let's look at some examples of equivalent forms, and see how the properties of a form behaves under equivalent.

Example 2.17. i) Consider the quadratic form $r(x,y) = x^2 + 2y^2$. As $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 7 & -3 \\ 5 & -2 \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, we can act by each of them to get a form equivalent to $r(x,y)$.

$$\begin{aligned}
\left(\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \cdot r\right)(x,y) &= r(2x+y, x+y) = (2x+y)^2 + 2(x+y)^2 = 6x^2 + 8xy + 3y^2 \\
\left(\left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right) \cdot r\right)(x,y) &= r(5x+3y, 3x+2y) = (5x+3y)^2 + 2(3x+2y)^2 = 43x^2 + 54xy + 17y^2 \\
\left(\left(\begin{smallmatrix} 7 & -3 \\ 5 & -2 \end{smallmatrix}\right) \cdot r\right)(x,y) &= r(7x+5y, -3x-2y) = (7x+5y)^2 + 2(-3x-2y)^2 = 67x^2 + 94xy + 33y^2
\end{aligned}$$

In each case the form seems to be getting more complicated, but it still retains some of the features of $r(x,y) = x^2 + 2y^2$. All of the equivalent forms are integral and primitive. Just before the final equality the forms are written in a way which shows they are positive definite, as is $r(x,y) = x^2 + 2y^2$. If we calculate the discriminants we get $D = 8^2 - 4 \cdot 6 \cdot 3 = 0^2 - 4 \cdot 1 \cdot 2 = -8$ in each case, which is the discriminant of $r(x,y) = x^2 + 2y^2$, the form that we started with.

ii) Now start with the form $s(x,y) = 2x^2 - 4y^2$, and act by the same matrices. We find the following forms are equivalent to $s(x,y)$:

$$\begin{aligned}
\left(\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \cdot s\right)(x,y) &= s(2x+y, x+y) = 2(2x+y)^2 - 4(x+y)^2 = 4x^2 - 2y^2 \\
\left(\left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right) \cdot s\right)(x,y) &= s(5x+3y, 3x+2y) = 2(5x+3y)^2 - 4(3x+2y)^2 = 14x^2 + 12xy + 2y^2 \\
\left(\left(\begin{smallmatrix} 7 & -3 \\ 5 & -2 \end{smallmatrix}\right) \cdot s\right)(x,y) &= s(7x+5y, -3x-2y) = 2(7x+5y)^2 - 4(-3x-2y)^2 = 62x^2 + 92xy + 34y^2
\end{aligned}$$

With the exception of the first result, the forms still seem to be getting increasingly more complicated. We can see that all of the forms are integral, and none are primitive. Just before

the final equality we see that each is indefinite, although it might not look it from the final result. Each form has discriminant $D = 0^2 - 4 \cdot 2 \cdot (-4) = 32$.

iii) If we start with a somewhat complicated form like $t(x, y) = 13x^2 - 42xy + 34y^2$, and act by a cleverly chosen matrix we can sometimes find a very simple equivalent form. Act by $\left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$, and after some calculation we find:

$$\begin{aligned} \left(\left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right) \cdot t\right)(x, y) &= t(5x + 3y, 3x + 2y) \\ &= 13(5x + 3y)^2 - 42(5x + 3y)(3x + 2y) + 34(3x + 2y)^2 \\ &= x^2 + y^2 \end{aligned}$$

So the form $t(x, y) = 13x^2 - 42xy + 34y^2$ is equivalent to simply the sum of two squares $x^2 + y^2$.

As we might notice in the example above, this equivalence behaves as we would like with respect to being primitive, being integral, the discriminant, and representing integers. We may then group the equivalent forms together and just study a representation of each equivalence class. Specifically we have the following easy results:

Proposition 2.18. *If $f(x, y)$ is integral, then so is any equivalent form.*

Proof. Expanding out the result of the definition $(A \cdot f)(x, y)$, for $A \in \mathrm{SL}(2, \mathbb{Z})$, involves only multiplication and addition of integers, this means integer coefficients remain integers. □

Proposition 2.19. *Equivalent forms have the same discriminant.*

Proof. From the matrix point of view, if the form $f(x, y)$ has matrix M, and we act by $A \in \mathrm{SL}(2, \mathbb{Z})$ to get an equivalent form, then the discriminant of $(A \cdot f)(x, y)$ is given by:

$$D(A \cdot f) = -4 \det(AMA^\top) = -4 \det(A)^2 \det(M) = -4 \det(M) = D(f)$$

since $A \in \mathrm{SL}(2, \mathbb{Z})$ has $\det(A) = 1$. □

Proposition 2.20. *Equivalent integral forms represent the same integers.*

Proof. We only need to show that if $f(x, y)$ represents an integer, then so does $(A \cdot f)(x, y)$, for any $A \in \mathrm{SL}(2, \mathbb{Z})$. If the form $f(x, y)$, with matrix M, represents the integer m, write $m = f(x_0, y_0)$. Now consider $(A \cdot f)(x_1, y_1)$, where:

$$\begin{pmatrix} x_1 & y_1 \end{pmatrix} = \begin{pmatrix} x_0 & y_0 \end{pmatrix} A^{-1}$$

Since $A \in \mathrm{SL}(2, \mathbb{Z})$, we know $A^{-1} \in \mathrm{SL}(2, \mathbb{Z})$, hence A^{-1} has integer entries, and $x_1, y_1 \in \mathbb{Z}$. Then we have by straight-forward calculation:

$$\begin{aligned} (A \cdot f)(x_1, y_1) &= \begin{pmatrix} x_1 & y_1 \end{pmatrix} AMA^\top \begin{pmatrix} x_1 & y_1 \end{pmatrix}^\top \\ &= \begin{pmatrix} x_0 & y_0 \end{pmatrix} A^{-1} AMA^\top \left(\begin{pmatrix} x_0 & y_0 \end{pmatrix} A^{-1}\right)^\top \\ &= \begin{pmatrix} x_0 & y_0 \end{pmatrix} A^{-1} AMA^\top (A^\top)^{-1} \begin{pmatrix} x_0 & y_0 \end{pmatrix}^\top \\ &= \begin{pmatrix} x_0 & y_0 \end{pmatrix} M \begin{pmatrix} x_0 & y_0 \end{pmatrix}^\top \\ &= f(x_0, y_0) \\ &= m \end{aligned}$$

So $(A \cdot f)(x, y)$ also represents m. □

Corollary 2.21. *Equivalent forms are both either positive-definite, negative-definite, or indefinite.*

Proof. They represent the same integers. □

Proposition 2.22. *If $f(x, y)$ is primitive, then so is any equivalent form.*

Proof. The statement here is $f(x, y)$ is primitive implies $(A \cdot f)(x, y)$ is primitive. An equivalent statement is given by the contrapositive: $(A \cdot f)(x, y)$ is not primitive implies $f(x, y)$ is not primitive. We prove the contrapositive.

Let $f(x, y) = ax^2 + bxy + cy^2$. Suppose the gcd of the coefficients of $(A \cdot f)(x, y)$ is $d > 1$, then any integer which $(A \cdot f)(x, y)$ represents is divisible by d. Since $f(x, y)$ and $(A \cdot f)(x, y)$ are equivalent they represent the same integers, in particular they both represent $f(1, 0) = a$, $f(0, 1) = c$, and $f(1, 1) = a + b + c$. This tell us that $d \mid a, c, a + b + c$, and so $d \mid a, b, c$, which precisely means $f(x, y)$ is not primitive. □

With these results we can make some headway in identifying which forms are equivalent, and which aren't.

Example 2.23. Which of the forms $r(x, y) = x^2 + 5y^2$, $s(x, y) = 2x^2 + 2xy + 3y^2$, $t(x, y) = 2x^2 - 2xy + 3y^2$, $u(x, y) = x^2 - 5y^2$, $v(x, y) = 2x^2 + 4y^2$ are equivalent?

We see straight away that $v(x, y)$ is the only non-primitive form, and so can't be equivalent to any others. Now we calculate the discriminant of each form $D(r) = D(s) = D(t) = -20$, and $D(u) = 20$. We then get that $u(x, y)$ is not equivalent to any other form in the list.

Now let us look at what integers the remaining forms represent. By changing the sign of x we see that both $s(x, y)$ and $t(x, y)$ represent the same integers, so we can't distinguish them this way, and so this suggests they might be equivalent. However we know $r(x, y)$ doesn't represent 2 or 3, whereas $s(x, y)$ and $t(x, y)$ do. So $r(x, y)$ is not equivalent to any other forms.

We are left with possibly $s(x, y)$ and $t(x, y)$ being equivalent. A pair of forms like this is of course equivalent under $\mathrm{GL}(2, \mathbb{Z})$, by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which changes the sign of x, but we want to know whether they are equivalent under $\mathrm{SL}(2, \mathbb{Z})$. It turns out that $\left(\begin{smallmatrix} -1 & 0 \\ -1 & -1 \end{smallmatrix}\right)$ transforms $t(x, y)$ into $s(x, y)$ so they are equivalent, although where this matrix comes from is not clear.

The question of whether two arbitrary quadratic forms are equivalent can be answered in a purely algorithmic manner, and is tied closely to the theory of reduced forms, and the finiteness of the number of equivalence classes of forms. It is to that we now turn.

2.4 Finiteness of the Class Number

Definition 2.24. The class number of a discriminant D is the number of equivalence classes of primitive integral binary quadratic forms of discriminant D. In the positive-definite case we may denote this by $h(D)$, and in general by $h^+(D)$ in order to match up with the corresponding notions in quadratic fields.

The goal of this section is to establish $h(D)$ and $h^+(D)$ are finite, and show how to effectively calculate it and list a representative of each equivalence class. We must treat the positive-definite and indefinite forms separately. We will work from Cohen [4].

2.4.1 Positive-Definite Forms

Section 5.4.1 of Cohen [4, pp. 231–234] deals with the positive definite case. Following Gauss and Cohen [4] we will define a reduced form, and establish that every equivalence class of forms of discriminant $D < 0$ contains a unique reduced form.

Definition 2.25. A primitive positive-definite integral quadratic form $ax^2 + bxy + cy^2$ of discriminant $D < 0$ is said to be reduced if $|b| \leq a \leq c$, and if when one of the two inequalities is an equality, either $|b| = a$ or $a = c$, then $b \geq 0$.

Proposition 5.3.3 in Cohen [4, pp. 231–232] gives us:

Proposition 2.26. *In every class of positive definite quadratic forms of discriminant $D < 0$ there is a unique reduced form.*

Proof. We follow the proof given in Cohen [4, p. 232].

We show each class contains a reduced form. Since the form is positive-definite we know $a > 0$, hence by the well-ordering principal, in any equivalence class there is a form with minimal a. If $ax^2 + bxy + cy^2$ is such a form, then $a \leq c$, since otherwise $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ sending $x \mapsto -y$ and $y \mapsto x$ changes $ax^2 + bxy + cy^2$ into $cx^2 - bxy + ay^2$ and would produce a smaller 'a'.

By acting with $\left(\begin{smallmatrix} 1 & 0 \\ k & 1 \end{smallmatrix}\right)$ sending $x \mapsto x + ky$ and $y \mapsto y$ we transform the form $ax^2 + bxy + cy^2$ into $ax^2 + (2ak + b)xy + (ak^2 + bk + c)y^2$. Hence we can put '$b$' into the range $(-a, a]$. Since a is minimal we still have $a \leq c$, and we now have $-a < b \leq a$, so $|b| \leq a$. Now we need to check whether the edge cases are are satisfied: by construction if $|b| = a$ then $b = a > 0$, and if $a = c$ with $b < 0$ then transforming by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ sending $x \mapsto -y$ and $y \mapsto x$ changes $ax^2 + bxy + cy^2$ into $cx^2 - bxy + ay^2$ with 'a' $\leq$ 'c' and 'b' > 0.

Cohen then goes on to prove this reduced form is unique. We do not need uniqueness in order to establish the class number is finite. □

Essentially the same proof appears in Flath [8, p. 58, Prop. 8.3], but Flath applies the two transformations $S := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and $T^k := \left(\begin{smallmatrix} 1 & 0 \\ k & 1 \end{smallmatrix}\right)$ alternately to an arbitrary (primitive) integral positive definite binary quadratic form. This forms a reduction operator leading to a sequence of equivalent forms which eventually terminates in a (nearly) reduced form. The procedure terminates in a reduced form or stops one step away, needing the final transformation $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ to make the form reduced.

This leads to an algorithm for determining whether two primitive positive-definite binary quadratic forms are equivalent. Apply the reduction procedure and produce a reduced form equivalent to each form. If the reduced forms are the same the forms are equivalent, otherwise the reduced forms are different and the forms are not equivalent.

Example 2.27. Are the forms $s(x, y) = 242x^2 + 300xy + 93y^2$ and $r(x, y) = 605x^2 + 184xy + 14y^2$ equivalent? We can see that these forms are both primitive and positive-definite. We apply the

reduction:

$$\begin{aligned}
s(x,y) &= 242x^2 + 300xy + 93y^2\text{; as } c < a \text{ apply } S \\
(S\cdot s)(x,y) &= 93x^2 - 300xy + 242y^2\text{; apply } T^2 \text{ to put } b \text{ in } (-93, 93] \\
(T^2S\cdot s)(x,y) &= 93x^2 + 72xy + 14y^2\text{; as } c < a \text{ apply } S \\
(ST^2S\cdot s)(x,y) &= 14x^2 - 72xy + 93y^2\text{; apply } T^3 \text{ to put } b \text{ in } (-14, 14] \\
(T^3ST^2S\cdot s)(x,y) &= 14x^2 + 12xy + 3y^2\text{; as } c < a \text{ apply } S \\
(ST^3ST^2S\cdot s)(x,y) &= 3x^2 + 12xy + 14y^2\text{; apply } T^2 \text{ to put } b \text{ in } (-3, 3] \\
(T^2ST^3ST^2S\cdot s)(x,y) &= 3x^2 + 2y^2\text{; as } c < a \text{ apply } S \\
(ST^2ST^3ST^2S\cdot s)(x,y) &= 2x^2 + 3y^2\text{; this is a reduced form so terminate}
\end{aligned}$$

Keeping track of the transformations we applied we see that $A \coloneqq ST^2ST^3ST^2S = \left(\begin{smallmatrix} -5 & 8 \\ 3 & -5 \end{smallmatrix}\right)$ transforms $s(x,y)$ into the reduced form $2x^2 + 3y^2$.

A similar computation shows that $B \coloneqq ST^2ST^7S = \left(\begin{smallmatrix} -2 & 13 \\ 1 & -7 \end{smallmatrix}\right)$ transforms $t(x,y)$ into the reduced form $2x^2 + 3y^2$.

Since they are both equivalent to the same reduced form we know the forms $s(x,y)$ and $t(x,y)$ are equivalent themselves. Moreover we have found a matrix which transforms one into the other: $B^{-1}A = \left(\begin{smallmatrix} -4 & 9 \\ -1 & 2 \end{smallmatrix}\right)$ first transforms $s(x,y)$ into $2x^2 + 3y^2$, and then transforms this into $r(x,y)$, so overall transforms $s(x,y)$ into $r(x,y)$.

Remark 2.28. As Cohen [4, p. 232] remarks before the proof of Proposition 5.3.3, the proposition and reduction procedure is equivalent to proving that $\mathcal{F} = \left\{\tau \in \mathbb{H} \mid -\frac{1}{2} \leq \operatorname{Re}\tau \leq \frac{1}{2} \text{ and } |\tau| \geq 1\right\}$ is a fundamental domain for the standard action of $\mathrm{SL}(2,\mathbb{Z})$ on the upper half plane $\mathbb{H}$, and to finding a representative in $\mathcal{F}$ for the number $\tau = \frac{-b+\sqrt{D}}{2a}$.

Returning to our goal of proving the class number is finite, we equivalently have to prove there are only finitely many reduced forms of a given discriminant. Lemma 5.3.4 from Cohen [4] gives us the following bounds:

Proposition 2.29. *Let $f(x,y) = ax^2 + bxy + cy^2$ be a reduced primitive positive-definite binary quadratic form of discriminant $D < 0$. Then:*

$$a \leq \sqrt{\frac{-D}{3}}$$

Proof. As $f(x,y)$ is reduced, we know $c \geq a \geq |b|$, so $a^2 \geq b^2$ or $-b^2 \geq -a^2$ and we find:

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$$

This implies $a \leq \sqrt{\frac{-D}{3}}$ as required. □

We have thus established an upper bound on a in a reduced form of discriminant $D < 0$, and this gives a bound on b using $|b| \leq a$. In particular there are only finitely many possible a and b. We can then calculate c via $c = \frac{b^2-D}{4a}$ in order to list the reduced forms. An immediate corollary of this is:

Corollary 2.30. *For a given discriminant $D < 0$, the class number $h(D)$ is finite.*

Proof. Since there is a unique reduced form in each equivalence class, the class number equals the number of reduced forms, and we have shown this is finite. □

We also get an algorithm to list a representative of each equivalence class, it is simply to compute the list of reduced forms.

Example 2.31. What are the binary quadratic forms of discriminant $D = -20$?

We start finding the bounds on each of a and b. Since $D = -20$, we know from the result above that:

$$0 < a \leq \sqrt{\frac{20}{3}} = 2.5818\ldots$$

Since a is an integer, we must have $a = 1$ or $a = 2$. We also have $|b| \leq a$ and can determine $c = \frac{b^2 - D}{4a}$. So we can check through all possibilities:

a	b	c	Reduced?
1	-1	$\frac{21}{4}$	
1	0	5	Yes
1	1	$\frac{21}{4}$	
2	-2	3	
2	-1	$\frac{21}{8}$	
2	0	$\frac{20}{8}$	
2	1	$\frac{21}{8}$	
2	2	3	Yes

Notice: $2x^2 - 2xy + 3y^2$ is not reduced since $|b| = a$, but $b < 0$. From this table we read off that there are two classes of quadratic forms of discriminant $D = -20$, namely $x^2 + 5y^2$, and $2x^2 + 2xy + 3y^2$. This means that class number of $D = -20$ is $h(-20) = 2$.

The algorithm used here can easily be implemented on a computer, and as Cohen [4, p. 233] states has a runtime of only a few seconds even for discriminants up to $D = -10^6$. Since we now have a method to compute the class number of discriminant $D < 0$, and list a representative of each class, we won't bother manually calculating these in future, but simply state the final results.

2.4.2 Indefinite Forms

In the indefinite case there is a corresponding notion of a reduced form, and every binary quadratic form is equivalent to some non-unique reduced form. It is possible for reduced forms here to be equivalent among themselves.

Heeding Exercise 7i) from Section 2.8 in Flath [8, p. 61], we can imitate the proof of Proposition 2.26 to get the following proposition:

Proposition 2.32. *Every primitive integral indefinite form of discriminant $D > 0$, D non-square is equivalent to one of the form $ax^2 + bxy + cy^2$ such that $|b| \leq |a| \leq |c|$. Such a form has $ac < 0$, and $|a| \leq \frac{1}{2}\sqrt{D}$.*

Proof. By the well-ordering principal, in any equivalence class there is a form with minimal $|a|$. If $ax^2 + bxy + cy^2$ is such a form, then $|a| \leq |c|$, otherwise transforming by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ gives the equivalent form $cx^2 - bxy + ay^2$, with a smaller '$|a|$'.

Now transforming by $\left(\begin{smallmatrix} 1 & 0 \\ k & 1 \end{smallmatrix}\right)$, which changes the coefficient b to $2ak + b$, we can put 'b' in the range $(-|a|, |a|]$. Since $|a|$ is minimal, we still have $|a| \leq |c|$, and we now have $|b| \leq |a|$, which is the required result.

Given a form satisfying these conditions, we have $b^2 = |b|^2 \leq |a|\,|c| = |ac|$, and by definition $D = b^2 - 4ac > 0$, so $4ac < b^2$. Putting these together gives:

$$4ac < b^2 \leq |ac|$$

This shows we must have $ac < 0$, as otherwise $|ac| = ac$, and we get the contradiction $4ac < ac$. Knowing $ac < 0$, we have $|ac| = -ac$, so $D = b^2 - 4ac = b^2 + 4\,|ac| > 0$. This implies $4\,|ac| = D - b^2 \leq D$. Since we have $|a| \leq |c|$ we get $|a|^2 \leq |ac|$, so:

$$|a|^2 \leq |ac| \leq \frac{1}{4}D^2$$

which implies $|a| \leq \frac{1}{2}\sqrt{D}$. □

This in itself is sufficient to prove that the class number is finite in the indefinite case, and so we get the corollary:

Corollary 2.33. *For a given discriminant $D > 0$, D non-square, the class number $h^+(D)$ is finite.*

Proof. Every equivalence class contains a form $ax^2 + bxy + cy^2$, with $|b| \leq |a| \leq |c|$. We have shown such a form has $|a| \leq \frac{1}{2}\sqrt{D}$, so $|b| \leq |a| \leq \frac{1}{2}\sqrt{D}$ and there are finitely many possibilities for a and b. This means there are finitely many such forms, and hence finitely many equivalence classes. □

We do not necessarily have that each class contains exactly one such form, so this does not allow us to calculate the class number. In order to calculate the class number we need to study the situation more carefully. Cohen has done so, and so we state the relevant results for this section and refer the reader to Section 5.6.1 in Cohen [4, pp. 262–266] for the details.

Definition 2.34. A primtive integral indefinite binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant $D > 0$ is called reduced if we have:

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

Proposition 2.35. *A reduced indefinite form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant $D > 0$ has $|a|, b, |c| < \sqrt{D}$, and $ac < 0$.*

Definition 2.36. Let $f(x, y) = ax^2 + bxy + cy^2$ be an indefinite quadratic form of discriminant $D > 0$. We define the reduction operator ρ on the form $f(x, y)$ to be the form:

$$(\rho f)(x, y) = cx^2 + r(-b, c)xy + \frac{r(-b, c)^2 - D}{4c}y^2$$

where $r(b, a)$ is the unique integer $r \equiv b \pmod{2a}$ such that:

$$\begin{cases} -|a| < r \leq |a| & \text{if } |a| > \sqrt{D} \\ \sqrt{D} - 2\,|a| < r < \sqrt{D} & \text{if } |a| < \sqrt{D} \end{cases}$$

The main result here is give in Proposition 5.6.6 of Cohen [4, p. 264] which states roughly that:

Proposition 2.37. *i) Iterating ρ on an indefinite form of discriminant $D > 0$ eventually produces a reduced form;*

ii) If $f(x, y)$ is a reduced form, then $(\rho f)(x, y)$ is again a reduced form;

iii) The reduced forms equivalent to $f(x,y)$ are exactly the reduced forms given by iterating ρ on $f(x,y)$.

Using this we can determine the class number by listing the finite number of reduced forms and counting the number of cycles they break up into under ρ. Again this can be implemented as a computer algorithm, and so we need not manually calculate class numbers or representatives for the equivalence classes in future.

Example 2.38. What are the quadratic forms of discriminant $D = 105$?

Let $ax^2 + bxy + cy^2$ be a reduced form of discriminant $D = 105$. We have the following bounds on a and b:

$$|a| < \sqrt{D} = \sqrt{105} = 10.24695\ldots$$
$$\left|\sqrt{D} - 2\,|a|\right| < b < \sqrt{D}$$

So $-10 \leq a \leq 10$. We then calculate c by $c = \frac{b^2-D}{4a}$.

We simply go through listing all possibilities, and check whether we get an integer c, and coprime coefficients. Only those a and b which give integer c are listed below to save space.

a	b	c	a	b	c
-7	7	2	1	9	-6
-6	3	4	2	9	-3
-6	9	1	2	7	-7
-5	5	4	3	9	-2
-4	3	6	4	5	-5
-4	5	5	4	3	-6
-3	9	2	5	5	-4
-2	7	7	6	9	-1
-2	9	3	6	3	-4
-1	9	6	7	7	-2

Now we need to see which forms are in the same orbit under the reduction operator ρ.

Let's start with $-7x^2+7xy+2y^2$. We calculate $r(-b,c) = r(-7,2) = 9$. This is because we need $r \equiv -7 \pmod{2\cdot 2}$, so $r \equiv 1 \pmod 4$. And we need to choose r such that $\sqrt{105} - 2\,|2| < r < \sqrt{105}$, since $|2| \leq \sqrt{D}$. This means $7 \leq r \leq 10$, and so we take $r = 9$.

Applying the reduction operator gives us the form:

$$\begin{aligned}\rho(-7x^2 + 7xy + 2y^2) &= 2x^2 + 9xy + \frac{9^2 - 105}{4\cdot 2}y^2 \\ &= 2x^2 + 9xy - 3y^2\end{aligned}$$

Iterating this operation gives us the cycle of forms:

$$-7x^2 + 7xy + 2y^2 \mapsto 2x^2 + 9xy - 3y^2 \mapsto -3y^2 + 9xy + 2y^2 \mapsto$$
$$2x^2 + 7xy - 7y^2 \mapsto -7x^2 + 7xy + 2y2$$

The next form still on the list is $-6x^2 + 3xy + 4y^2$. We calculate $r(-b,c) = r(-3,4) = 5$. This is because we need $r \equiv -3 \pmod{2\cdot 4}$, so $r \equiv 5 \pmod 8$. And we need to choose r such that $\sqrt{105} - 2\,|4| < r < \sqrt{105}$, since $|4| \leq \sqrt{D}$. This means $3 \leq r \leq 10$, and so we take $r = 5$.

Applying the reduction operator gives us the form:

$$\begin{aligned}\rho(-6x^2+3xy+4y^2) &= 4x^2+5xy+\frac{5^2-105}{4\cdot 4}y^2\\ &= 4x^2+5xy-5y^2\end{aligned}$$

Iterating this operation gives us the cycle of forms:

$$-6x^2+3xy+4y^2 \mapsto 4x^2+5xy-5y^2 \mapsto -5x^2+5xy+4y^2 \mapsto 4x^2+3xy-6y^2 \mapsto$$
$$-6x^2+9xy+y^2 \mapsto y^2+9xy-6y^2 \mapsto -6x^2+3xy+4y^2$$

Similarly we get the cycles:

$$-4x^2+3xy+6y^2 \mapsto 6x^2+9xy-y^2 \mapsto -x^2+9xy+6y^2 \mapsto 6x^2+3xy-4y^2 \mapsto$$
$$-4x^2+5xy+y^2 \mapsto 5x^2+5xy-4y^2 \mapsto -4x^2+3xy+6y^2$$

and

$$-2x^2+7xy+7y^2 \mapsto 7x^2+7xy-2y^2 \mapsto -2x^2+9xy+3y^2 \mapsto$$
$$3x^2+9xy-2y^2 \mapsto -2x^2+7xy+7y^2$$

This tells us that there are 4 equivalence classes of binary quadratic forms of discriminant $D=105$, so the class number is $h^+(105)=4$. By taking one form from each cycle we find that a representative of each class is: $-7x^2+7xy+2y^2$, $-6x^2+3xy+4y^2$, $-4x^2+3xy+6y^2$, and $-2x^2+7xy+7y^2$.

Implementations of the algorithms above to calculate the number of equivalence classes of quadratic forms and to produce a representative of each class are available online courtesy of Matthews [19].

2.5 The Correspondence Between Forms and Ideals

We now explore the link between quadratic forms and quadratic fields. We will use class field theory to investigate ideals in quadratic fields and properties of the class number, this link will then allow us to deduce results on the quadratic forms side. We have already seen that the norm on the integers of $K=\mathbb{Q}(\sqrt{d})$ gives rise to a quadratic form, the norm form, given by:

$$N(x+y\tfrac{1+\sqrt{d}}{2}) = x^2+xy+\tfrac{1-d}{4}y^2 \text{ if } d\equiv 1 \pmod 4$$
$$N(x+y\sqrt{d}) = x^2-dy^2 \text{ if } d\not\equiv 1 \pmod 4$$

The discriminant of both of these forms matches up with the discriminant of the number field K.

Definition 2.39. A discriminant D which occurs as the discriminant of a quadratic number field K is called a fundamental discriminant

An positive integer m is represented by the norm form if and only if there is some element $\alpha\in\mathcal{O}_K$ with norm $N(\alpha)=m$. The ideal (α) is then a totally positive principal ideal of norm $|m|=m$. Conversely if there is a totally positive principal ideal of norm m, then it is generated by some α with $N(\alpha)=m>0$. So m is represented by the norm form if and only if there is a totally positive principal ideal of norm m. Since the norm forms correspond to totally positive principal ideals they are also called the principal forms.

Following Section 7.2 of Fröhlich and Taylor [10, pp. 254–269], we will generalise the construction of the norm form above to construct other quadratic forms of discriminant Δ_K, and relate the representations of an integer to the existence of a particular ideal with the corresponding norm. We can treat the positive-definite and the indefinite case simultaneously since the narrow class group of an imaginary quadratic field is just the usual class group.

Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$. Theorem 5.9 in Stewart and Tall [25, pp. 115–116] tells us that $\mathfrak{a}$ has a $\mathbb{Z}$-basis of the form $\{\alpha_1, \alpha_2\}$, and gives the norm of the ideal as:

$$N(\mathfrak{a}) = \left| \frac{\Delta_K(\alpha_1, \alpha_2)}{\Delta_K} \right|^{1/2}$$

Everything extends multiplicatively to a fractional ideal $\lambda\mathfrak{a}$, which has $\mathbb{Z}$-basis $\{\lambda\alpha_1, \lambda\alpha_2\}$, with the same result. So take $\mathfrak{a}$ to be a fractional $\mathcal{O}_K$-ideal, with $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$.

By definition $\Delta_K(\alpha_1, \alpha_2) = \det \left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{smallmatrix} \right)^2$, where $\sim$ is the non-trivial automorphism of K. The above result tell us that:

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{pmatrix}^2 = N(\mathfrak{a})^2 \Delta_K$$

Call the ordered basis $\{\alpha_1, \alpha_2\}$ normalised when:

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{pmatrix} = N(\mathfrak{a}) \sqrt{\Delta_K}$$

where $\sqrt{\Delta_K}$ is the principal branch of the square root, $\sqrt{\Delta_K} > 0$ when $\Delta_K > 0$, and $\operatorname{Im} \sqrt{\Delta_K} > 0$ when $\Delta_K < 0$. Since the determinant changes sign when interchanging columns, exactly one of the ordered bases $\{\alpha_1, \alpha_2\}$ or $\{\alpha_2, \alpha_1\}$ is normalised.

Given a normalised basis $\{\alpha_1, \alpha_2\}$ of $\mathfrak{a}$, define the quadratic form:

$$Q_{\alpha_1, \alpha_2}(x, y) = \frac{N(\alpha_1 x + \alpha_2 y)}{N(\mathfrak{a})}$$

Proposition 2.40. *The quadratic form $Q_{\alpha_1,\alpha_2}(x, y)$ is a primitive integral quadratic form of discriminant Δ_K, positive definite if $\Delta_K < 0$.*

Proof. To see $Q_{\alpha_1,\alpha_2}(x, y)$ is integral we check the coefficients are in $\mathbb{Z}$. By multiplying up by $\lambda \in K^*$ we can assume $\alpha_1, \alpha_2 \in \mathcal{O}_K$, and $\mathfrak{a}$ is an integral ideal. Then for any $x, y \in \mathbb{Z}$, the linear combination $x\alpha_1 + y\alpha_2$ is in $\mathfrak{a}$. If $b \in \mathfrak{a}$, then $(b) \subset \mathfrak{a}$, and so $\mathfrak{a} \mid (b)$. Taking norms shows that $N(\mathfrak{a}) \mid N((b))$, so $N(\mathfrak{a}) \mid N(b)$.

The coefficient of x^2 in the form is given by $a = Q_{\alpha_1,\alpha_2}(1, 0)$, which is an integer by the above. Similarly the coefficient of y^2 is given by $c = Q_{\alpha_1,\alpha_2}(0, 1)$, and so is also an integer. The sum of the coefficients is given by the integer $Q_{\alpha_1,\alpha_2}(1, 1)$, hence the coefficient of xy is given by $b = Q_{\alpha_1,\alpha_2}(1, 1) - a - c$, and is also an integer.

Writing out the quadratic form $Q_{\alpha_1,\alpha_2}(x, y)$ in full as Fröhlich and Taylor [10, p. 260–261] do we find:

$$\begin{aligned} Q_{\alpha_1,\alpha_2}(x, y) &= \frac{N(\alpha_1 x + \alpha_2 y)}{N(\mathfrak{a})} \\ &= \frac{1}{N(\mathfrak{a})} (\alpha_1 x + \alpha_2 y)(\widetilde{\alpha_1} x + \widetilde{\alpha_2} y) \\ &= \frac{1}{N(\mathfrak{a})} (\alpha_1 \widetilde{\alpha_1} x^2 + (\alpha_1 \widetilde{\alpha_2} + \alpha_2 \widetilde{\alpha_1}) xy + \alpha_2 \widetilde{\alpha_2} y^2) \end{aligned}$$

So the discriminant of $Q_{\alpha_1,\alpha_2}(x,y)$ is given by:

$$\begin{aligned} D &= \frac{1}{N(\mathfrak{a})^2}[(\alpha_1\widetilde{\alpha_2}+\alpha_2\widetilde{\alpha_1})^2 - 4\alpha_1\widetilde{\alpha_1}\alpha_2\widetilde{\alpha_2}] \\ &= \frac{1}{N(\mathfrak{a})^2}(\alpha_1\widetilde{\alpha_2}-\alpha_2\widetilde{\alpha_1})^2 \\ &= \frac{1}{N(\mathfrak{a})^2}\det\begin{pmatrix}\alpha_1 & \alpha_2\\ \widetilde{\alpha_1} & \widetilde{\alpha_2}\end{pmatrix}^2 \\ &= \Delta_K \end{aligned}$$

If $\Delta_K < 0$, then the coefficient of x^2 is $a = Q_{\alpha_1,\alpha_2}(1,0) = N(\alpha_1)/N(\mathfrak{a}) > 0$, so the form is positive-definite.

Lastly we check the form is primitive. Proceeding as in Result 2.12 of Fröhlich and Taylor [10, pp. 256–259], we show any form of discriminant Δ_K is primitive. As d is square-free, if $d \equiv 1 \pmod 4$, then $\Delta_K = d$, no square can divide Δ_K, and so the coefficients have no common factor. If $d \not\equiv 1 \pmod 4$, then $\Delta_K = 4d$, and so the only square dividing Δ_K is 2. If the form is not primitive then the only possibility is $\gcd(a,b,c) = 2$. However, then we have:

$$d = \frac{\Delta_K}{4} = \left(\frac{b}{2}\right)^2 - 4\frac{a}{2}\frac{c}{2} \equiv \left(\frac{b}{2}\right)^2$$

This means $d \equiv 0, 1 \pmod 4$, but we took $d \not\equiv 1 \pmod 4$, and d is square-free, so $d \not\equiv 0 \pmod 4$. Hence $\gcd(a,b,c) = 1$, and the form is primitive. □

Example 2.41. i) Consider the field $K = \mathbb{Q}(\sqrt{-5})$, and the ideals $\mathcal{O}_K = [1, -\sqrt{-5}]$, $\mathfrak{p}_3 = [3, 1+\sqrt{-5}]$, of norm 1 and 3 respectively. We check that the indicated bases are normalised:

$$\det\begin{vmatrix}1 & -\sqrt{-5}\\ 1 & \sqrt{-5}\end{vmatrix}^2 = 2\sqrt{-5} = N(\mathcal{O}_K)\sqrt{-4\cdot 5}$$

$$\det\begin{vmatrix}3 & 1-\sqrt{-5}\\ 3 & 1+\sqrt{-5}\end{vmatrix}^2 = 6\sqrt{-5} = N(\mathfrak{p}_3)\sqrt{-4\cdot 53}$$

The corresponding forms are:

$$Q_{1,-\sqrt{-5}} = \frac{1}{N(\mathcal{O}_K)}N(1x - \sqrt{-5}y) = x^2 + 5y^2$$

and

$$\begin{aligned} Q_{3,1-\sqrt{-5}} &= \frac{1}{N(\mathfrak{p}_3)}N(3x + (1-\sqrt{-5})y) \\ &= \frac{1}{3}N((3x+y) - \sqrt{-5}y) \\ &= \frac{1}{3}((3x+y)^2 + 5y^2) \\ &= \frac{1}{3}(9x^2 + 6xy + 6y^2) \\ &= 3x^2 + 2xy + 2y^2 \end{aligned}$$

ii) Now look at $K = \mathbb{Q}(\sqrt{10})$, and the ideals $\mathcal{O}_K = [1, -\sqrt{10}]$, $\mathfrak{p}_2 = [2, -\sqrt{10}]$ of norm 1 and 2 respectively. The indicated bases are normalised and so we compute the corresponding forms:

$$Q_{1,-\sqrt{10}} = \frac{1}{N(\mathcal{O}_K)}N(x - \sqrt{10}y) = x^2 - 10y^2$$

and

$$\begin{aligned} Q_{2,\sqrt{10}} &= \frac{1}{N(\mathfrak{p}_2)} N(2x - \sqrt{10}y) \\ &= \frac{1}{2}(4x^2 - 10y^2) \\ &= 2x^2 - 5y^2 \end{aligned}$$

How do the forms change when we use a different normalised basis?

Proposition 2.42. *If $\{\beta_1, \beta_2\}$ is another normalised basis of the ideal $\mathfrak{a}$, then the forms Q_{α_1,α_2} and Q_{β_1,β_2} are equivalent.*

Proof. As Fröhlich and Taylor [10, p. 261] observe, since both of these are $\mathbb{Z}$-bases for $\mathfrak{a}$, we can write:

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

where the change of basis matrix is invertible, and has integer entries. The inverse of the matrix is the change of basis matrix going in the other direction, so it too has integer entries. Hence $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$.

Taking the conjugate of this change of basis relation and combining with the above gives the relation:

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

Since both bases are normalised, and the determinant is invariant under transposition, taking the determinant of both sides gives:

$$N(\mathfrak{a})\sqrt{\Delta_K} = \det \begin{pmatrix} p & q \\ r & s \end{pmatrix} N(\mathfrak{a})\sqrt{\Delta_K}$$

so in fact $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$.

Now we have:

$$\begin{aligned} Q_{\beta_1,\beta_2}(x, y) &= \frac{1}{N(\mathfrak{a})} N(\beta_1 x + \beta_2 y) \\ &= \frac{1}{N(\mathfrak{a})} N((p\alpha_1 + q\alpha_2)x + (r\alpha_1 + s\alpha_2)y) \\ &= \frac{1}{N(\mathfrak{a})} N((px + ry)\alpha_1 + (qx + sy)\alpha_2) \\ &= Q_{\alpha_1,\alpha_2}(px + ry, qx + sy) \\ &= \left(\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \cdot Q_{\alpha_1,\alpha_2}\right)(x, y) \end{aligned}$$

So the two forms are equivalent. □

How do the forms relate when we look at equivalent ideals?

Proposition 2.43. *If $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent ideals in the narrow class group, then the forms arising from any normalised bases of $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent.*

Proof. If $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent in the narrow class group, then $\mathfrak{a}\mathfrak{b}^{-1} = (\lambda)$, for some totally positive principal ideal (λ), so equivalently $\mathfrak{a} = (\lambda)\mathfrak{b}$. Let $\{\beta_1, \beta_2\}$ be a normalised basis for $\mathfrak{b}$, then

a basis for $\mathfrak{a}$ is given by $\{\lambda\beta_1, \lambda\beta_2\}$. Fröhlich and Taylor [10, p. 261] note that since (λ) is totally positive, $N(\lambda) > 0$, so the latter basis is also normalised:

$$\begin{aligned}\begin{vmatrix}\lambda\beta_1 & \lambda\beta_2 \\ \widetilde{\lambda\beta_1} & \widetilde{\lambda\beta_2}\end{vmatrix} &= \lambda\widetilde{\lambda}(\beta_1\widetilde{\beta_2} - \beta_2\widetilde{\beta_1}) \\ &= N(\lambda)\sqrt{\Delta_K}N(\mathfrak{b}) \\ &= \sqrt{\Delta_K}N((\lambda)\mathfrak{b}) \\ &= \sqrt{\Delta_K}N(\mathfrak{a})\end{aligned}$$

Then we compute:

$$\begin{aligned}Q_{\lambda\beta_1,\lambda\beta_2}(x,y) &= \frac{1}{\lambda\mathfrak{b}}N(\lambda\beta_1 x + \lambda\beta_2 y) \\ &= \frac{1}{N(\lambda)N(\mathfrak{b})}N(\lambda)N(\beta_1 x + \beta_2 y) \\ &= \frac{1}{N(\mathfrak{b})}N(\beta_1 x + \beta_2 y) \\ &= Q_{\beta_1,\beta_2}(x,y)\end{aligned}$$

So the forms arising are equal, and in particular they are equivalent. Choosing any other basis for $\mathfrak{a}$ gives an equivalent form, so the forms arising from equivalent ideals in the narrow class group are always equivalent. □

Overall the above results say that we have a well-defined map from the narrow class group $\mathcal{C}^+(K)$ of the quadratic field of discriminant Δ_K to the set of equivalence classes of primitive integral binary quadratic forms of discriminant Δ_K. Theorem 58 in Fröhlich and Taylor [10, pp. 252–264] tells us:

Theorem 2.44. *The map between ideal classes in the narrow class group and equivalence classes of quadratic forms defined above is a bijection*

Proof. For surjectivity, let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant Δ_K. Set $\mathfrak{a} = \mathbb{Z}\langle a, \frac{b-\sqrt{\Delta_K}}{2}\rangle$, this is a fractional $\mathcal{O}_K$-ideal, with $\mathbb{Z}$-basis $\{a, \frac{b-\sqrt{\Delta_K}}{2}\}$.

If $a > 0$, then set $\lambda = 1$, otherwise set $\lambda = \sqrt{\Delta_K}$. Then the fractional ideal $\lambda\mathfrak{a}$ has basis $\{\alpha_1 = \lambda a, \alpha_2 = \lambda\frac{b-\sqrt{\Delta_K}}{2}\}$. This basis is normalised since:

$$\begin{vmatrix}\alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2}\end{vmatrix} = N(\lambda)\begin{vmatrix}a & \frac{b-\sqrt{\Delta_K}}{2} \\ a & \frac{b+\sqrt{\Delta_K}}{2}\end{vmatrix} = N(\lambda)a\sqrt{\Delta_K}$$

and we have $N(\lambda)a > 0$. We also read off that $N(\lambda\mathfrak{a}) = aN(\lambda)$. Now the quadratic form arising from this normalised basis is:

$$\begin{aligned}Q_{\alpha_1,\alpha_2}(x,y) &= \frac{1}{N(\lambda\mathfrak{a})}N\left(\lambda ax + \lambda\frac{b-\sqrt{\Delta_K}}{2}y\right) \\ &= \frac{1}{aN(\lambda)}N(\lambda)N\left(\left(ax + \frac{b}{2}y\right) - \frac{\sqrt{\Delta_K}}{2}y\right) \\ &= \frac{1}{a}\left(a^2x^2 + abxy + \frac{b^2-\Delta_K}{4}y^2\right) \\ &= ax^2 + bxy + \frac{b^2-\Delta_K}{4a}y^2\end{aligned}$$

Since given form had discriminant Δ_K, we have $\Delta_K = b^2 - 4ac$, so the coefficient of y^2 here is just $\frac{b^2-\Delta_K}{4a} = c$. Hence the form arising from the ideal $\lambda\mathfrak{a}$ is equal to the original form, and the map is surjective.

For injectivity, suppose the ideals $\mathfrak{a}$ and $\mathfrak{b}$ map to the same class of quadratic forms. Let $\{\alpha_1, \alpha_2\}$ be a normalised basis for $\mathfrak{a}$, and $\{\beta_1, \beta_2\}$ be a normalised basis for $\mathfrak{b}$. By changing basis we can assume the forms arising are actually equal: $Q_{\alpha_1,\alpha_2}(x, y) = Q_{\beta_1,\beta_2}(x, y)$. We need to show that $\mathfrak{a} = \lambda\mathfrak{b}$, for some λ with $N(\lambda) > 0$.

Going back to the definition of $Q_{\alpha_1,\alpha_2}(x, y)$, we can see that $N(\alpha_1 + \alpha_2 y) = 0$, when $y = -\frac{\alpha_1}{\alpha_2}$, so the roots of the quadratic equation $Q_{\alpha_1,\alpha_2}(1, y)$ are given by:

$$y = -\frac{\alpha_1}{\alpha_2} \text{ and } y = -\frac{\widetilde{\alpha_1}}{\widetilde{\alpha_2}}$$

Comparing the roots of the two quadratic equations $Q_{\alpha_1,\alpha_2}(1, y)$ and $Q_{\beta_1,\beta_2}(1, y)$, we must have:

$$\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2} \text{ or } \frac{\alpha_1}{\alpha_2} = \frac{\widetilde{\beta_1}}{\widetilde{\beta_2}}$$

If the latter holds then set $\lambda = \frac{\alpha_1}{\widetilde{\beta_1}} = \frac{\alpha_2}{\widetilde{\beta_2}}$, then we have:

$$\begin{vmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{vmatrix} = -N(\lambda) \begin{vmatrix} \beta_1 & \beta_2 \\ \widetilde{\beta_1} & \widetilde{\beta_2} \end{vmatrix}$$

Since the bases are normalised, this says that $N(\lambda) < 0$. But this contradicts the equality:

$$\begin{aligned} \frac{1}{N(\mathfrak{b})} N(\beta_1 x + \beta_2 y) &= Q_{\beta_1,\beta_2}(x, y) \\ &= Q_{\alpha_1,\alpha_2}(x, y) \\ &= \frac{1}{N(\mathfrak{a})} N(\alpha_1 x + \alpha_2 y) \\ &= \frac{1}{N(\mathfrak{a})} N(\lambda\widetilde{\beta_1} x + \lambda\widetilde{\beta_2} y) \\ &= \frac{N(\lambda)}{N(\mathfrak{a})} N(\widetilde{\beta_1} x + \lambda\widetilde{\beta_2} y) \\ &= \frac{N(\lambda)}{N(\mathfrak{a})} N(\beta_1 x + \lambda\beta_2 y) \end{aligned}$$

which says $N(\lambda)N(\mathfrak{b}) = N(\mathfrak{a})$, and so $N(\lambda) > 0$.

Therefore we have:

$$\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2}$$

Now set $\lambda = \frac{\alpha_1}{\beta_1} = \frac{\alpha_2}{\beta_2}$, so $\alpha_1 = \lambda\beta_1$ and $\alpha_2 = \lambda\beta_2$, so $\mathfrak{a} = \lambda\mathfrak{b}$. This time we have:

$$\begin{vmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{vmatrix} = N(\lambda) \begin{vmatrix} \beta_1 & \beta_2 \\ \widetilde{\beta_1} & \widetilde{\beta_2} \end{vmatrix}$$

so $N(\lambda) > 0$, since the bases are normalised. Hence we have shown the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent in the narrow class group. So the map is injective. □

From this bijection we derive the following corollaries:

Corollary 2.45. *The narrow class number $h^+(K)$ of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ of discriminant Δ_K is equal to the class number $h^+(\Delta_K)$ of quadratic forms of discriminant Δ_K.*

Proof. The sets have the same size using the bijection above. □

Corollary 2.46. *There is a group structure on the set of quadratic forms of discriminant Δ_K.*

Proof. The group structure on the narrow class group pulls back to the set of binary quadratic forms under the above bijection. □

There is a more general correspondence between quadratic forms of discriminant D, and the proper ideals in an order of discriminant D. This more general correspondence shows there is a natural group structure on the set of binary quadratic forms of any fixed discriminant. This group structure was first given by Gauss using his composition of quadratic forms, although Dirichlet gives a more tractable method. For details of this see Chapter 14 of Cassels [3, pp. 331–361].

Using the correspondence between quadratic forms and ideals in a quadratic field, and our notion of reduced forms from earlier we have an algorithmic way of computing the class number of any quadratic field by finding the corresponding class number of the quadratic forms.

Example 2.47. i) We determined earlier that the reduced quadratic forms of discriminant $D = -20$ were $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. So the class number is $h(-20) = 2$. But $D = -20$ is a fundamental discriminant, it is the discriminant of the quadratic field $K = \mathbb{Q}(\sqrt{-5})$. Our correspondence implies that the class number of the field is $h(K) = 2$.

ii) We also determined that there are four classes of reduced forms of discriminant $D = 105$, given by $-7x^2 + 7xy + 2y^2$, $-6x^2 + 3xy + 4y^2$, $-4x^2 + 3xy + 6y^2$, and $-2x^2 + 7xy + 7y^2$. So the class number is $h^+(105) = 4$. But $D = 105$ is a fundamental discriminant, it is the discriminant of the quadratic field $K = \mathbb{Q}(\sqrt{105})$. Our correspondence implies that the narrow class number of the field is $h^+(K) = 4$. A remark made in Cohen [4, p. 265] says we can determine the class number of the field by identifying the reduced forms $ax^2 + bxy + cy^2$ and $-ax^2 + bxy - cy^2$. Doing this reduced the number of orbits down to 2, and so tells us $h(K) = 2$. A consequence of this is the fundamental unit u must have positive norm; explicitly computing it gives $u = 41 + 4\sqrt{105}$, and this indeed has norm $N(u) = 1$.

Arising from this correspondence is a criterion for when a quadratic form represents an integer. Result 2.17 in Fröhlich and Taylor [10, p. 260] tells us:

Proposition 2.48. *A positive integer m is represented by the quadratic form $f(x, y)$ corresponding to the narrow ideal class of $\mathfrak{a}$ if and only if there is an integral ideal of norm m in the same narrow ideal class as $\mathfrak{a}$.*

Proof. Write $f(x, y) = Q_{\alpha_1,\alpha_2}(x, y)$ for some normalised basis $\{\alpha_1, \alpha_2\}$ of $\mathfrak{a}$. Firstly note that $\mathfrak{c}^{-1}$ and $\widetilde{\mathfrak{c}}$ are in the same narrow ideal class and $N(\mathfrak{c}) = N(\widetilde{\mathfrak{c}})$ for any fractional $\mathcal{O}_K$-ideal $\mathfrak{c}$.

Now suppose $\mathfrak{b}$ is an integral ideal with norm m in the same narrow ideal class as $\mathfrak{a}$. We can then write $\mathfrak{b} = \alpha\mathfrak{a}^{-1}$ for some totally positive α. We compute $m = N(\mathfrak{b}) = N(\widetilde{\mathfrak{b}}) = N(\alpha)N(\mathfrak{a})^{-1}$ and we have $(\alpha) = \mathfrak{a}\widetilde{\mathfrak{b}} \subset \mathfrak{a}$, since $\mathfrak{b}$ is integral, so $\alpha \in \mathfrak{a}$. Write $\alpha = x\alpha_1 + y\alpha_2$, then $Q_{\alpha_1,\alpha_2}(x, y) = N(\alpha)N(\mathfrak{a})^{-1} = m$, so the form represents m.

Conversely, suppose $m = Q_{\alpha_1,\alpha_2}(x, y)$, then $m = N(\alpha)N(\mathfrak{a})^{-1}$, where $\alpha = x\alpha_1 + y\alpha_2$. Since $N(\alpha) > 0$, one of α or $-\alpha$ is totally positive, say α. Then set $\mathfrak{b} = \widetilde{\alpha\mathfrak{a}^{-1}}$. Certainly $N(\mathfrak{b}) = N(\alpha\mathfrak{a}^{-1}) = N(\alpha)N(\mathfrak{a})^{-1} = m$, and we see $\widetilde{\mathfrak{b}}\mathfrak{a} = (\alpha) \subset \mathfrak{a}$. Multiplying by $\mathfrak{a}^{-1}$ shows $\widetilde{\mathfrak{b}} \subset \mathcal{O}_K$, so $\widetilde{\mathfrak{b}}$ is integral, and hence $\mathfrak{b}$ is an integral ideal in the same narrow ideal class as $\mathfrak{a}$. □

This correspondence between ideals of norm m and representations of m by the quadratic form shows that the primes represented by two quadratic forms of fundamental discriminant Δ_K are disjoint or agree. Furthermore if two forms represent the same prime then the forms are either equivalent or are inverses (in the sense of corresponding to inverse ideal classes).

Suppose that two forms $f(x,y)$ and $g(x,y)$ represent the prime p. Then the prime (p) of $\mathbb{Q}$ decomposes as $p\mathcal{O}_K = \mathfrak{p}\widetilde{\mathfrak{p}}$. We therefore have $f(x,y)$ and $g(x,y)$ either correspond to the same ideal class $[\mathfrak{p}]$ or $[\widetilde{p}]$. Otherwise they correspond to different ideal classes, one to $[\mathfrak{p}]$ and one to $[\widetilde{\mathfrak{p}}]$, but these ideal classes are inverses.

Then necessarily the forms $f(x,y)$ and $g(x,y)$ represent the same primes. Either they are equivalent or if $\mathfrak{a}$ is an ideal of norm q in the class corresponding to $f(x,y)$, then $\widetilde{a}$ is an ideal of norm q in the inverse class, corresponding to $g(x,y)$.

The disjointedness of the primes that two forms represents holds in general for any discriminant.

2.6 Representing Primes by Quadratic Forms

We will now more generally answer the question of when a prime is represented by a given binary quadratic form. Following Cox [7] we will establish some results on which discriminants can represent which primes.

A special case of Lemma 2.3 in Cox [7, p. 25] gives us the following proposition:

Proposition 2.49. *A prime p is represented by the form $f(x,y)$ if and only if $f(x,y)$ is equivalent to a form $px^2+qxy+ry^2$, for some integers q and r.*

Proof. Firstly if $f(x,y)$ is equivalent to $px^2+qxy+ry^2$, then $f(x,y)$ represents p, since $px^2+qxy+ry^2$ represents p at $x=1$, $y=0$.

Now let $p=f(a,b)$ be a representation of p by $f(x,y)$. Since p is prime, a and b are coprime; otherwise the non-trivial gcd divides p and hence equals p. But this means $p^2 \mid f(a,b)=p$. Apply the extended Euclidean algorithm to find c and d such that $ad-bc=1$, and then consider $\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\cdot f\right)(x,y) = f(ax+cy, bx+dy)$. This is an equivalent binary quadratic form and so will have integer coefficients. Notice that the coefficient of x^2 in the form can be extracted by setting $x=1$, and $y=0$. In this case we get the coefficient as $f(a\cdot 1+c\cdot 0, b\cdot 1+d\cdot 0)=f(a,b)=p$. Hence $f(x,y)$ is equivalent to $\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\cdot f\right)(x,y) = px^2+qxy+ry^2$ for some integers q and r. □

Lemma 2.5 in Cox [7, p. 25] then tell us when a prime p is represented by some quadratic form of discriminant D:

Proposition 2.50. *An odd prime $p \nmid D$ is represented by some primitive form of discriminant D if and only if D is a quadratic residue modulo p.*

Proof. If the form $f(x,y)$ of discriminant D represents p, then $f(x,y)$ is equivalent to some form $px^2+qxy+ry^2$. Then $D+q^2-4pr$, and looking modulo p we find that $D \equiv q^2 \pmod{p}$, hence D is a quadratic residue modulo p.

Now suppose D is a quadratic residue modulo p, so $D \equiv q^2 \pmod{p}$. As p is odd, we can choose q and D to have the same parity, replacing q with $q+p$ if necessary. As D is a discriminant we know $D \equiv 0,1 \pmod{4}$, and since we chose q and D to have the same parity this means $D \equiv q^2 \pmod{4p}$. So we can write $D=q^2-4pr$, for some r.

Then take the form $f(x,y)=px^2+qxy+ry^2$. This is an integral binary quadratic form of discriminant D which represents p. Furthermore it is primitive: p and D are coprime, and $D=q^2-4pr$, so p and q are coprime, hence the form has coprime coefficients. □

The Legendre symbol tells us precisely when an integer is square modulo an odd prime. This leads us to our first simple but important criterion:

Theorem 2.51. *An odd prime $p \nmid D$ is represented by some binary quadratic form of discriminant D if and only if $\left(\frac{D}{p}\right) = 1$.*

Proof. The Legendre symbol $\left(\frac{D}{p}\right) = 1$ if and only if D is a quadratic residue modulo p. □

The case we are primarily interested in is representing primes by the quadratic form $x^2 - ny^2$ of even discriminant $D = 4n$, using properties of the Legendre symbol we can simplify the criterion:

Corollary 2.52. *An odd prime $p \nmid n$ is represented by some binary quadratic form of discriminant $D = 4n$ if and only if $\left(\frac{n}{p}\right) = 1$.*

Proof. Since p is odd, $p \nmid D$, and so p is represented by a form of discriminant D if and only if $\left(\frac{D}{p}\right) = 1$. But $\left(\frac{D}{p}\right) = \left(\frac{4n}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{n}{p}\right)$ using the multiplicativity of the Legendre symbol. We always have $\left(\frac{4}{p}\right) = 1$ since $4 = 2^2$ is always square modulo the odd prime p. So $\left(\frac{D}{p}\right) = 1$ if and only if $\left(\frac{n}{p}\right) = 1$. □

Remark 2.53. We can see a special case of these corollaries by relating the quadratic forms side to the quadratic fields side, specifically when D is a fundamental discriminant. An odd prime $p \nmid D$ is represented by some binary quadratic form of discriminant D if and only if there is an ideal of norm p in the quadratic field $\mathbb{Q}(\sqrt{d})$. This happens if and only if (p) splits, which happens if and only if $\left(\frac{d}{p}\right) = 1$.

If $d \equiv 1 \pmod 4$, then $D = d$, and to represent a prime $p \nmid D$ by some form of discriminant D the corollary says we need $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = 1$. Otherwise $d \not\equiv 1 \pmod 4$, so then $D = 4d$, and we get $\left(\frac{D}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{d}{p}\right) = 1$.

2.7 Class Number One

We have a criterion to determine when a prime is represented by *some* binary quadratic form of discriminant D. If there is exactly one quadratic form $f(x, y)$ of discriminant D, then any number represented *some* quadratic form of discriminant D must be represented by $f(x, y)$. An immediate corollary to this is if there is exactly one quadratic form of discriminant D, the Legendre symbol tells us exactly which primes it represents. Thus we seek discriminants D such that $h(D) = 1$ in order to apply our criterion in the first case.

Using this result we can now easily give proofs of Fermat's claims, and start to take some tentative steps beyond Fermat.

2.7.1 Fermat's Claims

Primes of the Form $x^2 + y^2$

By listing reduced forms we see that $x^2 + y^2$ is the only quadratic form of discriminant $D = -4$. Our observation says that an odd prime $p \nmid D$ is represented by $x^2 + y^2$ if and only if $\left(\frac{-1}{p}\right) = 1$. The first supplement to quadratic reciprocity tells us this happens if and only if $p \equiv 1 \pmod 4$.

For completeness we should go back and check the primes we excluded: they are $p = 2$, and $p \mid -1$, so just $p = 2$. We see that $2 = 1^2 + 1^2$, so 2 is represented by $x^2 + y^2$.

This finishes the proof of Fermat's first claim, and we have:

$$p = x^2 + y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1 \pmod 4$$

Primes of the Form $x^2 + 2y^2$

Again $x^2 + 2y^2$ is the only quadratic form of discriminant $D = -8$, so an odd prime $p \nmid -2$ is represented by $x^2 + 2y^2$ if and only if $\left(\frac{-2}{p}\right) = 1$.

Using the multiplicativity of the Legendre symbol: $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$, so we want either $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{-2}{p}\right) = 1$ or we want $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{2}{p}\right) = -1$. The first and second supplements to quadratic reciprocity tell us the form happens when:

$$p \equiv 1 \pmod 4 \text{ and } p \equiv 1, 7 \pmod 8, \text{ so when } p \equiv 1 \pmod 8$$

and the latter happens when:

$$p \equiv 3 \pmod 4 \text{ and } p \equiv 3, 5 \pmod 8, \text{ so when } p \equiv 3 \pmod 8$$

This mean $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$. We also check that $2 = 0^2 + 2 \cdot 1^2$, so 2 is represented by $x^2 + 2y^2$.

This proves Fermat's second claim, and we have:

$$p = x^2 + 2y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1, 3 \pmod 8$$

Primes of the Form $x^2 + 3y^2$

In exactly the same way $x^2 + 3y^2$ is the only quadratic form of discriminant $D = -12$,a nd so an odd prime $p \nmid -3$ is of the form $x^2 + 3y^2$ if and only if $\left(\frac{-3}{p}\right) = 1$. Since $3 \equiv 3 \pmod 4$ quadratic reciprocity tell us that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, so we see $\left(\frac{p}{3}\right) = 1$, but this means p is non-zero square modulo 3. The squares modulo 3 are $0^2, 1^2, 2^2 \equiv 0, 1, \pmod 3$, so $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. Lastly we see that $x^2 + 3y^2$ represents $p = 3$, and does not represent $p = 2$

This proves Fermat's third claim, and we have:

$$p = x^2 + 3y^2 \Leftrightarrow p = 3, \text{ or } p \equiv 1 \pmod 3$$

2.7.2 Beyond Fermat

Fermat's claims could be dealt with easily since the class number of the discriminant D was $h(D) = 1$ in each case. The question naturally arises: for what other discriminants do we have class number $h(D) = 1$.

In the positive-definite case a corollary to the Baker-Heegner-Stark Theorem completely classifies the possible discriminants $D < 0$ for which we have $h(D) = 1$:

Theorem 2.54 (Baker-Heegner-Stark)**.** *If $D < 0$ is a discriminant, then $h(D) = 1$ precisely when $D = -3, -4, -7 - 8, -11, -12, -16, -19, -27, -28, -43, -67, -163$.*

Proof. The proof is far from trivial. For the case of even discriminant $D \equiv 0 \pmod 4$ an elementary proof was given by Landau, see [15]. When then discriminant is odd the proof is more difficult, see [23]. □

This theorem tell us that there are exactly two further times when we can solve the question of $p = x^2 + ny^2$, in the positive-definite case.

Primes of the Form $x^2 + 4y^2$

The only form of discriminant $D = -16$ is x^2+4y^2. An odd prime $p \nmid -4$ is represented by x^2+4y^2 if and only if $\left(\frac{-4}{p}\right) = 1$. But $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$. Since $p = 2$ is not represented by $x^2 + 4y^2$ we get:

$$p = x^2 + 4y^2 \Leftrightarrow p \equiv 1 \pmod 4$$

This result actually follows easily once primes of the form x^2+y^2 have been classified. If $p \neq 2$, then p is odd and so looking modulo 2 we see that one of x or y is even. Hence we can write p as $p = x^2 + 4y^2$. Conversely any prime of the form $p = x^2 + 4y^2 = x^2 + (2y)^2$ is already the sum of two squares.

Primes of the Form $x^2 + 7y^2$

Now we truly do take a step beyond Fermat. We have an odd prime $p \nmid -7$ is of the form $p = x^2 + 7y^2$ if and only if $\left(\frac{-7}{p}\right) = 1$. By quadratic reciprocity this is when $\left(\frac{p}{7}\right) = 1$, so p is a non-zero square modulo 7, hence $p \equiv 1, 2, 4 \pmod 7$.

If we go back and check the excluded primes in this case we find that $p = 2$ is not of the form $x^2 + 7y^2$, however $p = 2$ does satisfy $p \equiv 1, 2, 4 \pmod 7$. To take this into account we would have to tweak the congruence to exclude the case $p = 2$. When we use class field theory to study the problem of representing primes by binary quadratic forms we will get excluded primes that cannot be handled so easily. For this reason we stop checking the excluded primes, and simply remove them from consideration.

So we have for a prime $p \neq 2, 7$, that:

$$p = x^2 + 7y^2 \Leftrightarrow p \equiv 1, 2, 4 \pmod 7$$

The list of discriminants with class number one in the Baker-Heegner-Stark Theorem includes several odd discriminants. Our condition Legendre symbol condition can handle these just as easily and we can find similar criterion for other forms. Odd discriminant arises from forms like $f(x, y) = x^2 + xy - ny^2$, which has discriminant $D = 1 + 4n$. The list tells us that we can find conditions for $p = x^2 + xy + ny^2$ exactly when $n = 1, 2, 3, 5, 7, 11, 17, 41$. We will give just one example.

Primes of the Form $x^2 + xy + 3y^2$

This is the only form of discriminant $D = -11$. An odd prime $p \nmid 11$ is of the form $x^2 + xy + 3y^2$ if and only if $\left(\frac{-11}{p}\right) = 1$. By quadratic reciprocity this is $\left(\frac{p}{11}\right) = 1$, and the non-zero squares here are $p \equiv 1, 3, 4, 5, 9 \pmod{11}$.

For $p \neq 2, 11$:

$$p = x^2 + xy + 3y^2 \Leftrightarrow p \equiv 1, 3, 4, 5, 9, \pmod{11}$$

2.7.3 Indefinite Forms

For indefinite forms no such classification for when $h(D) = 1$ is known. It is not even known whether than are infinitely many fundamental discriminants with class number $h(D) = 1$. As we will show later there *are* infinitely many times when we get class number $h(D) = 1$

Once we have studied some class field theory, we will be able to prove that for a quadratic field $K = \mathbb{Q}(\sqrt{m})$, narrow class number $h^+(K) = 1$ can only occur for $m \equiv 1 \pmod 4$, a prime (except

$m = 2$). Using the links to quadratic fields that will show that for a fundamental discriminant class number one can only occur when $D = p$ where $p \equiv 1 \pmod 4$ is a prime, as we might oberve below.

The list of discriminants with class number $h(D) = 1$ begins: $D = 5, 8, 13, 17, 20, 29, 37, 41, 52, 53, 61, 68, 73, 89, 97, 101, 109, 113, 116, 125, 137, 149, 157, 164, 173, 181, 193, 197, \ldots$. This corresponds to forms:

$$x^2 - ny^2 \text{ for } n = 2, 5, 13, 17, 29, 41, \ldots \text{ and}$$
$$x^2 + xy - ny^2 \text{ for } n = 1, 3, 4, 7, 9, 10, \ldots$$

Primes of the Form $x^2 - 2y^2$

This is the only quadratic form of discriminant $D = 8$. An odd prime $p \nmid 2$ is represented by $x^2 - 2y^2$ if and only if $\left(\frac{2}{p}\right) = 1$. The second supplement to quadratic reciprocity tell us that this is exactly when $p \equiv 1, 7 \pmod 8$.

For $p \neq 2$:

$$p = x^2 - 2y^2 \Leftrightarrow p \equiv 1, 7 \pmod 8$$

Using these results we can start answering questions about whether certain Diophantine equations have solutions, that we could not otherwise answer easily. For a fixed prime it was easy enough to test every possibility in the positive-definite case, but this does not work in the indefinite case. Now we can say with certainty that the Diophantine equations:

$$3 = x^2 - 2y^2 \text{ has no solutions in integers, and}$$
$$5 = x^2 - 2y^2 \text{ has no solutions in integers}$$

Primes of the Form $x^2 - 5y^2$

This is the only quadratic form of discriminant $D = 20$. An odd prime $p \nmid 5$ is represented by $x^2 - 5y^2$ if an only if $\left(\frac{5}{p}\right) = 1$. Quadratic reciprocity says that this is the same as $\left(\frac{p}{5}\right) = 1$, so p is a non-zero square modulo 5. The squares are $p \equiv 1, 4 \pmod 5$.

For $p \neq 2, 5$:

$$p = x^2 - 5y^2 \Leftrightarrow p \equiv 1, 4 \pmod 5$$

Primes of the Form $x^2 - 13y^2$

This is the only quadratic form of discriminant $D = 52$. An odd prime $p \nmid 13$ is represented by $x^2 - 13y^2$ if and only if $\left(\frac{13}{p}\right) = 1$, or by quadratic reciprocity $\left(\frac{p}{13}\right) = 1$. The non-zero squares here are $p \equiv 1, 3, 4, 9, 10, 12$.

For $p \neq 2, 13$:

$$p = x^2 - 13y^2 \Leftrightarrow p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$$

We get similar results for the other forms $x^2 + ny^2$, with increasingly long congruence conditions on the primes represented, and can easily generate these results using the same technique. We also get similar results for the odd discriminants

Primes of the Form $x^2 + xy - 3y^2$

This is the only quadratic form of discriminant $D = 11$. An odd prime $p \nmid 11$ is represented by $x^2 + xy - 3y^2$ if and only if $\left(\frac{11}{p}\right) = 1$. Using quadratic reciprocity this is equivalent to $p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$.

For $p \neq 2, 11$:

$$p = x^2 + xy - 3y^2 \Leftrightarrow p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$$

Primes of the Form $x^2 + xy - 9y^2$

This is the only quadratic form of discriminant $D = 37$. An odd prime $p \nmid 37$ is represented by $x^2 + xy - 9y^2$ if and only if $\left(\frac{37}{p}\right) = 1$. Using quadratic reciprocity this is equivalent to $p \equiv 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36$.

For $p \neq 2, 37$:

$$p = x^2 + xy - 9y^2 \Leftrightarrow p \equiv \begin{array}{l} 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, \\ 25, 26, 27, 28, 30, 33, 34, 36 \end{array}$$

Something interesting happens in the indefinite case that does not happen in the positive-definite case. There are in fact infinitely many discriminants which have class number one. Theorem 2 in Section 13.2 of Cohn [6, p. 217] gives a formula relating the class number of the order $\mathcal{O}_f$ of discriminant $D = f^2 d$ to the class number of the maximal order $\mathcal{O}_K$ of discriminant d. This then gives a relation between the 'non-narrow' class numbers of quadratic forms, from which we can derive the class number of the discriminant $D = f^2 d$. It states:

Theorem 2.55. *For $d > 0$, the class number of the order $\mathcal{O}_f$ is given by:*

$$h(f^2 d) = \frac{f}{u} h(d) \prod_{q \mid f} \left(1 - \frac{1}{q}\left(\frac{d}{q}\right)\right)$$

where the product is taken over primes, and $u = \frac{\log \eta_f}{\log \eta_1}$ is the 'unit index', η_1 being the fundamental unit of $\mathcal{O}_K$ and η_f the fundamental unit of $\mathcal{O}_f$. We have $\eta_f = \eta_1^u$ for some integer u since η_f is also a unit of $\mathcal{O}_K$.

Using this I will give a sketch proof that $h^+(4 \cdot 13 \cdot 169^m) = 1$, for any m.

Proposition 2.56. *For any m, the class number $h^+(4 \cdot 13 \cdot 169^m) = 1$.*

Proof. Firstly the fundamental discriminant $d = 13$, and so $f = 2 \cdot 13^m$. This means we are considering the order $\mathcal{O}_f = \mathbb{Z}[13^m \sqrt{13}]$ in $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, the ring of integers of $K = \mathbb{Q}(\sqrt{13})$.

The fundamental unit in $\mathcal{O}_K$ is $\eta_1 = \frac{3+\sqrt{13}}{2}$, and it has norm $N(\eta_1) = -1$, and so we know $h(13) = h^+(13) = 1$.

The primes dividing $f = 2 \cdot 13^m$ are $q = 2, 13$, so we calculate:

$$\begin{aligned} \prod_{q \mid f} \left(1 - \frac{1}{q}\left(\frac{d}{q}\right)\right) &= \left(1 - \frac{1}{2}\left(\frac{13}{2}\right)\right)\left(1 - \frac{1}{13}\left(\frac{13}{13}\right)\right) \\ &= \left(1 - \frac{1}{2} \cdot (-1)\right)\left(1 - \frac{1}{13} \cdot 0\right) \\ &= \frac{3}{2} \end{aligned}$$

So we have:

$$h(f^2 d) = \frac{2 \cdot 13^m}{u} \cdot 1 \cdot \frac{3}{2} = \frac{3 \cdot 13^m}{u}$$

We have to calculate u, and we can do this inductively by viewing $\mathbb{Z}[13^{m+1}\sqrt{13}] \subset \mathbb{Z}[13^m\sqrt{13}]$. The start is $m = 0$, when $\mathbb{Z}[\sqrt{13}] \subset \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, in this case we directly see that $\eta_2 := \eta_1^3 = 18+5\sqrt{13}$ is the fundamental unit of $\mathbb{Z}[\sqrt{13}]$.

To find the fundamental unit $\eta_{2\cdot 13}$ of $\mathbb{Z}[13\sqrt{13}]$ we need to take a sufficiently high power of $\eta_2 = 18 + 5\sqrt{13}$ so that 13 divides the coefficient of $\sqrt{13}$. Expanding $(a + b\sqrt{13})^n$ and looking modulo 13 we see:

$$\begin{aligned}(a + b\sqrt{13})^n &= a^n + \binom{n}{1} a^{n-1} b\sqrt{13} + \text{terms divisible by } 13 \\ &= a^n + n a^{n-1} b\sqrt{13} + \text{terms divisible by } 13\end{aligned}$$

Since the coefficients of η_2, $a = 18$ and $b = 5$, are not divisible by 13, we need to take $n = 13$ to get another factor of 13, so the fundamental unit $\eta_{2\cdot 13} = {\eta_2}^{13}$. The above then shows that the coefficient of 1 in $\eta_{2\cdot 13}$ is not divisible by 13, and the coefficient of $\sqrt{13}$ has exactly one factor of 13.

Now suppose the coefficient of 1 in $\eta_{2\cdot 13^m}$ is not divisible by 13, and the coefficient of $\sqrt{13}$ is divisible by exactly m factors of 13. To find $\eta_{2\cdot 13^{m+1}}$ we need a sufficiently high power of $\eta_{2\cdot 13^m}$ that 13^{m+1} divides the coefficient of $\sqrt{13}$. Just as above, we need to take ${\eta_{2\cdot 13^m}}^{13}$, this gives exactly one extra factor of 13 in the coefficient of $\sqrt{13}$, and the coefficient of 1 is still not divisible by 13.

By induction this shows that $\eta_{2\cdot 13^m} = {\eta_{2\cdot 13}}^{13^m} = {\eta_{13}}^{3\cdot 13^m}$, and we read off $u = 3 \cdot 13^m$. Note that u is odd, so $N(\eta_{2\cdot 13^m}) = N(\eta_{13}) = -1$, so the fundamental unit of the order has negative norm. This means $h^+(4 \cdot 13 \cdot 169^m) = h(4 \cdot 13 \cdot 169^m)$.

The final step is to plug $u = 3 \cdot 13^m$ into the result above, and see that:

$$h(f^2 d) = \frac{3 \cdot 13^m}{u} = \frac{3 \cdot 13^m}{3 \cdot 13^m} = 1$$

This then shows that $h^+(4 \cdot 13 \cdot 169^m) = h(4 \cdot 13 \cdot 169^m) = 1$ as claimed. □

This result allows us to give a criterion which applies to an entire infinite family of quadratic forms.

Primes of the Form $x^2 - 13 \cdot 169^m y^2$

Since the class number is 1, this is the only quadratic form of discriminant $D = 4 \cdot 13 \cdot 169^m$. Hence an odd prime $p \nmid 13 \cdot 169^m$ is of the form $x^2 - 13 \cdot 169^m y^2$ if and only if $\left(\frac{13 \cdot 169^m}{p}\right) = 1$. Using the multiplicativity of the Legendre symbol:

$$\left(\frac{13 \cdot 169^m}{p}\right) = \left(\frac{13}{p}\right)\left(\frac{169^m}{p}\right) = \left(\frac{13}{p}\right)\left(\frac{13^{2m}}{p}\right) = \left(\frac{13}{p}\right)$$

since $169^m = 13^{2m}$ is always a square modulo the odd prime p. This means an odd prime $p \nmid 13 \cdot 169^m$ is represented by $x^2 - 13 \cdot 169^m y^2$ if and only if $\left(\frac{13}{p}\right) = 1$. We determined above that is when $p \equiv 1, 3, 4, 9, 1012 \pmod{13}$.

For $p \neq 2, 13$, and any m:

$$p = x^2 - 13 \cdot 169^m y^2 \Leftrightarrow p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$$

We now know with certainty that the equation:

$$3 = x^2 - 13 \cdot 169^m y^2 \text{ has a solution in integers for any } m$$

but even with for very small m, say $m = 1$, the smallest solution is rather large:

$$3 = 726662475293296^2 - 13 \cdot 169 \cdot 15503069909027^2$$

Using the brute force method of checking every possibility, even on a computer, you would give it up as a lost cause well before reaching this.

Chapter 3

Genus Theory

Genus theory provides an intermediate stepping stone between the relatively simple but highly specific case of class number one, and the more complicated but very general situation where class field theory is used to find criterion. In this chapter we will give a brief overview of the ideas of genus theory, and use this to derive criterion in more cases. Genus theory explains why the primes represented by certain quadratic forms can be characterised purely in terms of congruences, and when this fails. Most of the results on genus theory will come from Cox [7].

3.1 Genera of Quadratic Forms

When the class number is not one we need some way to separate the quadratic forms of this discriminant in order to find a criterion on which primes they can represent. The key idea of genus theory, due to Lagrange, is to look at what values each form represents modulo D, and to group forms representing the same values together.

The idea will become apparent if we look at an example.

Primes of the Form $x^2 + 6y^2$ and Other Forms of Discriminant $D = -24$

Consider $D = -24$, there are two quadratic forms of this discriminant: x^2+6y^2, and $2x^2+3y^2$. Our result tells us that an odd prime $p \nmid -24$ is represented by some quadratic form of discriminant -24, if and only if $\left(\frac{-6}{p}\right) = 1$, and this by quadratic reciprocity is if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$.

Let's look at what values the two quadratic forms represent modulo 24. Our result gives a criterion for primes $p \nmid 24$, so p is invertible modulo 24, and we should look at $(\mathbb{Z}/24\mathbb{Z})^*$. Substituting in all possible x and y modulo 24, we see that:

$$x^2 + 6y^2 \text{ represents } 1, 7 \text{ in } (\mathbb{Z}/24\mathbb{Z})^*$$
$$2x^2 + 3y^2 \text{ represents } 5, 11 \text{ in } (\mathbb{Z}/24\mathbb{Z})^*$$

Now we can say $p \equiv 1, 7 \pmod{24}$ implies p is represented by some quadratic form of discriminant -24, and so p is represented by one of $x^2 + 6y^2$, and $2x^2 + 3y^2$. It can't be represented by $2x^2 + 3y^2$ since reducing modulo 24 would give $p \equiv 5, 11 \pmod{24}$. Hence p must be represented by $x^2 + 6y^2$. Conversely if p is represented by $x^2 + 6y^2$, looking modulo 24 gives $p \equiv 1, 7 \pmod{24}$. This tell us an odd prime $p \nmid -24$, is represented by $x^2 + 6y^2$ if and only if $p \equiv 1, 7 \pmod{24}$.

Similarly we get $p = 2x^2 + 3y^2$ if and only if $p \equiv 5, 11 \pmod{24}$. These results just drop out from almost nothing.

Overall, for $p \neq 2, 3$:

$$p = x^2 + 6y^2 \Leftrightarrow p \equiv 1, 7 \pmod{24}$$
$$p = 2x^2 + 3y^2 \Leftrightarrow p \equiv 5, 11 \pmod{24}$$

From this we can start to develop and explain some general theory. In order to full develop and appreciate the genus theory of binary quadratic forms we would need to use the group structure on the set of classes of binary quadratic forms. Since we haven't defined this group structure fully, the theoretic details here will remain sketchy. However any criteria we find *can* be checked explicitly as in the example above, and so are valid.

We begin with the definition of when two quadratic forms are in the same genus.

Definition 3.1. Two quadratic forms $f(x, y)$ and $g(x, y)$ of discriminant D are said to be in the same genus if they represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$.

Since equivalent forms represent the same numbers, equivalent forms certainly represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$, and so the notion of being in the same genus is well defined on equivalence classes of binary quadratic forms. Each genus consists of a finite number of equivalence classes since the total number of classes is finite, and the number of genera is finite.

Extending the Legendre symbol multiplicatively to any positive bottom argument, leads to the Jacobi Symbol $\left(\frac{D}{\cdot}\right)$. As shown in Lemma 1.14 of Cox [7, p. 16–18], for $D \equiv 0, 1$, the map $\chi\colon (\mathbb{Z}/D\mathbb{Z})^* \to \{1, -1\}$ defined by $\chi([m]) = \left(\frac{D}{m}\right)$ is a well-defined homomorphism.

For a discriminant $D \equiv 0, 1 \pmod 4$, the forms:

$$x^2 + xy + \tfrac{1-D}{4}y^2 \text{ if } D \equiv 1 \pmod 4$$
$$x^2 - \tfrac{D}{4}y^2 \text{ if } D \equiv 0 \pmod 4$$

are more generally called the principal forms, reducing to the previous when D is a fundamental discriminant.

In Lemma 2.24, Cox [7, p. 34–35] then establishes the following result for negative discriminants, which holds in general:

Proposition 3.2. *Let $D \equiv 0, 1 \pmod 4$ be a discriminant, and χ be the map above. Then:*

i) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D are a subgroup $H \subset \ker \chi$.

ii) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by a form $f(x, y)$ of discriminant D are a coset of H in $\ker \chi$.

In particular whilst proving this he establishes that if, for some prime odd prime $p \nmid D$, the class $[p] \in (\mathbb{Z}/D\mathbb{Z})^*$ is represented by some quadratic form, then $\left(\frac{D}{p}\right) = 1$, so p itself is represented by some quadratic form of discriminant D.

As a corollary of this Proposition, since cosets are disjoint or agree, the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by different forms are disjoint or agree. Consequently different genera represent disjoint values.

Taken together these results show that the argument in the example above works in general to find the primes which a given genus of quadratic forms represents. We get Theorem 2.26 in Cox [7, p. 35] which states:

Theorem 3.3. *Suppose a genus of quadratic forms of discriminant D represents the values H in $(\mathbb{Z}/D\mathbb{Z})^*$. Then an odd prime $p \nmid D$ is represented by a form of this genus if and only if $[p] \in H$.*

If a genus consist of only one form, then the above Theorem tells us exactly which primes it represents, in terms of a congruence condition modulo D.

3.2 One Form per Genus

The natural question now is: for which discriminants D do we have a genus with only one form? The answer to this requires studying the group of equivalence classes of quadratic forms. Let $\mathcal{C}^+(D)$ denotes the set of binary quadratic forms of discriminant D endowed with the group structure Gauss defined. Cox then defines a map:

$$\Phi\colon \mathcal{C}^+(D) \to \ker \chi / H$$

which sends a class to the values it represents in $(\mathbb{Z}/D\mathbb{Z})^*$, with the notation as before.

In Lemma 3.13 Cox [7, p. 54] establishes that this map is a group homomorphism. This leads to Corollary 3.14 which states:

Corollary 3.4. *i) All genera of forms of discriminant D consist of the same number of values.*
ii) The number of genera of forms of discriminant D is a power of two.

Theorem 3.15 in Cox [7, p. 54-56] explicitly describes the genus containing the principal form, and provides a way to count the number of genera.

Theorem 3.5. *i) The genus containing the principal form consists of the classes in $\mathcal{C}^+(D)^2$, the subgroup of squares in $\mathcal{C}^+(D)$.*
ii) There are $2^{\mu-1}$ genera of forms of discriminant D, where μ is defined as follows. Let r be the number of odd primes dividing D. If $D \equiv 1 \pmod 4$, then set $\mu = r$. Otherwise write $D = 4n$, then μ is determined by:

n	μ
$n \equiv 1 \pmod 4$	r
$n \equiv 2, 3 \pmod 4$	$r+1$
$n \equiv 4 \pmod 8$	$r+1$
$n \equiv 0 \pmod 8$	$r+2$

If we want each genus to contain a single form, then the number of genera needs to equal the number of classes. This leads to Theorem 3.22 in Cox [7, pp. 59–60], which gives various equivalent criteria for there to be one form per genus. It also gives us a way to effectively tell when there is one form per genus by only knowing the class number:

Theorem 3.6. *The following are equivalent:*
i) Every genus of forms of discriminant D consist of a single class.
ii) The class group $\mathcal{C}^+(D)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some m.
iii) The class number $h^+(D)$ equals $2^{\mu-1}$, where μ is defined above.

In particular there is definitely one form per genus whenever the class number is 1 or 2. More generally we can check for any given discriminant whether there is one form per genus, and if there is we can give a criterion for a prime to be represented by any of the forms of that discriminant.

According to Cassels [3, p. 357], in the positive definite case there are 101 known values for which there is one form per genus, and this is conjectured to be all. This list is known to be finite, and so genus theory does not get us much further in the positive-definite case. Since we know class number one occurs infinitely often in the indefinite case, genus theory works infinitely often, but obvious doesn't always work; not every class number is a power of two.

We give some examples of the criterion which arise in a variety of cases:

Primes of the Form $x^2 + 8y^2$ and Other Forms of Discriminant $D = -32$

There are two quadratic forms of discriminant $D = -32$, the forms $x^2 + 8y^2$, and $3x^2 + 2xy + 3y^2$. Since the class number is two we know that each genus contains one form. Explicitly these forms are in different genera since they represent different values in $(\mathbb{Z}/32\mathbb{Z})^*$.

$$x^2 + 8y^2 \text{ represents } 1, 9, 17, 25 \text{ in } (\mathbb{Z}/32\mathbb{Z})^*$$
$$3x^2 + 2xy + 3y^2 \text{ represents } 3, 11, 19, 27 \text{ in } (\mathbb{Z}/32\mathbb{Z})^*$$

We immediately conclude for $p \neq 2$ that:

$$p = x^2 + 8y^2 \Leftrightarrow p \equiv 1, 9, 17, 25 \pmod{32}$$
$$p = 3x^2 + 2xy + 3y^2 \Leftrightarrow p \equiv 3, 11, 19, 27 \pmod{32}$$

Primes of the Form $x^2 - 3y^2$ and Other Forms of Discriminant $D = 12$

There are two quadratic forms of discriminant $D = 12$, they are $x^2 - 3y^2$ and $-x^2 + 3y^2$. Since the class number is 2 we know that each genus contains one form. Explicitly these forms are in different genera:

$$x^2 - 3y^2 \text{ represents } 1 \text{ in } (\mathbb{Z}/12\mathbb{Z})^*$$
$$-x^2 + 3y^2 \text{ represents } 11 \text{ in } (\mathbb{Z}/12\mathbb{Z})^*$$

So for $p \neq 2, 3$, we have:

$$p = x^2 - 3y^2 \Leftrightarrow p \equiv 1 \pmod{12}$$
$$p = -x^2 + 3y^2 \Leftrightarrow p \equiv 11 \pmod{12}$$

Primes of the Form $x^2 - 15y^2$ and Other Forms of Discriminant $D = 60$

There are four quadratic forms of discriminant $D = 60$, they are $x^2 - 15y^2$, $-x^2 + 15y^2$, $2x^2 + 6xy - 3y^2$, and $-2x^2 + 6xy + 3y^2$. We compute μ and check whether there is one form per genus. As $D = 60 = 2^2 \cdot 3 \cdot 5$ there are $r = 2$ odd prime divisors. We calculate $n = 15 \equiv 3 \pmod{4}$, so $\mu = r + 1 = 3$. Then $2^{\mu-1} = 2^2 = 4 = h^+(60)$, and so by the Theorem there is one form per genus. Explicitly we find:

$$x^2 - 15y^2 \text{ represents } 1, 49 \text{ in } (\mathbb{Z}/60\mathbb{Z})^*$$
$$-x^2 + 15y^2 \text{ represents } 11, 59 \text{ in } (\mathbb{Z}/60\mathbb{Z})^*$$
$$2x^2 + 6xy - 3y^2 \text{ represents } 17, 53 \text{ in } (\mathbb{Z}/60\mathbb{Z})^*$$
$$-2x^2 + 6xy + 3y^2 \text{ represents } 7, 43 \text{ in } (\mathbb{Z}/60\mathbb{Z})^*$$

So for $p \neq 2, 3, 5$, we have:

$$p = x^2 - 15y^2 \Leftrightarrow p \equiv 1, 49 \pmod{60}$$
$$p = -x^2 + 15y^2 \Leftrightarrow p \equiv 11, 59 \pmod{60}$$
$$p = 2x^2 + 6xy - 3y^2 \Leftrightarrow p \equiv 17, 53 \pmod{60}$$
$$p = -2x^2 + 6xy + 3y^2 \Leftrightarrow p \equiv 7, 43 \pmod{60}$$

Primes of the Form $x^2 + xy + 4y^2$ and Other Forms of Discriminant $D = -15$

There are two quadratic forms of discriminant $D = -15$, namely $x^2+xy+4y^2$, and $2x^2+xy+2y^2$. As the class number is 2 we know there is one form per genus. Explicitly:

$$x^2 + xy + 4y^2 \text{ represents } 1, 4 \text{ in } (\mathbb{Z}/15\mathbb{Z})^*$$
$$2x^2 + xy + 2y^2 \text{ represents } 2, 8 \text{ in } (\mathbb{Z}/15\mathbb{Z})^*$$

This gives for $p \neq 2, 3, 5$, that:

$$p = x^2 + xy + 4y^2 \Leftrightarrow p \equiv 1, 4 \pmod{15}$$
$$p = 2x^2 + xy + 2y^2 \Leftrightarrow p \equiv 2, 8 \pmod{15}$$

When there is one form per genus we can find a congruence condition on which primes the form represents. Theorem 3.21 in Cox [7, p. 58–59] tells us that two forms $f(x, y)$ and $g(x, y)$ of discriminant D are in the same genus if and only if $f(x, y)$ and $g(x, y)$ represent the same values in $(\mathbb{Z}/m\mathbb{Z})^*$ for all non-zero integers m. So conversely forms in the same genus cannot be separated using congruences. To find criteria in these cases we need more advanced ideas.

3.3 Euler's Convenient Numbers

The positive m for which the discriminant $D = -4m$ has one genus per class were known to Euler in a different context and under a different definition. Euler called a positive integer m convenient if $p = x^2+my^2$ has exactly one solution in positive integers implies that p is prime. Gauss observed that these definitions are equivalent, a proof is given in Proposition 3.24 of Cox [7, p. 61–62].

Using convenient numbers Euler was able to prove that certain large integers are prime. He conjectured that $m = 1848$ is a convenient number and used this to prove 18 518 809 is prime.

Using the equivalence of these two definitions we can prove $m = 1848$ is convenient. The class number of discriminant $D = -4 \cdot 1848$ is $h(D) = 16$. We have that $D = 2^5 \cdot 3 \cdot 7 \cdot 11$, so $r = 3$. Since $n = -1848$, and $n \equiv 0 \pmod{8}$, we set $\mu = r + 2 = 5$. Then $2^{\mu-1} = 2^4 = 16 = h(D)$. By a Theorem above there is one form per genus, and so $m = 1848$ is convenient.

Following Euler we can establish:

Proposition 3.7. *The number $p = 18\,518\,809$ is prime.*

Proof. Firstly we have that $m = 1848$ is convenient. Now we count the number of solutions to:

$$18\,518\,809 = x^2 + 1848y^2$$

in positive integers.

We have a bound on y as follows:

$$1848y^2 = 18\,518\,809 - x^2 \leq 18\,518\,809$$

But this implies

$$|y| \leq \sqrt{\frac{18\,518\,809}{1848}} = 100.1049\ldots$$

Since y is an integer, we get $|y| \leq 100$. Now it is a relatively simple, if tedious, task to check up to $y = 100$ whether $18\,518\,809 - 1848y^2$ is a square, and so whether we get a solution to the equation.

On doing this it turns out that the only solution in positive integers is $x = 197, y = 100$. But since 1848 is convenient, Euler's definition of convenient immediately implies that $p = 18\,518\,809$ must be prime. □

This method involves significantly fewer calculations that the naive method of checking for divisors of $p = 18\,518\,809$. The naive method would require checking that $p = 18\,518\,809$ is not divisible by any prime to up $q = \sqrt{18\,518\,809} = 4303.3485\ldots$.

More details on Euler's convenient numbers can be found in the article by Frei [9].

Part II

Class Fields

Chapter 4

Class Field Theory

Class field theory studies the abelian extensions of number fields. It seeks to classify and construct all abelian extensions of a number field, and to predict their arithmetic properties in terms of the base number field itself. After an introduction to infinite primes from Milne [20], we will work from Janusz [14] to give an introduction to class field theory.

4.1 Infinite Primes

Before delving into class field theory and being able to state the main theorems we need to introduce the notion of a modulus, and to do this we need to understand so-called infinite primes.

As some motivation to introduce the concept of an infinite prime, we first look at a Theorem of Alexander Ostrowski, which deals with the possible non-trivial absolute values on $\mathbb{Q}$, up to equivalence. For this we will work from Milne [20, pp. 101-108], using the first half of Chapter 7.

Definition 4.1. An absolute value on an integral domain D is a function $|\cdot| : D \to \mathbb{R}$ satisfying:
i) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
ii) $|xy| = |x|\,|y|$,
iii) $|x + y| \leq |x| + |y|$,
for all x, $y \in D$.

Example 4.2. Every integral domain admits the following absolute value:

$$|x|_0 = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise} \end{cases}$$

This absolute value is called the trivial absolute value.

Give an absolute value on an integral domain, we may define a distance function $d\colon D \to \mathbb{R}$ by $d(x, y) = |x - y|$. Equipping D with this metric makes the pair (D, d) into a metric space, and hence induces a topology on the set D making it a topological space.

Example 4.3. On $\mathbb{Q}$ we have, amongst others, the ordinary absolute value restricted from $\mathbb{R}$:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

We also have the p-adic absolute values, one for each prime p of $\mathbb{Q}$. They are defined as follows: for a fixed prime p, every non-zero rational x can be written uniquely as $x = p^n \frac{a}{b}$, with a, b, and p coprime, and $n \in \mathbb{Z}$. The absolute value defined by:

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{otherwise} \end{cases}$$

is called the p-adic absolute value.

Completing $\mathbb{Q}$ with respect to the p-adic metric induced by the p-adic absolute value gives us the field of p-adic numbers $\mathbb{Q}_p$.

As with all mathematical objects, we want a notion of equivalence between absolute values; some way to recognise certain absolute values are essentially the same, and to treat them as such.

Proposition 4.4. *Let $|\cdot|_a$ and $|\cdot|_b$ be two absolute values on a field K, with $|\cdot|_a$ non-trivial. Then the following conditions are equivalent:*

i) $|\cdot|_a$ and $|\cdot|_b$ define the same topology on K,
ii) $|\alpha|_a < 1$ implies $|\alpha|_b < 1$,
iii) $|\cdot|_b = |\cdot|_a^{\,c}$ for some real number $c > 0$.

Proof. See Proposition 7.8 in Milne [20, p. 104]. □

Definition 4.5. Two absolute values $|\cdot|_a$ and $|\cdot|_b$ are called equivalent if they satisfy any (and so all) of the conditions given in the proposition.

A natural question then arises: what are all the possible absolute values up to equivalence? Ostrowski answered this question for $\mathbb{Q}$ with the following theorem:

Theorem 4.6 (Ostrowski)**.** *Up to equivalence, the possible non-trivial absolute values on $\mathbb{Q}$ are: the ordinary absolute value and the p-adic absolute values, one for each prime p.*

Proof. See Theorem 7.12 in Milne [20, p. 105]. □

After identifying the a prime p with its corresponding p-adic absolute value, this theorem strongly suggests that the ordinary absolute value on $\mathbb{Q}$ should be considered as another prime. And so it is, this is an example of a so-called infinite prime. More generally we make the following definition:

Definition 4.7. A prime of a number field K, also called a place, is an equivalence class of absolute values on K.

Example 4.8. Ostrowski's Theorem shows that the primes of $\mathbb{Q}$ are $\{2, 3, 5, 7, \ldots, \infty\}$, that is: the ordinary primes in $\mathbb{Z}$, and the infinite prime we saw above. Here a prime integer p refers to the corresponding p-adic absolute value $|\cdot|_p$, and ∞ refers to the ordinary absolute value $|\cdot| = |\cdot|_\infty$.

How do these primes relate to the prime ideals we already know about? In the case $K = \mathbb{Q}$, the p-adic absolute values $|\cdot|_p$ correspond to the prime integers p in $\mathbb{Z}$, and these correspond to the prime ideals (p) of $\mathbb{Q}$. This holds more generally, specifically we have the theorem:

Theorem 4.9. *The primes of a number field K fall into three classes:*

i) The $\mathfrak{p}$-adic absolute values $|\cdot|_\mathfrak{p}$, one for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. These are called the finite primes.
ii) The absolute values obtained from the real embeddings $K \hookrightarrow \mathbb{R}$ by an composing with the ordinary absolute value $|\cdot| : \mathbb{R} \to \mathbb{R}$. These are the real infinite primes.

iii) The absolute values obtained from the complex conjugate pairs of non-real embeddings $K \hookrightarrow \mathbb{C}$ by an composing with the ordinary absolute value $|\cdot| : \mathbb{C} \to \mathbb{R}$. These are the complex infinite primes.

Proof. See Theorem 7.14 in Milne [20, p. 107]. □

The infinite primes of a number field correspond to embeddings of the number field, so we will identify the infinite primes with their embeddings.

We need to understand what it means for an infinite prime to ramify in order to be able to state the results of class field theory and work with class fields.

Definition 4.10. An infinite prime σ of a number field K is said to ramify the extension L/K if σ is a real infinite prime of K, and has an extension to a complex infinite prime of L.

Remark 4.11. This definition is comparable to the ramification of finite primes. If an infinite prime σ ramifies in the extension L/K, then the same prime lies twice over σ as σ may be extended to a complex embedding τ or to its conjugate $\overline{\tau}$, both of which correspond to the same infinite prime of L.

We can now take a look at some examples of infinite primes in number fields an their ramification.

Example 4.12. i) Consider the number field $K = \mathbb{Q}(\sqrt{2})$. This field has two real embeddings $\sigma_1 \colon \sqrt{2} \mapsto \sqrt{2}$, and $\sigma_2 \colon \sqrt{2} \mapsto -\sqrt{2}$, and no complex embeddings. So K has two real infinite primes, and no complex infinite primes.

Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ be an extension of K. Do the infinite primes σ_1 and σ_2 of K ramify in L/K? All the infinite primes of L are real, the embeddings are $\tau_i \colon \sqrt{2} \mapsto \pm\sqrt{2}, \sqrt{3} \mapsto \pm\sqrt{3}$. So no real infinite prime of K has a complex extension, and all infinite primes are unramified in L/K.

Now let $M = \mathbb{Q}(\sqrt{2}, \mathrm{i})$ be another extension of K. Here the infinite primes are all complex, any embedding must have $\tau_i \colon \mathrm{i} \mapsto \pm\mathrm{i}$. This means real infinite primes of K necessarily have complex extensions, and so all infinite primes are ramified in M/K.

ii) Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. This field has one pair of complex embeddings and so one complex infinite prime. Since there are no real infinite primes there cannot be any ramified infinite primes and so the infinite prime is unramified in any extension L/K.

More generally if the only infinite primes of a number field are complex, then by definition they are unramified in any extension.

iii) Consider the number field $K = \mathbb{Q}(\sqrt[3]{7})$. This field has one real embedding $\sigma_1 : \sqrt[3]{7} \mapsto \sqrt[3]{7}$, and one pair of complex embeddings $\sigma_2, \overline{\sigma_2} : \sqrt[3]{7} \mapsto \sqrt[3]{7}\rho, \sqrt[3]{7}\overline{\rho}$, where $\rho^3 = 1$ is a primitive cube root of 1.

Let $L = \mathbb{Q}(\sqrt[3]{7}, \sqrt{5})$. If we extend the real embedding σ_1 of K to an embedding of L we must have $\tau \colon \sqrt{5} \mapsto \pm\sqrt{5}$. Both of these possibilities are real embeddings, hence σ_1 does not extend to a complex embedding and hence is unramified in L/K.

Now let $M = \mathbb{Q}(\sqrt[3]{7}, \sqrt[3]{3})$. The real embedding σ_1 of K can extend to the following complex embedding $\tau \colon \sqrt[3]{3} \mapsto \sqrt[3]{3}\rho$ of M, and so σ_1 ramifies in M/K.

4.2 Moduli and Generalised Ideal Class Groups

The central theme of class field theory is the connection between generalised ideal class groups and abelian extensions of a number field. To define a generalised ideal class group we first introduce a modulus.

Definition 4.13. A modulus in a number field K is a formal product of primes of K:

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

where the product is taken over all primes $\mathfrak{p}$ of K, finite or infinite, and the exponents $n_{\mathfrak{p}}$ satisfy:

i) $n_{\mathfrak{p}} \geq 0$, with all but finitely many being zero,
ii) $n_{\mathfrak{p}} = 0$ whenever $\mathfrak{p}$ is a complex infinite prime, and
iii) $n_{\mathfrak{P}} \leq 1$ whenever $\mathfrak{p}$ is a real infinite prime.

If all the exponents $n_{\mathfrak{p}} = 0$, then the modulus is simply $\mathfrak{m} = 1$.

We may write a modulus $\mathfrak{m}$ as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_K$, and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. If K is an imaginary quadratic field, then the only infinite primes are complex, and so a modulus $\mathfrak{m}$ can be regarded as an ideal of $\mathcal{O}_K$.

Definition 4.14. Given a modulus $\mathfrak{m}$ of a number field K, let $\mathcal{I}_K(\mathfrak{m})$ be the group of all fractional ideals of K which are relatively prime to $\mathfrak{m}$, that is relatively prime to $\mathfrak{m}_0$ in the decomposition above. Let $\mathcal{P}_{K,1}(\mathfrak{m})$ be the subgroup generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies:

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0}, \text{ and}$$
$$\sigma(\alpha) > 0 \text{ for every real infinite prime } \sigma \text{ dividing } \mathfrak{m}$$

Definition 4.15. A subgroup $H \subset \mathcal{I}_K(\mathfrak{m})$ is called a congruence subgroup for $\mathfrak{m}$ if it satisfies:

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subset H \subset \mathcal{I}_K(\mathfrak{m})$$

and then the quotient $\mathcal{I}_K(\mathfrak{m})/H$ is called a generalised ideal class group for $\mathfrak{m}$.

In Corollary 1.3 of Section 4.1 of Janusz [14, p. 111], he establishes that the subgroup $\mathcal{P}_{1,K}(\mathfrak{m})$ has finite index in $\mathcal{I}_K(\mathfrak{m})$. Hence the quotient $\mathcal{I}_K(\mathfrak{m})/\mathcal{P}_{K,1}(\mathfrak{m})$ is finite, and so is any generalised ideal class group.

We already know two generalised ideal class groups.

Example 4.16. For any number field K:

i) The ideal class group $\mathcal{C}(K)$ is a generalised ideal class group for the modulus $\mathfrak{m} = 1$. If $\mathfrak{m} = 1$, then $\mathcal{I}_K(\mathfrak{m}) = \mathcal{I}_K(1) = \mathcal{I}(K)$ is the group of all fractional ideals of K, since there are no primes dividing $\mathfrak{m}$ to check. And $\mathcal{P}_{1,K}(\mathfrak{m}) = \mathcal{P}_{1,K}(1) = \mathcal{P}(K)$, since there is also nothing to check. Now $H = \mathcal{P}(K)$ is a congruence subgroup for $\mathfrak{m} = 1$, and the quotient is $\mathcal{I}(K)/H = \mathcal{I}(K)/\mathcal{P}(K) = \mathcal{C}(K)$ the ideal class group of K.

ii) The narrow class group $\mathcal{C}^+(K)$ is also a generalised ideal class group for the modulus $\mathfrak{m}$ consisting of the product of all real infinite primes of K. Here $\mathcal{I}_K(\mathfrak{m}) = \mathcal{I}(K)$ since there are no finite primes to check. Then the subgroup $\mathcal{P}_{1,K}(K) = \mathcal{P}^+(K)$, since it is generated by $\alpha \in \mathcal{O}_K$ satisfying $\sigma(\alpha) > 0$, for all real embeddings σ. Then $H = \mathcal{P}^+(K)$ is a congruence subgroup, and the quotient is $\mathcal{I}(K)/\mathcal{P}^+(K) = \mathcal{C}^+(K)$, the narrow class group.

Any subgroup of a generalised class group is also a generalised class group. The pre-image of a subgroup under the quotient map defines a subgroup sitting between $\mathcal{P}_{K,1}(\mathfrak{m})$, and $\mathcal{I}_K(\mathfrak{m})$, so is a congruence subgroup for $\mathfrak{m}$.

Using the observation above this establishes that the class group and the narrow class group of any number field is finite.

4.3 The Artin Symbol and the Artin Map

The basic ideal of class field theory is that generalised ideal class groups of a number field K are exactly the Galois groups of abelian extensions of K. A link is provided by the Artin symbol.

Let L/K be a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of K which is unramified in L. Take a prime $\mathfrak{P}$ above $\mathfrak{p}$ in L. Since the prime $\mathfrak{p}$ is unramified the inertia group $I_{\mathfrak{P}}$ is trivial: it has order $|I_{\mathfrak{P}}| = e = 1$. As before this means we have a canonical isomorphism:

$$D_{\mathfrak{P}} \cong D_{\mathfrak{P}}/I_{\mathfrak{P}} \to \widetilde{G}$$

where $\widetilde{G}$ is the Galois group of the residue field extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$. Since this is an finite extension of finite fields, the Galois group is known to be cyclic, with a distinguished generator given by the Frobenius Frob: $x \mapsto x^q$, where $q = |\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p})$.

Working backwards through these isomorphisms, the Frobenius picks out a distinguished generator of $D_{\mathfrak{P}}$, which we will also call the Frobenius.

Definition 4.17. In the situation above, the Artin symbol of the prime $\mathfrak{P}$ of L is defined to be the Frobenius generator of $D_{\mathfrak{P}}$. The Artin symbol of $\mathfrak{P}$ is an element of $\mathrm{Gal}(L/K)$, and we denoted it by:

$$\left(\frac{L/K}{\mathfrak{P}}\right)$$

The notation for the Artin symbol is reminiscent of the Legendre symbol, this is no coincidence. The Artin symbol generalises the Legendre symbol, and as we will show later class field theory subsumes and generalises quadratic reciprocity. In simple cases we can already easily determine exactly what the Artin symbol is for each prime.

Example 4.18. Consider the number field $K = \mathbb{Q}(\sqrt{3})$, which is an Galois extension of $\mathbb{Q}$. The Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}_2 = \{1, -1\}$, where we identify 1 with the identity automorphism $\sqrt{3} \mapsto \sqrt{3}$, and -1 with conjugation $\sqrt{3} \mapsto -\sqrt{3}$.

The only ramified prime of $K/\mathbb{Q}$ is 3. If $p \neq 3$, and $\mathfrak{p}$ is a prime of K above p we can define the Artin symbol of $\mathfrak{p}$. We will calculate it in some cases.

Let $p = 5$, then $\left(\frac{3}{5}\right) = -1$, so the prime $p = 5$ is inert in K. The only prime above 5 is $\mathfrak{p} = 5$ itself. We have $f = 2$ for this prime, and so comparing orders gives $D_{\mathfrak{p}} = \mathrm{Gal}(L/K)$. Only -1 generates $D_{\mathfrak{p}}$, so we must have $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) = -1$. The same result holds true for any inert prime.

Now look at $p = 11$, where $\left(\frac{3}{11}\right) = 1$, so the prime $p = 11$ splits in K. There are two primes $\mathfrak{p}$, and $\widetilde{\mathfrak{p}}$ above 11. We have $f = 1$ for these primes, so we must have $D_{\mathfrak{p}} = \{1\}$. Hence the generator is 1, and we have $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) = \left(\frac{K/\mathbb{Q}}{\widetilde{\mathfrak{p}}}\right) = 1$. The same results holds for any split prime.

Under the identification of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ with $\{-1, 1\}$, the value of the Artin symbol of a prime $\mathfrak{p}$ corresponds exactly with the value of the Legendre symbol of the prime p below $\mathfrak{p}$, so we can write:

$$\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) = \left(\frac{3}{p}\right)$$

Now we will prove some properties of the Artin symbol.

Proposition 4.19. *The Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right)$ is the unique element $\sigma \in D_{\mathfrak{P}}$ satisfying:*

$$\sigma(x) \equiv x^q \pmod{\mathfrak{P}}, \text{ for all } x \in \mathcal{O}_L$$

where $q = N(\mathfrak{p})$ is the norm of the prime $\mathfrak{p}$ of K below $\mathfrak{P}$.

Proof. This is essentially the *definition* of the Artin symbol. The Artin symbol σ corresponds canonically to the Frobenius generator of $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$, which sends $x \mapsto x^q$, and so $\sigma(x) \equiv x^q \pmod{P}$. □

Property 2.2 in Janusz [14, p. 98] gives us the following:

Proposition 4.20. *Let L/K be an abelian extension, and $\mathfrak{P}$ be a prime of L above the unramified prime $\mathfrak{p}$ of K. Then for $\sigma \in \mathrm{Gal}(L/K)$:*

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$$

Proof. Following the proof given by Janusz, we can write any element of $\mathcal{O}_L$ as $\sigma^{-1}(x)$ for $x \in \mathcal{O}_L$. The definition of the Artin symbol tell us that:

$$\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(x) \equiv \sigma^{-1}(x)^q \pmod{\mathfrak{P}}$$

Applying σ gives:

$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(x) \equiv x^q \pmod{\sigma(\mathfrak{P})}$$

Since $\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} \in D_{\sigma(\mathfrak{P})}f$, this precisely shows that $\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$ satisfies the property needed to be the Artin symbol of $\sigma(\mathfrak{P})$. Hence by the uniqueness of the Artin symbol

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$$

□

This has the following useful corollary as noted later in Janusz [14, pp. 102–103]:

Corollary 4.21. *If L/K is an abelian extension, then the Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right)$ depends only on the prime $\mathfrak{p}$ of K below $\mathfrak{P}$, hence we may write it as $\left(\frac{L/K}{\mathfrak{p}}\right)$.*

Proof. Let $\mathfrak{P}$, and $\mathfrak{P}'$ be two primes above $\mathfrak{p}$, then as the Galois group acts transitively, we can write $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in \mathrm{Gal}(L/K)$. Then

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$$

since the Galois group is abelian. □

From Janusz [14, pp. 100–101] we have the following simple results:

Proposition 4.22. *The order of the Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right)$ the inertial degree $f(\mathfrak{P} \mid \mathfrak{p})$.*

Proof. The Artin symbol generates the decomposition group $D_{\mathfrak{P}}$ which has order $f = f(\mathfrak{P} \mid \mathfrak{p})$, hence it has order $f(\mathfrak{P} \mid \mathfrak{p})$. □

Corollary 4.23. *A prime $\mathfrak{p}$ splits completely if and only if $\left(\frac{L/K}{\mathfrak{P}}\right) = 1$.*

Proof. If the Artin symbol of a prime above $\mathfrak{p}$ is trivial, it has order 1, hence $f = 1$. We already have $e = 1$, and so this means $\mathfrak{p}$ splits completely. □

We are now in a position to define the Artin map for an abelian extension L/K. In an extension L/K only a finite number of primes can ramify, any prime which ramifies in L/K sits above a prime p which ramifies in $L/\mathbb{Q}$. These primes divide the discriminant Δ_L, so there are only finitely many, and there are a finite number of primes in K above these.

Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. The fractional ideals of $\mathcal{I}_K(\mathfrak{m})$ are relatively prime to $\mathfrak{m}$, and so when we decompose $\mathfrak{a} \in \mathcal{I}_K(\mathfrak{m})$ as a product of primes:

$$\mathfrak{a} = \prod_{i=1}^{g} \mathfrak{p}_i^{r_i}$$

every prime $\mathfrak{p}_i$ is unramified in the extension, and hence its Artin symbol $\left(\frac{L/K}{\mathfrak{p}_i}\right)$ is defined. Extend the Artin symbol multiplicatively to all ideals $\mathfrak{a} \in \mathcal{I}_K(\mathfrak{m})$ via:

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{g} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

This gives the following definition:

Definition 4.24. Extending the Artin symbol multiplicatively to all of $\mathcal{I}_K(\mathfrak{m})$, defines a homomorphism:

$$\Phi_{L/K,\mathfrak{m}} \colon \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

called the Artin map of the extension L/K and the modulus $\mathfrak{m}$.

Example 4.25. Let us find the Artin map of the extension $K = \mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$. The extension is Galois with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \cong \{1, -1\}$. The discriminant of K is $\Delta_K = d$ or $\Delta_K = 4d$, so primes $p \nmid 4d$ are unramified in the extension. Take the modulus $\mathfrak{m} = 4d$, then any the fractional ideals $\mathcal{I}_K(\mathfrak{m})$ consist of ideals $(\frac{a}{b})$, where $\gcd(a, 4d) = \gcd(b, 4d) = 1$.

First let's work out the Artin symbol of the unramified primes. If p is an unramified prime of $\mathbb{Q}$, then the Legendre symbol $\left(\frac{d}{p}\right)$ tell us how the prime factors in the extension. If $\left(\frac{d}{p}\right) = 1$, then p splits, so $f = 1$ and the decomposition group is trivial, hence $\left(\frac{K/\mathbb{Q}}{(p)}\right) = 1 = \left(\frac{d}{p}\right)$. Otherwise $\left(\frac{d}{p}\right) = -1$, then p is inert so $f = 2$ and the decomposition group is $\{1, -1\}$, hence $\left(\frac{L/\mathbb{Q}}{(p)}\right) = -1 = \left(\frac{d}{p}\right)$.

Extending this multiplicatively to all ideals in $\mathcal{I}_K(\mathfrak{m})$ gives the map:

$$\begin{aligned} \Phi_{\mathfrak{m}} \colon \mathcal{I}_K(\mathfrak{m}) &\to \{1, -1\} \\ \frac{a}{b} &\mapsto \left(\frac{d}{a}\right)\left(\frac{d}{b}\right)^{-1} \end{aligned}$$

using the multiplicativity of the bottom argument of the Jacobi symbol, an extension of the Legendre symbol to all odd integers for the bottom argument. So the Artin map of a quadratic field is just the Jacobi symbol.

4.4 The Theorems of Class Field Theory

The Artin Reciprocity Theorem, Theorem 5.7 in Section 5.5 of Janusz [14] shows that the Galois group of any abelian extension is a generalised ideal class group for some modulus:

Theorem 4.26 (Artin Reciprocity Theorem)**.** *Let L/K be an abelian extension, and $\mathfrak{m}$ a modulus divisible by all primes, finite of infinite, or K which ramify in L. If the exponents of the primes dividing $\mathfrak{m}$ are sufficiently large then*

i) The Artin map $\Phi_{\mathfrak{m}}$ *is surjective*
ii) The kernel $\ker \Phi_{\mathfrak{m}}$ *is a congruence subgroup for* $\mathfrak{m}$
The isomorphism $\mathcal{I}_K(\mathfrak{m})/\ker \Phi_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$ *shows that* $\mathrm{Gal}(L/K)$ *is a generalised ideal class group for the modulus* $\mathfrak{m}$

Section 5.6 and Theorem 12.7 in Section 5.12 of Janusz [14, pp. 166–169 and p. 189] establish that there is one modulus which is better than others:

Theorem 4.27 (Conductor Theorem)**.** *Let* L/K *be an Abelian extension. Then there is a modulus* $\mathfrak{f} = \mathfrak{f}(L/K)$*, called the conductor, such that*
i) A prime of K *finite or infinite ramifies in* L *if and only if it divides* $\mathfrak{f}$
ii) Let $\mathfrak{m}$ *be a modulus divisible by all primes of* K *which ramify in* L*. Then the kernel* $\ker(\Phi)$ *of the Artin map* Φ *is a congruence subgroup for* $\mathfrak{m}$ *if and only if* $\mathfrak{f} \mid \mathfrak{m}$*.*

The Existence Theorem, Theorem 9.16 in Section 5.9 of Janusz [14] establishes that every generalised ideal class group is the Galois group of some abelian extension:

Theorem 4.28 (Existence Theorem)**.** *Let* $\mathfrak{m}$ *be a modulus of* K*, and let* H *be a congruence subgroup for* $\mathfrak{m}$*. Then there is a unique abelian extension* L *of* K*, all of whose ramified primes, finite or infinite, divide* $\mathfrak{m}$ *such that* H *is the kernel of the Artin map of* L/K*.*

A corollary to the uniqueness in the Existence theorem is given by Corollary 8.7 in Cox [7, p. 163]:

Corollary 4.29. *Let* L *and* M *be abelian extensions of* K*. Then* $L \subset M$ *if and only if there is a modulus* $\mathfrak{m}$*, divisible by all primes of* K *ramified in either* L *or* M *such that:*

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$$

4.5 Class Field Theory and Reciprocity Laws

Class Field Theory generalises the law of quadratic reciprocity and is the source of most other reciprocity laws.

We will prove Euler's statement of quadratic reciprocity, which is equivalent to the usual statement as given in Theorem 1.49. Euler's statement, as given in Lemmermeyer [17, p. 4–5], is the following:

Theorem 4.30 (Euler's Quadratic Reciprocity)**.** *Let* p *and* q *be odd primes, not dividing* $a > 0$*.*

$$\text{If } p \equiv q \pmod{4a} \text{ or } p \equiv -q \pmod{4a} \text{ then } \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

Proof. We can assume a is square-free and positive so let $K = \mathbb{Q}(\sqrt{a})$. From Example 3.11 in Milne [21], we have that the conductor of the extension $K/\mathbb{Q}$ is given by $\mathfrak{f} = \Delta_K$ since K is real.

Let the modulus $\mathfrak{m}$ be given by $\mathfrak{m} = 4a$. Then certainly $\mathfrak{f} \mid \mathfrak{m}$, so if $\Phi_{\mathfrak{m}}$ is the Artin map of the extension $K/\mathbb{Q}$, its kernel $\ker \Phi_{\mathfrak{m}}$ is a congruence subgroup for this modulus.

From the example above, we know the Artin map of this extension can be described in terms of the Jacobi symbol:

$$\left(\frac{K/\mathbb{Q}}{(p)}\right) = \left(\frac{a}{p}\right)$$

Since $\ker \Phi$ is a congruence subgroup we have $\mathcal{P}_{K,1}(\mathfrak{m}) \subset \ker \Phi$. But $p \equiv \pm q \pmod{4a}$ means $\pm pq^{-1} \equiv 1 \pmod{\mathfrak{m}_0}$. So the ideal (pq^{-1}) is in $\mathcal{P}_{K,1}(\mathfrak{m})$, and in particular in $\ker \Phi$. From this we have:

$$\left(\frac{a}{p}\right) = \left(\frac{K/\mathbb{Q}}{(p)}\right) = \left(\frac{K/\mathbb{Q}}{(q)}\right) = \left(\frac{a}{q}\right)$$

□

Using properties of the Artin symbol we can also give a direct proof of the more usual formulation of quadratic reciprocity. A special case of Propsition 3.11 in Lemmermeyer [17] gives us the following result:

Theorem 4.31 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes, then:*

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

Proof. Let $L = \mathbb{Q}(\zeta_q)$ be the q-th cyclotomic field. The unique quadratic subfield of L is given by $K = \mathbb{Q}(\sqrt{(-1)^{(q-1)/2}q})$, corresponding to the unique index 2 subgroup H of $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_q^*$. The subgroup H is the subgroup of squares since the map $x \mapsto x^2$ has kernel exactly $\overline{\pm 1}$.

From this and what we know of the Artin map of $K/\mathbb{Q}$, we have:

$$\left(\frac{(-1)^{(q-1)/2}}{p}\right) = 1 \Leftrightarrow \left(\frac{K/\mathbb{Q}}{(p)}\right) = 1$$

As in Corollary 3.10 of Lemmermeyer [17, p. 87–88], the restriction of $\left(\frac{L/\mathbb{Q}}{(p)}\right)$ to K coincides with $\left(\frac{K/\mathbb{Q}}{(p)}\right)$, therefore:

$$\left(\frac{K/\mathbb{Q}}{(p)}\right) = 1 \Leftrightarrow \left(\frac{L/\mathbb{Q}}{(p)}\right)\Bigg|_K = 1$$

Since K is the fixed field of the subgroup H, the Galois group is $K/\mathbb{Q}$ is $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}_q^*/H$, and so this means:

$$\left(\frac{L/\mathbb{Q}}{(p)}\right)\Bigg|_K = 1 \Leftrightarrow \left(\frac{L/\mathbb{Q}}{(p)}\right) \in H$$

One last fact that we need is the Artin map of $L/\mathbb{Q}$ can be described as: $\left(\frac{L/\mathbb{Q}}{(p)}\right) = \overline{p}$. This is remarked on just before Proposition 3.11 in Lemmermeyer [17, p. 88]. This tells us:

$$\begin{aligned}\left(\frac{L/\mathbb{Q}}{(p)}\right) \in H &\Leftrightarrow \overline{p} \in H \\ &\Leftrightarrow p \equiv x^2 \pmod{q} \\ &\Leftrightarrow \left(\frac{p}{q}\right) = 1\end{aligned}$$

and so establishes the required result. □

Chapter 5

The Hilbert Class Field

Our first application of the results of class field theory to the study of quadratic forms will use the Hilbert class field. Using the Hilbert class field we can determine whether or not a prime ideal is principal, and so study which primes the principal form represents in the positive-definite case. We will follow Cox [7] when studying binary quadratic forms with the Hilbert class field. Using the Hilbert class field we can also explore the class number of number fields as in Marcus [18] and Artin and Tate [1].

5.1 Definition and Properties

To define the Hilbert class field we appeal to the Existence Theorem:

Definition 5.1. The Hilbert class field of a number field K is the unique abelian extension of K arising from applying the existence theorem to the modulus $\mathfrak{m} = 1$, and the congruence subgroup $\mathcal{P}(K) = \mathcal{P}_{K,1}(1)$.

We call an extension L/K in unramified if all primes of K, both the finite and the infinite primes, are unramified in L. An alternative characterisation of the Hilbert class field is provided by Theorem 8.10 in Cox [7, p. 164]:

Theorem 5.2. *The Hilbert class field is the maximal unramified abelian extension of a number field.*

Proof. By construction the Hilbert class field is unramified and abelian: the ramified primes divide the modulus, but this is $\mathfrak{m} = 1$.

Let M be another unramified abelian extension of K. By the Conductor Theorem $\mathfrak{f}(M/K) = 1$ since a prime ramifies if and only if it divides the conductor. Then since $\mathfrak{f} \mid 1$, the kernel of the Artin map $\ker \Phi$ is a congruence subgroup for $\mathfrak{m} = 1$. So

$$\mathcal{P}_{K,1}(K) \subset \ker(\Phi_{M/K,1})$$

By the definition of the Hilbert class field we have:

$$\mathcal{P}_{K,1}(K) = \ker(\Phi_{L/K,1}) \subset \ker(\Phi_{M/K,1})$$

and hence $M \subset L$ follows from the Corollary to uniqueness. □

The Artin map induces an isomorphism between the class group of K and the Galois group of L/K, where L is the Hilbert class field of K. Using this we can link the ideal structure of K with the field structure of the extension and use this to study ideals of the number field. A special case of the results in the previous chapter tell us:

Proposition 5.3. *If L is the Hilbert class field of K, then the Artin map $\left(\frac{L/K}{\cdot}\right) : \mathcal{I}_K(1) = \mathcal{I}(K) \to \mathrm{Gal}(L/K)$ is surjective, and its kernel is the subgroup $\mathcal{P}_{K,1}(1) = \mathcal{P}(K)$ of principal ideals.*

From this we have the following corollaries:

Corollary 5.4. *If L is the Hilbert class field of K, then $\mathrm{Gal}(L/K) \cong \mathcal{C}(K)$, and hence $[L : K] = h(K)$.*

Proof. The First Isomorphism Theorem applied to the above says: $\mathrm{Gal}(L/K) \cong \mathcal{I}(K)/\mathcal{P}(K) = \mathcal{C}(K)$. The order of $\mathcal{C}(K)$ is by definition the class number $h(K)$. □

Corollary 5.5. *A prime ideal $\mathfrak{p}$ of K is principal if and only if it splits completely in L, the Hilbert class field of K.*

Proof. A prime ideal of K is principal if and only if $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. We know that the order of the Artin symbol is the inertial degree, hence $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$ if and only if $f = 1$. Since the extension L/K is unramified we necessarily have $e = 1$. So $\mathfrak{p}$ is principal if and only if $e = f = 1$ in the extension L/K, and this is precisely the condition that $\mathfrak{p}$ splits completely. □

Using this corollary we have a method to determine if a prime ideal is principal. Using the connection between quadratic forms and ideals in quadratic field we will answer the question of which primes a form represents by deriving a condition for (p) to split into principal ideals.

A useful result for later is given by Lemma 10 of Baker [2, p. 7]:

Proposition 5.6. *If $K/\mathbb{Q}$ is a Galois extension and L is the Hilbert class field of K, then $L/\mathbb{Q}$ is Galois.*

Proof. Let $\sigma\colon L \to \mathbb{C}$ be an embedding of L in $\mathbb{C}$ which fixes $\mathbb{Q}$ pointwise. Then $\sigma(L)$ is an unramified abelian extension of $\sigma(K)$, but since K is Galois $\sigma(K) = K$. Hence $\sigma(L)$ is an unramified abelian extension of K, and $\sigma(L) \subset L$. They have the same degree over K and so $\sigma(L) = L$. □

5.2 Class Number of Quadratic Fields

Class field theory shows there is an intimate relationship between the ideal class group of a number field K and the unramified abelian extension of k. We know the degree of the Hilbert class field L over a number field K is the class number $h(K)$ of K. If we can construct another unramified abelian extension M of K, then necessarily $M \subset L$, and by the tower theorem we have $[M : L] \mid [L : K] = h(K)$.

Using this insight we can prove some results on the divisibility of the class number for quadratic fields, and determine when the class number can possibly be 1.

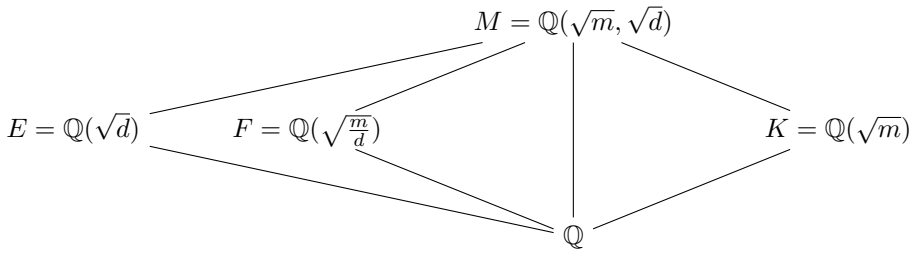
We first begin with a Lemma. The statement of the Lemma comes from part of Exercise 15 in Chapter 8 of Marcus [18, p. 246], tweaked to match up with our definitions.

Lemma 5.7. *Let m be a square-free integer, and let d be a non-trivial divisor of m. Assume that $d \equiv 1 \pmod 4$ or $\frac{m}{d} \equiv 1 \pmod 4$. Then $M = \mathbb{Q}(\sqrt{m}, \sqrt{d})$ is an abelian extension of $K = \mathbb{Q}(\sqrt{m})$ unramified at all finite primes.*

Proof. Firstly, the extension M/K is clearly Galois with abelian Galois group. One way to see this is by observing that $M/\mathbb{Q}$ is Galois with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$. The field K is the fixed field of a (necessarily) abelian subgroup, this subgroup is the Galois group of M/K.

Now we need to study the ramification of primes in the extension M/K. Without loss of generality, swapping d and $\frac{m}{d}$, we may assume that it is d which satisfies $d \equiv 1 \pmod 4$.

Now consider the following diagram of fields:



We can view M as the composite of the two quadratic subfields E and K. By calculating the discriminant we know exactly what primes ramify in a quadratic extension. We see that any prime $p \nmid 2m$ is unramified in K and in E since $\Delta_K \mid 4m$ and $\Delta_E \mid 4d$ where $d \mid m$. Since these primes are unramified in E and in K they are also unramified in the composite $EK = M$. Using the multiplicativity of the ramification index, any prime above p in K is unramified in M/K.

Now we need to look at the primes $p \mid 2m$. Firstly suppose that P is odd, and $p \mid m$, then let $\mathfrak{p}_K$ be a prime above p in K, ane $\mathfrak{P}$ a prime above $\mathfrak{p}_K$ in M. We need to show $e(\mathfrak{P} \mid \mathfrak{p}_K) = 1$. Since p divides m, and m is square-free it divides exactly one of d and $\frac{m}{d}$, say d (otherwise repeat the argument with d and $\frac{m}{d}$ interchanged). Let $\mathfrak{p}_F = \mathfrak{P} \cap \mathcal{O}_F$, this is a prime of F below $\mathfrak{P}$ and above p. By the multiplicativity of e in towers we have:

$$\begin{aligned} e(\mathfrak{P} \mid p) &= e(\mathfrak{P} \mid \mathfrak{p}_F) e(\mathfrak{p}_F \mid p) \\ &= e(\mathfrak{P} \mid \mathfrak{p}_K) e(\mathfrak{p}_K \mid p) \end{aligned}$$

Since $p \nmid \frac{m}{d}$, and p is odd we know p is unramified in F, so $e(\mathfrak{p}_F \mid p) = 1$. As always we have: $e(\mathfrak{P} \mid \mathfrak{p}_F) \leq [M : F] = 2$. Hence $e(\mathfrak{P} \mid p) \leq 1 \cdot 2 = 2$. On the other hand we have $e(\mathfrak{P}_K \mid p) = 2$ since p ramifies in K, and $e(\mathfrak{P} \mid \mathfrak{p}_K) \geq 1$ as always. Hence $e(\mathfrak{P} \mid p) \geq 2 \cdot 1 = 2$. From this we must have $e(\mathfrak{P} \mid p) = 2$, and so all the inequalities are in fact equalities. Hence $e(\mathfrak{P} \mid \mathfrak{p}_K) = 1$, and all the primes above p are unramified in M/K.

Lastly we need to look at $p = 2$. Since $d \equiv 1 \pmod 4$, 2 is unramified in E. If it is also unramified in K, it's unramified in the composite $M/\mathbb{Q}$, so the primes above 2 are unramified in L/K. Otherwise 2 ramifies in K, and the argument above using ramification indices again gives the primes above 2 are unramified in M/K.

Hence the extension is unramified at all finite primes as claimed. □

Now we are in a position to make some conclusions about the class number of certain quadratic fields. Firstly if we look at the imaginary quadratic fields $\mathbb{Q}(\sqrt{m})$, with $m < 0$, then the infinite primes are (trivially) unramified in any extension. So if we can apply the above Lemma to such a quadratic field, we will produce an unramified abelian extension which will sit as an intermediate field between the number field K and the Hilbert class field L. From this we conclude $2 \mid h(K)$, and in particular the class number isn't 1.

Example 5.8. Consider the number field $K = \mathbb{Q}(\sqrt{-35})$. We have $m = -35$, and we can take the non-trivial divisor $d = 5$. Then $d \equiv 1 \pmod 4$, and so the Lemma tells us that $M = \mathbb{Q}(\sqrt{-35}, \sqrt{5})$

is an abelian extension, unramified at all primes; it's unramified at the finite primes by the Lemma, and at the infinite primes since K is imaginary quadratic. We immediately conclude that $2 \mid h(K)$, and so K can't have class number $h(K) = 1$.

We can explicitly calculate the class number, if we do we find $h(K) = 2$. This confirms that $2 \mid h(K)$, but we can extract more from this. We know the Hilbert class field L has degree $[L : K] = h(K) = 2$, but we have a field M sitting between K and L, with degree $[M : K] = 2$. By the Tower theorem, we find $[L : M] = 1$, and so M *is* the Hilbert class field of K.

We can now go on to give a more general theorem which narrows down the possible window of odd class number, and in particular class number 1, for an imaginary quadratic field. The statement comes from a special case of part of Exercise 16 in Chapter 8 of Marcus [18]:

Theorem 5.9. *Let $K = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field (hence m square-free), and suppose $m \geq 3$. Then $h(K)$ is even except possibly when $m \equiv 3 \pmod 4$, and m is prime.*

Proof. Suppose that m is not prime, then we want to show that $h(K)$ is even. Since m is not prime, we can find a divisor $d \mid m$ of m. If $d \equiv 2 \pmod 4$, then $\frac{m}{d}$ can't be even, otherwise $4 \mid m$, but m was square-free. So by swapping d and $\frac{m}{d}$ we can assume $d \equiv 1, 3 \pmod 4$. Now if $d \equiv 3 \pmod 4$, we have $-d \equiv 1 \pmod 4$, so by negating we can assume $d \equiv 1 \pmod 4$. Now we're in a position to use the Lemma above: with this choice of d we know that $M = \mathbb{Q}(\sqrt{-m}, \sqrt{d})$ is an abelian extension unramified at all primes (including the infinite primes since K is imaginary quadratic). As before M sits between the Hilbert class field and K, and proves that $2 \mid h(K)$.

Now suppose that m is prime, but $m \not\equiv 3 \pmod 4$. As we're taking $m \geq 3$, this leaves the only possibility that $m \equiv 1 \pmod 4$, in particular $2 \nmid m$. We again want to construct an unramified abelian extension with degree 2 over K. Consider $M = \mathbb{Q}(\sqrt{-m}, \mathrm{i})$, clearly an abelian extension of K. As before, primes above $p \nmid m$ are unramified in M since p doesn't ramify in $\mathbb{Q}(\sqrt{-m})$ or $\mathbb{Q}(\mathrm{i})$ and so can't ramify in the composite field. Finally primes above $p \mid m$ are unramified in M by considering ramification indices in the subfields $E = \mathbb{Q}(\mathrm{i})$, and $K = \mathbb{Q}(\sqrt{-m})$. The infinite primes are automatically unramified since K is imaginary quadratic. So M is an unramified abelian extension with degree 2 over K. As before M sits between the Hilbert class field and K, and proves that $2 \mid h(K)$. □

5.3 Class Number of Subfields

It is not always the case that the class number of a subfield divides the class number of a field, for example consider:

$$K = \mathbb{Q}(\sqrt{-5}) \subset L = \mathbb{Q}(\sqrt{-5}, \mathrm{i})$$

It can be shown that L has class number $h(L) = 1$, but K has class number $h(K) = 2$.

Using class field theory we can determine a sufficient condition for the class number of K to divide the class number of an extension L.

Theorem 9 in Artin and Tate [1, p. 75] gives us the following result:

Theorem 5.10. *Let L be the Hilbert class field of K, and E be a finite dimension extension of K such that $E \cap L = K$. Then $h(K) \mid h(E)$.*

Proof. As in Proposition 3.18 of Milne [22, p. 38], there is an isomorphism $\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(L/E \cap L)$. By assumption $E \cap L = K$ so $\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(L/K)$, and hence the extension LE/E is abelian since L/K is abelian. It can be shown that the extension LE/E is also unramified.

Therefore LE is contained in the Hilbert class field F of E. We have $[LE : E] = [L : K] = h(K)$, so we conclude $h(K) \mid [F : E] = h(E)$. □

And using this we can prove the following theorem

Theorem 5.11. *Suppose some prime is totally ramified in the extension E/K. Then $h(K) \mid h(E)$.*

Proof. If $\mathfrak{p}$ is totally ramified in E/K, then we have $e = [E : L], f = 1$ for the single prime $\mathfrak{P}$ above $\mathfrak{p}$. In any intermediate field $K \subset M \subset E$, the prime $\mathfrak{p}$ must also ramify by the multiplicativity of the ramification index.

If L is the Hilbert class field of K, then we have $K \subset E \cap L \subset L$ and E. Any non-trivial extension of K contained in E is ramified, hence cannot be a subfield of the Hilbert class field. So the extension $E \cap L$ of K must be trivial. Therefore $E \cap L = K$. Then the previous Theorem immediate gives $h(K) \mid h(E)$. □

Example 5.12. It is show in Corollary 2 to Theorem 12 of Marcus [18, pp. 35–36] that the ring of integers of the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$ is always $\mathbb{Z}[\zeta_m]$, hence Dedekind's Theorem works to find the decomposition of all primes. Using this we can show that p is totally ramified in the p-th cyclotomic field $E = \mathbb{Q}(\zeta_p)$. The prime factorisation of p is given by the decomposition of the polynomial $\frac{x^p-1}{x-1}$ modulo p. Looking modulo p we find:

$$\frac{x^p - 1}{x - 1} \equiv \frac{(x-1)^p}{x-1} \equiv (x-1)^{p-1} \pmod{p}$$

so the prime p is totally ramified.

The previous theorem now tells us that the class number $h(K)$ of any subfield $K \subset E$ divides the class number $h(E)$ of E. In particular if p is an odd prime, the class number of the quadratic subfield $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ is a divisor of $h(E)$.

For $p = 23$, the quadratic subfield is $K = \mathbb{Q}(\sqrt{-23})$, which has class number 3. This means the class number of $E = \mathbb{Q}(\zeta_{23})$ is divisible by 3.

Similarly for $p = 47$, the quadratic subfield is $K = \mathbb{Q}(\sqrt{-47})$, which has class number 5. This means the class number of $E = \mathbb{Q}(\zeta_{47})$ is divisible by 5.

More details and results on the class numbers of the cyclotomic fields can be found in Chapter 11 of Washington [28].

Example 5.13. i) We can easily show the number of ideal classes in $E = \mathbb{Q}(\sqrt{-5}, \sqrt{-23})$ is divisible by 6 as follows. The subfield $K = \mathbb{Q}(\sqrt{-5})$ has class number $h(K) = 2$, and the subfield $M = \mathbb{Q}(\sqrt{-23})$ has class number $h(M) = 3$.

The prime $p = 23$ ramifies in M with $e(\mathfrak{p}_M \mid 23) = 2$, where $\mathfrak{p}_M$ is the prime above 23. Therefore in $E/\mathbb{Q}$ we have $e(\mathfrak{P} \mid 23) \geq 2$, where $\mathfrak{P}$ is a prime above 23. But $p = 23$ does not ramify in K, so $e(\mathfrak{p}_K \mid 23) = 1$ for any prime $\mathfrak{p}_K$ above 23. Hence we also have $e(\mathfrak{P} \mid 23) \leq 2$. From this we get $e(\mathfrak{P} \mid 23) = 2$, so for a prime $\mathfrak{p}_K$ above 23 in K we have $e(\mathfrak{P} \mid \mathfrak{p}_K) = 2 = [E : K]$, hence $\mathfrak{p}_K$ is totally ramified in E/K. With precisely the same argument a prime above $p = 5$ in M totally ramified in E/M.

From this the Theorem tells us $h(K) \mid h(E)$, and $h(M) \mid h(E)$. Therefore 2 and 3 divide $h(E)$, and so as claimed $6 \mid h(E)$.

ii) Extending this further, we can show the class number of $E = \mathbb{Q}(\sqrt{-5}, \sqrt{-23}, \sqrt{-47})$ is divisible by 30.

From above the subfield $K = \mathbb{Q}(\sqrt{-5}, \sqrt{-23})$ has class number divisible by 6. By the same argument the subfield $M = \mathbb{Q}(\sqrt{-5}, \sqrt{-47})$ has class number divisible by 10 since the class number of $\mathbb{Q}(\sqrt{-47})$ is 5.

The prime $p = 47$ is unramified in K, and ramifies in $\mathbb{Q}(\sqrt{-47})$ with $e = 2$. The same argument as above using the multiplicativity of e shows a prime $\mathfrak{p}_K$ above 47 in K is totally ramified in E/K. Hence $h(K) \mid h(E)$.

Similarly $p = 23$ is unramified in M, and ramifies in $\mathbb{Q}(\sqrt{-23})$ with $e = 2$. Therefore a prime $\mathfrak{p}_M$ above 23 in M is totally ramified in M/K. Hence $h(M) \mid h(E)$.

From this we get $10 \mid h(E)$, and $6 \mid h(E)$. Overall this means $30 \mid h(E)$, as claimed.

5.4 Representing Primes by Quadratic Forms

We will now put the Hilbert class field to use in determining which primes a binary quadratic form represents. We must restrict our attention to fundamental discriminants for our correspondence between forms and ideals works. Furthermore we will assume that the class group and the narrow class group are isomorphic and we have a correspondence between quadratic forms and ideal classes in the class group.

Using this correspondence we know that a prime p is represented b the binary quadratic form $q(x, y)$ if and only if there is an ideal of norm p in the ideal class corresponding to $q(x, y)$. In particular p is represented by the principal form if and only if there is a principal ideal of norm p.

We will work through a specific example from which we can then extract some general result. We will begin by re-deriving a result we achieved using genus theory.

Primes of the Form $x^2 + 6y^2$ Again

The form x^2+6y^2 corresponds to the principal ideal class in $K = \mathbb{Q}(\sqrt{-6})$, so we are really asking: is there a principal ideal of norm p in $K = \mathbb{Q}(\sqrt{-6})$. The question of determining whether an ideal is principal or not demands to look at the Hilbert class field.

We compute that the class number of K is $h(K) = 2$. From the results above we know that $L = \mathbb{Q}(\sqrt{-6}, \sqrt{-3}) = \mathbb{Q}(\sqrt{-6}, \sqrt{2})$ is an unramified abelian extension of K. By comparing degrees we see that it must be the Hilbert class field of K. The polynomial generating this extension is $f(x) = x^4 + 8x^2 + 64$ of discriminant $2^{22}3^2$.

Excluding the primes $p = 2, 3$ which ramify in K, there is a principal ideal of norm p in K if and only if (p) splits completely in K, and one (hence both) of these ideals is principal. If (p) splits into principal ideals in K, then since L is the Hilbert class field of K, these ideals split completely in L. The multiplicativity of e and f means that (p) splits completely in $L/\mathbb{Q}$.

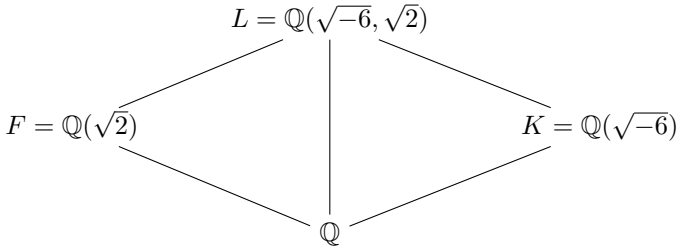
Conversely if (p) splits completely in $L/\mathbb{Q}$, then (p) splits completely in K into ideals which split completely in L/K. But by properties of the Hilbert class field, this means that (p) splits into principal ideals in K.

Since $K/\mathbb{Q}$ is a Galois extension $L/\mathbb{Q}$ is also Galois, so complete splitting of (p) is equivalent to there being a prime $\mathfrak{P}$ above p with $e(\mathfrak{P} \mid p) = f(\mathfrak{P} \mid p) = 1$. Applying Dedekind's Theorem to the extension $L/\mathbb{Q}$ says that for $p \neq 2, 3$, the decomposition of (p) corresponds to the factorisation of $f(x)$ modulo p. Hence (p) splits completely in $L/\mathbb{Q}$ if and only if $f(x)$ has a linear factor modulo p, and this is simply if and only if $f(x)$ has a root modulo p.

So our first criterion in this case is that for $p \neq 2, 3$:

$$p = x^2 + 6y^2 \Leftrightarrow x^4 + 8x^2 + 64 \text{ has a root modulo } p$$

Can we derive from this our previous criterion? Yes. Consider the field diagram:



The field F is the fixed field of L under complex conjugation, and the composite FK is the Hilbert class field L. The polynomial $g(x) = x^2 - 2$, of discriminant 2^3, which generates the extension $F/\mathbb{Q}$ also generates the extension L/K, and so we can relate the decomposition in each of these extensions using Dedekind's Theorem.

From our analysis above we know that $p \neq 2, 3$ is represented by $x^2 + 6y^2$ if and only if (p) splits completely in K as $p\mathcal{O}_K = \mathfrak{p}\widetilde{\mathfrak{p}}$, and $\mathfrak{p}$ splits completely in L. Modulo p the polynomial $g(x)$ is separable, and since $f(\mathfrak{p} \mid p) = 1$ so $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$, it is also separable modulo $\mathfrak{p}$. Applying Dedekind's Theorem and using that L/K is Galois we get that $\mathfrak{p}$ splits completely in L/K if and only if $g(x)$ has a root modulo $\mathfrak{p}$ which is equivalent to $g(x)$ has a root modulo p.

Our criterion then becomes for $p \neq 2, 3$:

$$p = x^2 + 6y^2 \Leftrightarrow \begin{cases} \left(\frac{-6}{p}\right) = 1 \text{ and} \\ x^2 - 2 \text{ has a root modulo } p \end{cases}$$

From this version we can extract our previous criterion; we need $\left(\frac{-6}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = 1$. Quadratic reciprocity says this is equivalent to $p \equiv 1, 7 \pmod{24}$.

We also have another example of how the interaction between number fields and Galois theory forces a strict behaviour on a polynomial. As in a previous example, the polynomial $f(x) = x^4 + 8x^2 + 64$ is reducible modulo every prime. Now we can say that if $p \equiv 1, 7 \pmod{24}$, the polynomial has a root, and since it generates a Galois extension, it splits into 4 linear factors. Otherwise the polynomial doesn't have a root, and so can only split into 2 quadratic factors.

From this we can now state the abstract criterion which determines when a prime is represented by the form corresponding to the principal ideal class. The statement is a generalisation of Theorem 5.26 in Cox [7, p. 100].

Theorem 5.14. *Suppose the narrow class group and the class group are isomorphic in the quadratic field $K = \mathbb{Q}(\sqrt{d})$, and let $q(x, y)$ be the quadratic form corresponding to the principal ideal class. Let L be the Hilbert class field of K. For a prime p not dividing the discriminant Δ_K, we have:*

$$p \text{ is represented by } q(x, y) \Leftrightarrow (p) \text{ splits completely in } L$$

Proof. The proof goes through pretty much as in the example above.

The correspondence between forms and ideals tells us that $q(x, y)$ represents the prime p if and only if there is a principal ideal of norm p in K. Primes which don't divide the discriminant are unramified, hence for these primes there is a an ideal of norm p if and only if the prime (p) of $\mathbb{Q}$ splits completely in K.

If one (and hence both) of the ideals above (p) is principal, then it splits completely in L/K. By the multiplicativity of e and f this shows that (p) splits completely in $L/\mathbb{Q}$. Conversely if (p) splits completely in $L/\mathbb{Q}$, then it splits completely in $K/\mathbb{Q}$ into ideals which split completely in L/K. Since L is the Hilbert class field of K this means (p) splits into principal ideals. □

A quadratic field K is always Galois over $\mathbb{Q}$, and so by a previous proposition the Hilbert class field of K is also Galois over $\mathbb{Q}$. In the situation above we can describe complete splitting easily, and we get the following criterion:

Proposition 5.15. *Let everything be as in the previous Theorem, and suppose the Hilbert class field $L/\mathbb{Q}$ is generated by the polynomial $f(x)$. Then a prime p not dividing Δ_K and not dividing the discriminant of f is represented by the form $q(x, y)$ if and only if the polynomial $f(x)$ has a root modulo p.*

Proof. By the previous Theorem we have that such p is represented by $q(x, y)$ if and only if (p) splits completely in $L/\mathbb{Q}$. Since the extension $L/\mathbb{Q}$ is Galois this is equivalent to there being a prime $\mathfrak{P}$ above (p) with $e(\mathfrak{P} \mid p) = f(\mathfrak{P} \mid p) = 1$. As the prime doesn't divide the discriminant of f we can apply Dedekind's Theorem. It says that there is such a prime $\mathfrak{P}$ above (p) if and only if the polynomial $f(x)$ has a linear factor modulo p. This means $f(x)$ has a root modulo p. □

By looking at the fixed field of L under the conjugation automorphism of K we can find a simpler criterion. An adaption of Proposition 5.29 in Cox [7, p. 111] gives us the following results:

Proposition 5.16. *Let L be an extension of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, such that $L/\mathbb{Q}$ is Galois. Then:*

i) L can be written as $K(\alpha)$, where α is the root of some monic polynomial $f(x) \in \mathbb{Z}[x]$. That is L is the composite of K and some $\mathbb{Q}(\alpha)$.

ii) If p is an odd prime not dividing Δ_K and not dividing discriminant of $f(x)$, then:

$$p \text{ splits completely in } L \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

Proof. For i) the conjugation automorphism of K extends to an automorphism of L. Let $F = \mathbb{Q}(\alpha)$ be the fixed field of L under conjugation, then $[L : F] = 2$, and $[F : \mathbb{Q}] = [L : K]$. Certainly $KF \subset L$, however since $K \not\subset F$ we have $KF \neq F$, hence $[L : KF] = 1$, and so they are equal. We can choose α to be an algebraic integer, hence it is the root of a monic polynomial. We read off the the degree of the minimal polynomial of α over $\mathbb{Q}$ has degree $[F : \mathbb{Q}] = [L : K]$.

For ii) we know (p) splits completely in L is equivalent to (p) splits in K as $p\mathcal{O}_K = \widetilde{\mathfrak{p}\mathfrak{p}}$, and one (hence both) of the primes of K above (p) splits completely in L. Splitting in K is equivalent to $\left(\frac{d}{p}\right) = 1$. Since $f(\mathfrak{p} \mid p) = 1$, we have $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. As p doesn't divide the discriminant of $f(x)$, the polynomial is separable modulo p, and so separable modulo $\mathfrak{p}$. Therefore $\mathfrak{p}$ splits completely in L/K if and only if $f(x)$ has a root modulo $\mathfrak{p}$, which is if and only if $f(x)$ has a root modulo p. □

In particular these results apply to the Hilbert class field, and will allow us to write down a criterion with a standard form. This leads immediately to the main theorem, Theorem 5.1, of Section 5 of Cox [7], a generalisation of which is:

Theorem 5.17. *Suppose the narrow class group and the class group of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ are isomorphic. Let $q(x, y)$ be the quadratic form corresponding to the principal ideal class in K. Then there is a polynomial $f(x)$ of degree $h(K) = h(\Delta_K)$ such that for p an odd prime not dividing Δ_K or the discriminant of $f(x)$, we have:*

$$p \text{ is represented by } q(x, y) \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

This polynomial can be taken to be the minimal polynomial of the algebraic integer α for which $L = K(\alpha)$ is the Hilbert class field of K.

The main problem now is actually computing the Hilbert class field of the quadratic field we are interested in. This is not a simple matter, but various methods and algorithms have been developed to compute class fields in general. For the purposes of this report we won't spend time looking at them. The computer algebra system Magma [26] implements algorithms to compute class fields, and so if need be we can simply take the output as given.

Several sections of Cohen [5] are devoted to developing algorithms to compute the Hilbert class field of a number field. With these Cohen draws up tables giving the Hilbert class field for a range of real and imaginary quadratic fields. These tables are found in Section 12.1, Appendix C, of Cohen [5, pp. 533–542].

Using these we can give some further examples in the positive-definite and indefinite cases, for odd and even fundamental discriminants. In some cases we can even obtain results for non-fundamental discriminants without needing any further theory.

Primes of the Form $x^2 + xy + 6y^2$ and $x^2 + 23y^2$

The form $x^2 + xy + 6y^2$ of discriminant $D = -23$ corresponds to the principal ideal class in the quadratic field $K = \mathbb{Q}(\sqrt{-23})$. Cohen says the Hilbert class field of K is given by $L = K(\alpha)$, where α is a root of the polynomial $f(x) = x^3 - x^2 + 1$, of discriminant -23.

In this case it is not *too* difficult to prove L is the Hilbert class field of K. Firstly calculate that the class number of K is $h(K) = 3$. We need to show that L/K is an unramified abelian extension of degree 3.

Since the discriminant of $x^3 - x^2 + 1$ is -23, we know from Galois theory that the splitting field of $f(x) = x^3 - x^2 + 1$ is given by $\mathbb{Q}(\alpha, \sqrt{-23})$. In particular the extension $L/\mathbb{Q}$ is Galois with Galois group S_3. This shows the extension L/K is Galois, and since it is of degree $[L : K] = 3$, its Galois group must be $\mathbb{Z}_3$. Therefore L/K is an Abelian extension. Its degree is equal to the class number of K, so all we need to show it that it is unramified.

Since K is imaginary quadratic, the infinite primes are automatically unramified. Since disc $f = -23$ is square-free, the discriminant of F must be -23, and its ring of integers is $\mathbb{Z}[\alpha]$. The discriminant of $F = \mathbb{Q}(\alpha)$ and of K is -23, so a prime $p \nmid 23$ is unramified in both of these, and hence is unramified in the composite L. Therefore any prime above $p \nmid 23$ is unramified in L/K. Now we look at the primes above 23. Since the ring of integers of F is given by $\mathbb{Z}[\alpha]$, Dedekind's Theorem works to give the decomposition of all primes. In particular for $p = 23$ we have:

$$x^3 - x^2 + 1 \equiv (x + 7)^2(x + 8) \pmod{23}$$

And so the decomposition of $23\mathcal{O}_F$ is given by:

$$23\mathcal{O}_F = (23, \alpha + 7)^2(23, \alpha + 8)$$

Let $\mathfrak{p}_K$ be a prime of K above $p = 23$, and let $\mathfrak{P}$ be a prime of L above $\mathfrak{p}_K$. Then $\mathfrak{p}_F = \mathfrak{P} \cap \mathcal{O}_F$ is a prime of F above 23 and below $\mathfrak{P}$. We need to show that $e(\mathfrak{P} \mid \mathfrak{p}_K) = 1$, so the prime $\mathfrak{p}_K$ of K is unramified in L. By the multiplicativity of e we have:

$$\begin{aligned} e(\mathfrak{P} \mid 23) &= e(\mathfrak{P} \mid \mathfrak{p}_F)e(\mathfrak{p}_F \mid 23) \\ &= e(\mathfrak{P} \mid \mathfrak{p}_K)e(\mathfrak{p}_K \mid 23) \end{aligned}$$

We know L/K is Galois, so $e(\mathfrak{P} \mid \mathfrak{p}_K)$ is a divisor of 3. We know that $e(\mathfrak{p}_K \mid 23) = 2$, since 23 ramifies in K, and $[K : \mathbb{Q}] = 2$. We also have that $e(\mathfrak{p}_F \mid 23) = 1$ or 2, from the decomposition above. Overall this tells us that $e(\mathfrak{P} \mid 23) = e(\mathfrak{P} \mid \mathfrak{p}_F)e(\mathfrak{p}_F \mid 23) \leq 2 \cdot 2 = 4$. Therefore $e(\mathfrak{P} \mid \mathfrak{p}_K) = 3$ is not possible, and we must have $e(\mathfrak{P} \mid \mathfrak{p}_K) = 1$.

Hence L is an unramified abelian extension of K with degree $[L:K] = h(K) = 3$. So L is a subfield of the Hilbert class field, and by the Tower Theorem the Hilbert class field has degree 1 over L. Therefore L is the Hilbert class field of K as claimed.

Now we can use this to find a criterion on which primes the principal form represents. Theorem 5.17 says for $p \neq 2, 23$:

$$p = x^2 + xy + 6y^2 \Leftrightarrow \begin{cases} \left(\frac{-23}{p}\right) = 1 \text{ and} \\ x^3 - x^2 + 1 \text{ has a root modulo } p \end{cases}$$

Using the identity:

$$(x + \tfrac{y}{2})^2 + 23(\tfrac{y}{2})^2 = x^2 + xy + 6y^2$$

we see that if we can write p as $x^2 + xy + 6y^2$ with y even, then we can also write it in the form $x^2 + 23y^2$. Conversely if we can write p as $x^2 + 23y^2$, then we can always go back the other way and write it as $x^2 + xy + 6y^2$.

If we exclude $p = 2$, then the prime p is odd. Reducing the equation $p = x^2 + xy + 6y^2$ modulo 2, we obtain:

$$1 \equiv x^2 + xy \equiv x(x + y) \pmod 2$$

Hence x is odd, and y is even. So any prime $p \neq 2$ which can be written as $x^2 + xy + 6y^2$ has y even, and so can be written as $x^2 + 23y^2$ as well.

Combining with the previous this gives for $p \neq 2, 23$:

$$p = x^2 + 23y^2 \Leftrightarrow \begin{cases} \left(\frac{-23}{p}\right) = 1 \text{ and} \\ x^3 - x^2 + 1 \text{ has a root modulo } p \end{cases}$$

Primes of the Form $x^2 + 29y^2$

The form $x^2 + 29y^2$ of discriminant $D = -116$ corresponds to the principal ideal class in $K = \mathbb{Q}(\sqrt{-29})$. Cohen says the Hilbert class field of K is given by $L = K(\alpha)$, where α is a root of the polynomial $f(x) = x^6 - 2x^3 + x^2 + 2x + 2$, of discriminant $-2^{10}29^2$.

So we get that for $p \neq 2, 29$:

$$p = x^2 + 29y^2 \Leftrightarrow \begin{cases} \left(\frac{-29}{p}\right) = 1 \text{ and} \\ x^6 - 2x^3 + x^2 + 2x + 2 \text{ has a root modulo } p \end{cases}$$

Primes of the Form $x^2 + xy - 64y^2$ and $x^2 - 257y^2$

The quadratic field $K = \mathbb{Q}(\sqrt{257})$ has fundamental unit $u = 16 + \sqrt{257}$ of norm -1. This means the class group and the narrow class group are isomorphic. The form $x^2 + xy - 64y^2$ of discriminant $D = 257$ corresponds to the principal ideal class in K. Cohen says the Hilbert class field of K is given by $K(\alpha)$ where α is a root of the polynomial $x^3 - x^2 - 4x + 3$ of discriminant 257.

Thus we have for $p \neq 2, 257$:

$$p = x^2 + xy - 64y^2 \Leftrightarrow \begin{cases} \left(\frac{257}{p}\right) = 1 \text{ and} \\ x^3 - x^2 - 4x + 3 \text{ has a root modulo } p \end{cases}$$

As before we can make use of the identity:

$$x^2 + xy - 64y^2 = (x + \tfrac{y}{2})^2 - 257(\tfrac{y}{2})^2$$

to write a prime of the form $x^2+xy-64y^2$ as x^2-257y^2 if y is even. Excluding $p=2$ and reducing modulo 2 shows any odd prime written $x^2+xy-64y^2$ necessarily has y even so is of the form x^2-257y^2.

This gives for $p \neq 2, 257$:

$$p = x^2 - 257y^2 \Leftrightarrow \begin{cases} \left(\frac{257}{p}\right) = 1 \text{ and} \\ x^3 - x^2 - 4x + 3 \text{ has a root modulo } p \end{cases}$$

Now we can easily produce a list of primes these forms represent, and so definitively answer the question of whether or not certain primes are represented. Excluding $p = 2, 257$, both forms represent the same primes, and this list begins:

$$61, 67, 113, 157, 193, 197, 227, 241, 419, 499, 587, 631, 643,$$
$$653, 739, 821, 823, 859, 863, 907, 929, 947, 971, 997, \ldots$$

5.5 Representing Primes by Higher Forms

We can apply these results and ideas more widely. By relating norms and principal ideals in a higher degree field we can analyse the situation using the Hilbert class field and extract from this conditions on when there are elements of a given norm. Here I will generalise the results to study some cubic forms.

Primes of the Form $a^3 + 11b^3 + 121c^3 - 33abc$

I will find a condition for a prime p to be represented by the ternary cubic form:

$$a^3 + 11b^3 + 121c^3 - 33abc$$

The first thing to do it to recognise this cubic form as the norm form on $\mathbb{Z}[\sqrt[3]{11}]$, the ring of integers of $K = \mathbb{Q}(\sqrt[3]{11})$, and so to translate the question to: is there an element of norm p in $\mathcal{O}_K$. Since the unit -1 has negative norm we can choose the generator of a principal ideal of norm p to have positive norm, and so the existence of an element of norm p is equivalent to the existence of a principal ideal of norm p.

As a note, this field $K = \mathbb{Q}(\sqrt[3]{11})$ has class number $h(K) = 2$, and so the existence of an ideal of norm p is not sufficient to guarantee it is principal.

Since the extension $K/\mathbb{Q}$ is not Galois, the decomposition of the prime p in K is more erratic. Ignoring concerns about ramification which will be captured as a repeated factor, the possible decompositions in K are given by:

$$p\mathcal{O}_K \text{ is inert}$$
$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{q}_1$$
$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

where the primes $\mathfrak{p}_i$ have inertial degree 1, so norm p, and the prime $\mathfrak{q}_1$ has inertial degree 2, so norm p^2, and in the inert case $p\mathcal{O}_K$ has inertial degree 3, so norm p^3. From this we see there is an ideal of norm p if and only if the prime p of $\mathbb{Q}$ splits in K. But when is this ideal principal?

Magma tells us the Hilbert class field of K is $L = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $f(x) = x^6 - 15x^4 + 9x^2 - 4$ of discriminant $2^8 3^{10} 11^4$. We shall show that, for $p \neq 2, 3, 11$, there is a principal ideal of norm p in K if and only if $f(x)$ has a root modulo p.

Suppose there is a principal ideal $\mathfrak{p}$ of norm p. Then in the extension L/K, the ideal $\mathfrak{p}$ splits completely, so there is an ideal $\mathfrak{R}$, with $e(\mathfrak{R} \mid \mathfrak{p}) = f(\mathfrak{R} \mid \mathfrak{p}) = 1$. For $p \neq 2, 3, 11$ we are unramified in $L/\mathbb{Q}$ and hence in $K/\mathbb{Q}$, so we have $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$, and by the multiplicativity:

$$e(\mathfrak{R} \mid p) = 1$$
$$f(\mathfrak{R} \mid p) = 1$$

We can apply Dedekind's Theorem to the extension $L/\mathbb{Q}$ to obtain the decomposition of p in L, doing so tells us the polynomial $f(x)$ must have a linear factor modulo p, in order to give rise to the ideal $\mathfrak{R}$ above. Hence $f(x)$ has a root modulo p.

Now suppose $f(x)$ has a root modulo p. Then for $p \neq 2, 3, 11$, this tells us there is a prime $\mathfrak{R}$ in L above p with:

$$e(\mathfrak{R} \mid p) = 1$$
$$f(\mathfrak{R} \mid p) = 1$$

This prime $\mathfrak{R}$ sits above a prime $\mathfrak{p}$ of K, and so by the multiplicativity of e and f we must have:

$$e(\mathfrak{R} \mid \mathfrak{p}) = 1$$
$$f(\mathfrak{R} \mid \mathfrak{p}) = 1$$

and since L/K is Galois, this tells us $\mathfrak{p}$ splits completely in L/K, hence is principal. By the multiplicativity of f in a tower of fields, we also have $f(\mathfrak{p} \mid p) = 1$, and hence $\mathfrak{p}$ has norm p. So $\mathfrak{p}$ is a principal ideal of norm p.

Therefore there is a principal ideal of norm p in K if and only if the polynomial $f(x)$ has a root modulo p. Combined with our earlier observation we get the following: for $p \neq 2, 3, 11$:

$$p = a^3 + 11b^3 + 121c^3 - 33abc \Leftrightarrow t^6 - 15t^4 + 9t^2 - 4 \text{ has a root modulo } p$$

This gives an easy condition which is checkable in finite time so we can produce a complete list of primes, except possibly for $p = 2, 3, 11$, that this form represents. The list begins:

$$19, 29, 37, 43, 53, 61, 71, 83, 89, 107, 113, 131, 167, 173, 179, 193, 199, 211,$$
$$227, 229, 233, 239, 281, 293, 311, 337, 349, 353, 389, 409, 431, 457, 461, 467, \ldots$$

From this we can see that even though the prime 5 splits in K, using Dedekind and that $x^3 - 11$ has a root $x = 1$ modulo 5, and hence there is an ideal of norm 5, there is no *principal* ideal of norm 5. Consequently the Diophantine equation:

$$5 = a^3 + 11b^3 + 121c^3 - 33abc$$

has no solutions in integers.

Precisely the same analysis works for any number field to determine when there is a principal ideal of norm p. As long as we can relate the existence of ideals of norm p and the existence of elements of norm p we can then tell when there is an element of norm p. This will then tell us what primes p the norm form on $\mathcal{O}_K$ represents.

Primes of the Form $a^3 + 7b^3 + 49c^3 - 21abc$

The cubic form $a^3+7b^3+49c^3-21abc$ is the norm form on the ring of integers $\mathbb{Z}[\sqrt[3]{7}]$ of $K = \mathbb{Q}(\sqrt[3]{7})$. Again multiplying by -1 allows us to take the generator of a principal ideal of norm p to have

positive norm. So this form represents the prime p if and only if there is a principal ideal of norm p in K.

The field $K = \mathbb{Q}(\sqrt[3]{7})$ has class number $h(K) = 3$, so we actually do need to determine when there is a principal ideal of norm p. Magma tells us the Hilbert class field of K is $\mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^9 - 9x^7 - 69x^6 + 27x^5 + 414x^4 + 1560x^3 - 621x^2 - 4761x - 1583$ of discriminant $-2^{18}3^{39}7^{14}71^2$.

The same analysis as before then tells us that for $p \neq 2, 3, 7, 71$ there is a principal ideal of norm p if and only if the polynomial $f(x)$ has a root modulo p. This gives the condition for $p \neq 2, 3, 7, 71$ that:

$$p = a^3 + 7b^3 + 49c^3 - 21abc \Leftrightarrow \begin{cases} x^9 - 9x^7 - 69x^6 + 27x^5 + 414x^4 + 1560x^3 \\ \quad - 621x^2 - 4761x - 1583 \text{ has a root modulo } p \end{cases}$$

Using this condition we can produce a list of primes, except possibly $p = 2, 3, 7, 71$, that the form represents. The list begins:

$$29, 41, 83, 113, 167, 181, 197, 223, 239, 251, 281, 293, 337, 419, 421, 449, 461, 463, 491,$$
$$503, 587, 617, 659, 673, 701, 743, 769, 797, 811, 827, 839, 853, 881, 883, 911, 953, \ldots$$

Chapter 6

Other Class Fields

The Hilbert class field is very useful for analysing when a prime is represented by the principal for an imaginary quadratic field, and certain real quadratic fields. Once we move to a general real quadratic field the Hilbert class field is no longer able to distinguish whether the form represents p or $-p$. For this reason we introduce the narrow class field.

To answer the question of which primes a non-principal form represents we look at class fields arising from subgroups of the class group or narrow class group. These class fields can detect when an ideal lies in the given subgroup, hence when a prime p is represented by a certain subset of quadratic forms. Using an inclusion-exclusion style procedure we can pin down criteria for a prime to be represented by some non-principal forms.

These results are some generalisations of the results in Cox [7], spurred on by the introduction of the narrow class field in Section 6.3 of Janusz [14, p. 203] and the mention of class fields for subgroups of the class group in Theorem 0.1 of Milne [21, p. 2].

6.1 The Narrow Class Field

To define the narrow class field (also called the narrow Hilbert class field, or the extended Hilbert class field in some texts) we again appeal to the Existence Theorem and make the following definition:

Definition 6.1. The narrow class field of a number field K is the unique abelian extension of K arising from applying the existence theorem to the modulus $\mathfrak{m}$ consisting of all real infinite primes of K, and the congruence subgroup $\mathcal{P}^+(K) = \mathcal{P}_K(\mathfrak{m})$.

Since an imaginary quadratic field has no real infinite primes, this definition just reduces to that of the Hilbert class field in the imaginary quadratic case. This section is a generalisation of the results of the previous chapter to the case of all real quadratic fields and the corresponding indefinite quadratic forms.

An alternative characterisation of the narrow class field is provided by the following theorem:

Theorem 6.2. *The narrow class field is the maximal abelian extension of a number field unramified at all finite primes.*

Proof. The proof is analogous to the corresponding result for the Hilbert class field.

The narrow class field is unramified at all the finite primes and is abelian since the ramified primes divide the defining modulus $\mathfrak{m}$ above. Let M be another abelian extension unramified at all the finite primes.

By the Conductor Theorem $\mathfrak{f}(M/K)$ must divide $\mathfrak{m}$, and hence $\ker(\Phi_{M/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. By the definition of the narrow class field we have:

$$\mathcal{P}_{K,1}(\mathfrak{m}) = \ker(\Phi_{L/K,\mathfrak{m}}) \subset \ker(\Phi_{M/K,\mathfrak{m}})$$

from this and the Corollary to uniqueness it follows that $M \subset L$. □

The Artin map for this class field gives the following:

Proposition 6.3. *If L is the narrow class field of K, then the Artin map $\left(\frac{L/K}{\cdot}\right): \mathcal{I}_K(\mathfrak{m}) = \mathcal{I}(K) \to \mathrm{Gal}(L/K)$ is surjective and its kernel is the subgroup $\mathcal{P}_{K,1}(\mathfrak{m}) = \mathcal{P}^+(K)$.*

Corollary 6.4. *If L is the narrow class field of K, then $\mathrm{Gal}(L/K) \cong \mathcal{C}^+(K)$, in particular $[L:K] = h^+(K)$.*

Proof. The First Isomorphism Theorem applied to the above says: $\mathrm{Gal}(L/K) \cong \mathcal{I}(K)/\mathcal{P}^+(K) = \mathcal{C}^+(K)$. The order of $\mathcal{C}^+(K)$ is by definition the class number $h^+(K)$. □

And as before, from the properties of the Artin symbol we get the following result:

Corollary 6.5. *A prime ideal $\mathfrak{p}$ of K is a totally positive principal ideal if and only if it splits completely in L, the narrow class field.*

Proof. A prime ideal $\mathfrak{p}$ of K is a totally positive principal ideal if and only if $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. We know that the order of the Artin symbol is the inertial degree, hence $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$ if and only if $f = 1$. Since the extension L/K is unramified we necessarily have $e = 1$. So $\mathfrak{p}$ is a totally positive principal ideal if and only if $e = f = 1$ in the extension L/K, and this is precisely the condition that $\mathfrak{p}$ splits completely. □

Using this result we have a method to determine if a prime ideal is a totally positive principal ideal, and so by the connection to quadratic forms, we can tell which primes an indefinite form represents by determining when (p) splits into totally positive principal ideals.

Like before we have the following useful result:

Proposition 6.6. *If $K/\mathbb{Q}$ is a Galois extension and L is the narrow class field of K, then $L/\mathbb{Q}$ is Galois.*

Proof. If σ is any embedding of L into $\mathbb{C}$ which fixes $\mathbb{Q}$ pointwise, then $\sigma(L)$ is an abelian extension of $\sigma(K)$ unramified at all finite primes. Since $K/\mathbb{Q}$ is Galois $\sigma(K) = K$, so $\sigma(L)$ is contained in the narrow class field of K. Comparing degrees shows $\sigma(L) = L$. Therefore $L/\mathbb{Q}$ is Galois. □

We can use the narrow class field to prove results on the narrow class number of a number field. We have the following result on the narrow class number of a real quadratic field:

Theorem 6.7. *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field (hence m square-free), and suppose $m \geq 3$. Then $h^+(K)$ is even except possibly when $m \equiv 1 \pmod 4$ and m is prime.*

Proof. The proof is identical to Theorem 5.9. We don't need to worry about the infinite primes ramifying as they may ramify in the narrow class field. □

We will re-derive some earlier results on primes represented by quadratic forms to get a feel for how the narrow class field works. Then we can use it to go even further.

Primes of the Form $x^2 - 3y^2$ Again

The form $x^2 - 3y^2$ corresponds to the totally positive principal ideal class in $K = \mathbb{Q}(\sqrt{3})$, so we need to look at the narrow class field of K. The narrow class number of K is $h^+(K) = 2$, since the field K has class number $h(K) = 1$, and the fundamental unit of K is $u = 2 + \sqrt{3}$, which has norm $N(u) = 1$. Therefore the narrow class field has degree 2 over K.

From earlier results we know that $L = \mathbb{Q}(\sqrt{3}, \mathrm{i})$ is an abelian extension of K which is unramified at all finite primes. Thus it is contained in the narrow class field of K. Moreover they have the same degree over K. Therefore L is the narrow class field of K.

A prime p is represented by $x^2 - 3y^2$ if and only if there is a totally positive principal ideal of norm p in K. There is a totally positive principal ideal of norm p if and only if the prime (p) of $\mathbb{Q}$ splits into totally positive principal ideals in K, and by the properties of the Artin symbol these split completely in L/K, hence (p) splits completely in $L/\mathbb{Q}$. Vice versa if (p) splits completely in $L/\mathbb{Q}$ it splits into two ideals in K which split completely in L/K, hence the ideals are totally positive principal ideals.

The polynomial generating the narrow class field over $\mathbb{Q}$ is $f(x) = x^4 - 4x^2 + 16$ of discriminant $2^{16}3^2$. As before, complete splitting of (p) in $L/\mathbb{Q}$ is equivalent to $f(x)$ having a root modulo p, for primes not dividing the discriminant.

For $p \neq 2, 3$:

$$p = x^2 - 3y^2 \Leftrightarrow x^4 - 4x^2 + 16 \text{ has a root modulo } p$$

Viewing L as $K(\mathrm{i})$, so as the composite of K and $F = \mathbb{Q}(\mathrm{i})$, the condition for complete splitting becomes splitting in K and in F, just as before. The polynomial generating F is $g(x) = x^2 + 1$ of discriminant -2^2, so the condition becomes, for $p \neq 2, 3$:

$$p = x^2 - 3y^2 \Leftrightarrow \begin{cases} \left(\frac{3}{p}\right) = 1 \text{ and} \\ x^2 + 1 \text{ has a root modulo } p \end{cases}$$

In terms of the Legendre symbol this is $\left(\frac{3}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$, which by quadratic reciprocity is equivalent to $p \equiv 1 \pmod{12}$, just as we found with genus theory.

Since the narrow class field of a quadratic field is Galois over $\mathbb{Q}$, same results and theorems on when a prime is represented by the form corresponding to the totally positive principal ideal class hold. From this we have the following generalisation of Theorem 5.17 to all quadratic fields:

Theorem 6.8. *Let $q(x, y)$ be the quadratic form corresponding to the totally positive principal ideal class in K. Then there is a polynomial $f(x)$ of degree $h^+(K) = h^+(\Delta_K)$ such that for p an odd prime not dividing Δ_K or the discriminant of $f(x)$, we have:*

$$p \text{ is represented by } q(x, y) \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

This polynomial can be taken to be the minimal polynomial of the algebraic integer α for which $L = K(\alpha)$ is the narrow class field of K.

Again we left with the problem of actually computing the narrow class field of a quadratic field. When the narrow class field is larger than the Hilbert class field we will have to rely on Magma for the computations. Using the tables from Cohen we may be able to spot an abelian extension of K which is unramified at the finite primes but ramifies at the infinite primes, something like $K(\mathrm{i})$. The composite of this with the Hilbert class field will be the narrow class field, we will still have to rely on Magma to find the polynomial generating this extension.

We are now in a position to find criterion for primes to be represented by the form corresponding to the totally positive principal ideal class in the remaining real quadratic fields.

Primes of the Form $x^2 - 142y^2$

The form $x^2 - 142y^2$ corresponds to the totally positive principal ideal class in the real quadratic field $K = \mathbb{Q}(\sqrt{142})$. This field has class number $h(K) = 3$, and narrow class number $h^+(K) = 6$. Cohen tell us that the Hilbert class field of K is given by $K(\omega)$, where ω is a root of the polynomial $z(x) = x^3 - x^2 - 6x - 2$. From earlier results we know that $K(\sqrt{-2}) = K(\sqrt{-71})$ is an abelian extension of K unramified outside of the finite primes. Therefore $L = K(\omega, \sqrt{-2})$, the composite of this and the Hilbert class field, is an abelian extension of K unramified outside of the finite primes. It has degree $[L : K] = 6$, and therefore is the narrow class field of K.

Magma tells us that this field is also given by $L = K(\alpha)$, where α is a root of the polynomial $f(x) = x^6 - 2x^5 - 5x^4 + 56x^2 + 64x + 128$ of discriminant $-2^{31}5^471^2$.

Theorem 6.8 then says that for $p \neq 2, 5, 71$:

$$p = x^2 - 142y^2 \Leftrightarrow \begin{cases} \left(\frac{142}{p}\right) = 1 \text{ and} \\ x^6 - 2x^5 - 5x^4 + 56x^2 + 64x + 128 \text{ has a root modulo } p \end{cases}$$

Primes of the Form $x^2 + xy - 80y^2$ and $x^2 - 321y^2$

The form $X^2 + xy - 80y^2$ corresponds to the totally positive principal ideal class in $K = \mathbb{Q}(\sqrt{321})$. This field has class number $h(K) = 3$, and narrow class number $h^+(K) = 6$. Cohen tells us that the Hilbert class field of K is given by $K(\omega)$, where ω is a root of the polynomial $z(x) = x^3 - x^2 - 4x + 1$. Since $-3 \equiv 1 \pmod 4$, the field $K(\sqrt{-3})$ is an abelian extension of K unramified outside of the infinite primes. The composite, $L = K(\omega, \sqrt{-3})$, of this and the Hilbert class field is therefore an abelian extension unramified outside of the infinite primes of degree $[L : K] = 6$. Therefore L is the narrow class field of K.

Magma tells us that this field is also given by $L = K(\alpha)$, where α is a root of the polynomial $f(x) = x^6 - 2x^5 + 2x^4 - 2x^3 + 47x^2 - 20x + 163$ of discriminant $-2^6 3^9 11^2 79^2 107^2$.

So, as always, we have for $p \neq 2, 3, 11, 79, 107$:

$$p = x^2 + xy - 80y^2 \Leftrightarrow \begin{cases} \left(\frac{321}{p}\right) = 1 \text{ and} \\ x^6 - 2x^5 + 2x^4 - 2x^3 + 47x^2 - 20x + 163 \text{ has a root modulo } p \end{cases}$$

Using the identity:

$$x^2 + xy - 80y^2 = (x + \tfrac{y}{2})^2 - 321y^2$$

and looking modulo 2, we see that any prime of the form $x^2 + xy - 80y^2$ is of the form $x^2 - 321y^2$, and vice versa.

Hence we also have for $p \neq 2, 3, 11, 79, 107$:

$$p = x^2 - 321y^2 \Leftrightarrow \begin{cases} \left(\frac{321}{p}\right) = 1 \text{ and} \\ x^6 - 2x^5 + 2x^4 - 2x^3 + 47x^2 - 20x + 163 \text{ has a root modulo } p \end{cases}$$

6.2 Subgroups of the Class Group

For each subgroup H of the class group, or the narrow class group there is an associated class field which can detect when a prime ideal lies in H.

Let H be a subgroup of the ideal class group $\mathcal{C}(K)$. Then the pre-image of H under the quotient map $j \colon \mathcal{I}(K) \to \mathcal{I}(K)/\mathcal{P}(K)$ defines a subgroup $j^{-1}(H)$ of $\mathcal{I}(K)$ containing $\mathcal{P}(K)$. So $j^{-1}(H)$ is a congruence subgroup for the modulus $\mathfrak{m} = 1$.

By the Existence Theorem there is a unique abelian extension M of K arising from the modulus $\mathfrak{m} = 1$, and the congruence subgroup $j^{-1}(H)$. The Artin map $\Phi\colon \mathcal{I}(K) \to \mathrm{Gal}(M/K)$ has kernel $j^{-1}(H)$. Therefore:

$$\mathrm{Gal}(M/K) \cong \mathcal{I}(K)/j^{-1}(H)$$

The homomorphism induces from the composition:

$$\mathcal{I}(K) \xrightarrow{\mathrm{j}} \mathcal{C}(K) \longrightarrow \mathcal{C}(K)/H$$

has kernel $j^{-1}(H)$, therefore we have an isomorphism:

$$\mathcal{I}(K)/j^{-1}(H) \cong \mathcal{C}(K)/H$$

Combined with the isomorphism arising from the Artin map we have:

$$\mathrm{Gal}(M/K) \cong \mathcal{C}(K)/H$$

By the corollary to uniqueness in the existence theorem since $\mathcal{P}(K) \subset j^{-1}(H)$, the class field M is a subfield of the Hilbert class field L. Since L/K is Galois M must be a fixed field of L for some subgroup of the Galois group $\mathrm{Gal}(L/K) \cong \mathcal{C}(K)$. The result above shows $M = L^H$. We have precisely the same result with subgroups of the narrow class group too.

By construction the kernel of the Artin map $\Phi_{M/K,\mathfrak{m}}$ is the congruence subgroup $j^{-1}(H)$, that is the ideals in any ideal class of H. Therefore the prime ideals which split completely in M/K are the prime ideals which lie in some class in H.

Since $\mathrm{Gal}(L/K)$ is abelian, every subgroup is normal, and so every intermediate field of L/K is Galois over K. If K is a quadratic field, our previous results show that the class field M, corresponding to the subgroup H of either class group, is a Galois extension of $\mathbb{Q}$. As before M is the composite of K and some field $F = \mathbb{Q}(\alpha)$, and we can formula complete splitting in M as splitting in K and in F.

From this we have a further generalisation of Theorem 5.17:

Theorem 6.9. *Let the subset of forms $\{q_i(x,y)\}$ correspond to the subgroup H of the narrow class group of the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Then there is a polynomial $f(x)$ of degree $h^+(K)/|H| = h^+(\Delta_K)/|H|$ such that for p an odd prime not dividing Δ_K or the discriminant of $f(x)$, we have:*

$$p \text{ is represented by some } q_i(x,y) \Leftrightarrow \begin{cases} \left(\frac{d}{p}\right) = 1 \text{ and} \\ f(x) \text{ has a root modulo } p \end{cases}$$

This polynomial can be taken to be the minimal polynomial of the algebraic integer α for which $M = K(\alpha)$ is the fixed field L^H of the narrow class field, that is the class field corresponding to the subgroup H.

Primes of the Form $x^2 + 26y^2$ and Other Forms of Discriminant $D = -104$

The form $x^2 + 26y^2$ corresponds to the principal ideal class in $K = \mathbb{Q}(\sqrt{26})$. The field K class number $h(K) = 6$, so its class group is isomorphic to $\mathbb{Z}_6$, generated by r. The correspondence between forms and ideals tell us we have the following identifications:

Class Group	Quadratic Form
e	$x^2 + 26y^2$

Class Group	Quadratic Form
r	$5x^2+4xy+6y^2$
r^2	$3x^2-2xy+9y^2$
r^3	$2x^2+13y^2$
r^4	$3x^2+2xy+9y^2$
r^5	$5x^2-4xy+6y^2$

Through a sequence of steps we will find a criterion to determine which primes each of these forms represents.

Cohen says the Hilbert class field of K is $K(\alpha)$, where α is a root of the polynomial $f(x) = x^6-x^5+2x^4+x^3-2x^2-x-1$ of discriminant $2^{10}13^2$. By our previous result we get the result for $p \neq 2, 13$ that:

$$p = x^2+26y^2 \Leftrightarrow \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ and,} \\ x^6-x^5+2x^4+x^3-2x^2-x-1 \text{ has a root modulo } p \end{cases}$$

The forms x^2+26y^2 and $2x^2+13y^2$ correspond to the subgroup $H_1 = \{e, r^3\}$ of the class group. The associated class field is the fixed field L^{H_1} of the Hilbert class field, this field is $K(\beta)$, where β is a root of the polynomial $g(x) = x^3+x^2+5x+1$ of discriminant $-2^5 13$. Splitting completely in L^{H_1} tells us when (p) splits into ideals in the subgroup H_1, and so p is represented by x^2+26y^2 or $2x^2+13y^2$. Now Theorem 6.9 says for $p \neq 2, 13$ that:

$$\left.\begin{array}{l} p = x^2+26y^2 \text{ or} \\ p = 2x^2+13y^2 \end{array}\right\} \Leftrightarrow \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ and,} \\ x^3+x^2+5x+1 \text{ has a root modulo } p \end{cases}$$

As we observed earlier, except for opposite forms, different forms represent disjoint sets of primes since ideals factor uniquely in a number field. We know when p is of the form x^2+26y^2, and when it is represented by x^2+26y^2 or $2x^2+13y^2$. By discounting primes represented by x^2+26y^2 we can find when a prime is represented by $2x^2+13y^2$ exactly; this simply means $f(x) = x^6-x^5+2x^4+x^3-2x^2-x-1$ doesn't have a root modulo p. For $p \neq 2, 13$

$$p = 2x^2+13y^2 \Leftrightarrow \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ and,} \\ x^3+x^2+5x+1 \text{ has a root modulo } p \text{ and,} \\ x^6-x^5+2x^4+x^3-2x^2-x-1 \text{ has no roots modulo } p \end{cases}$$

Similarly the forms x^2+26y^2, $3x^2+2xy+9y^2$ and $3x^2-2xy+9y^2$ correspond to the subgroup $H_2 = \{e, r^2, r^4\}$ of the class group. The corresponding class field is L^{H_2}, which is $K(\gamma)$, where γ is a root of $h(x) = x^2-13$ of discriminant $2^2 13$. Splitting completely in L^{H_2} tells us when a prime p is represented by x^2+26y^2 or $3x^2 \pm 2xy+9y^2$. For $p \neq 2, 13$:

$$\left.\begin{array}{l} p = x^2+26y^2 \text{ or} \\ p = 3x^2 \pm 2xy+9y^2 \end{array}\right\} \Leftrightarrow \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ and,} \\ x^2-13 \text{ has a root modulo } p \end{cases}$$

Since the forms $3x^2 \pm 2xy+9y^2$ are opposite they represent the same primes, excluding the primes represented by x^2+26y^2, we find a criterion for primes to be represented by these forms. For $p \neq 2, 13$:

$$p = 3x^2 \pm 2xy+9y^2 \Leftrightarrow \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ and,} \\ x^2-13 \text{ has a root modulo } p \text{ and,} \\ x^6-x^5+2x^4+x^3-2x^2-x-1 \text{ has no roots modulo } p \end{cases}$$

Lastly we are left with the forms $5x^2+4xy+6y^2$ and $5x^2-4xy+6y^2$. We have determined when a prime is represented by any of the other forms, and these two are opposite forms. The Legendre symbol $\left(\frac{-26}{p}\right)$ tell us when a prime is represented by one of the above quadratic forms, this is equivalent to splitting in K, and K is the class field corresponding to the entire class group. Excluding primes represented by the other forms gives us a criterion. For $p \neq 2, 13$:

$$p = 3x^2 \pm 2xy + 9y^2 \Leftrightarrow \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ and,} \\ x^3 + x^2 + 5x + 1 \text{ has no roots modulo } p \text{ and,} \\ x^2 - 13 \text{ has no roots modulo } p \end{cases}$$

Even if we can't distinguish every quadratic form of a given discriminant, we can use the same ideal to find which primes an arbitrary subgroup of quadratic forms represents.

Primes of the Form x^2+74y^2 an Other Forms of Discriminant $D=-296$

The quadratic form x^2+74y^2 corresponds to the principal ideal class in $K=\mathbb{Q}(\sqrt{-74})$. This field has class number $h(K)=10$ and its class group is isomorphic to $\mathbb{Z}_{10}$, generated by r. We have the following correspondence between forms and ideals:

Class Group	Quadratic Form
e	x^2+74y^2
r	$5x^2+2xy+15y^2$
r^2	$3x^2-2xy+25y^2$
r^3	$6x^2-4xy+13y^2$
r^4	$9x^2-8xy+10y^2$
r^5	$2x^2+37y^2$
r^6	$9x^2+8xy+10y^2$
r^7	$6x^2+4xy+13y^2$
r^8	$3x^2+2xy+25y^2$
r^9	$5x^2-2xy+15y^2$

Cohen tells us the Hilbert class field of K is given by $K(\alpha)$ where α is a root of the polynomial $f(x)=x^{10}-2x^9-3x^8+4x^7+5x^6-2x^5+5x^4+4x^3-3x^2-2x+1$ of discriminant $-2^{29}37^4$. We therefore get the condition for $p \neq 2, 37$:

$$p = x^2+74y^2 \Leftrightarrow \begin{cases} \left(\frac{-74}{p}\right) = 1 \text{ and,} \\ x^{10}-2x^9-3x^8+4x^7+5x^6-2x^5 \\ \quad +5x^4+4x^3-3x^2-2x+1 \text{ has a root modulo } p \end{cases}$$

The quadratic forms x^2+74y^2, $3x^2 \pm 2xy + 25y^2$ and $9x^2 \pm 8xy + 10y^2$ correspond to the subgroup $H_1\{e, r^2, r^4, r^6, r^8\}$ of the class group. The corresponding class field is $L^{H_1} = K(\beta)$ where β is a root of the polynomial $g(x)=x^2+2$ of discriminant -2^3. Therefore for $p \neq 2, 37$

$$\left.\begin{array}{l} p = x^2+74y^2 \text{ or} \\ p = 3x^2 \pm 2xy + 25y^2 \text{ or} \\ p = 9x^2 \pm 8xy + 10y^2 \end{array}\right\} \Leftrightarrow \begin{cases} \left(\frac{-74}{p}\right) = 1 \text{ and} \\ x^2+2 \text{ has a root modulo } p \end{cases}$$

Excluding primes represented by the form x^2+74y^2 we obtain the condition for $p \neq 2, 37$:

$$\left.\begin{array}{l} p = 3x^2 \pm 2xy + 25y^2 \text{ or} \\ p = 9x^2 \pm 8xy + 10y^2 \end{array}\right\} \Leftrightarrow \begin{cases} \left(\frac{-74}{p}\right) = 1 \text{ and} \\ x^2+2 \text{ has a root modulo } p \text{ and} \\ x^{10} - 2x^9 - 3x^8 + 4x^7 + 5x^6 - 2x^5 \\ \quad + 5x^4 + 4x^3 - 3x^2 - 2x + 1 \text{ has no roots modulo } p \end{cases}$$

Unfortunately using class field theory we cannot distinguish these forms any further.

Similarly the forms x^2+74y^2 and $2x^2+37y^2$ correspond to the subgroup $H_2 = \{e, r^5\}$, and the class field for this subgroup is $L^{H_2} = K(\gamma)$, where γ is a root of the polynomial $h(x) = x^5 - 8x^4 + 16x^3 + 4x^2 - 13x - 8$ of discriminant $2^{12}37^2$. So we get for $p \neq 2, 37$:

$$\left.\begin{array}{l} p = x^2 + 74y^2 \text{ or} \\ p = 2x^2 + 37y^2 \end{array}\right\} \Leftrightarrow \begin{cases} \left(\frac{-74}{p}\right) = 1 \text{ and} \\ x^5 - 8x^4 + 16x^3 + 4x^2 - 13x - 8 \text{ has a root modulo } p \end{cases}$$

Excluding those primes represented by the principal form we obtain for $p \neq 2, 37$:

$$p = 2x^2 + 37y^2 \Leftrightarrow \begin{cases} \left(\frac{-74}{p}\right) = 1 \text{ and} \\ x^5 - 8x^4 + 16x^3 + 4x^2 - 13x - 8 \text{ has a root modulo } p \text{ and} \\ x^{10} - 2x^9 - 3x^8 + 4x^7 + 5x^6 - 2x^5 \\ \quad + 5x^4 + 4x^3 - 3x^2 - 2x + 1 \text{ has no roots modulo } p \end{cases}$$

We can play precisely the same game with indefinite forms and subfields of the narrow class field.

Primes of the Form $x^2 - 79y^2$ and Other Forms of Discriminant $D = 316$

The form $x^2 - 79y^2$ corresponds to the totally positive principal ideal class in $K = \mathbb{Q}(\sqrt{79})$. This field has narrow class number $h^+(K) = 6$, and the narrow class group is isomorphic to $\mathbb{Z}_6$ generated by r. By the correspondence between forms and ideals we have the following identification:

Class Group	Quadratic Form
e	$x^2 - 79y^2$
r	$3x^2 + 14xy - 10y^2$
r^2	$-3x^2 + 16xy + 5y^2$
r^3	$-x^2 + 79y^2$
r^4	$-3x^2 - 16xy + 5y^2$
r^5	$3x^2 - 14xy - 10y^2$

Cohen tell us that the Hilbert class field of $K = \mathbb{Q}(\sqrt{79})$ is $K(\omega)$, where ω is a root of the polynomial $z(x) = x^3 - x^2 - 4x + 2$. We then observe that $K(\mathrm{i}) = \mathbb{Q}(\sqrt{-79})$ is an abelian extension unramified at all the finite primes. The composite $L = K(\omega, \mathrm{i})$ is then an abelian extension unramified at all primes with degree $[L : K] = 6$. Since K has narrow class number $h^+(K) = 6$ we conclude that L is the narrow class field of K.

Complete splitting of (p) in the narrow class field tell us when p is represented by $x^2 - 79y^2$. Magma tells us that the composite field above which is the narrow class field of $K = \mathbb{Q}(\sqrt{79})$ is $K(\alpha)$, where α is a root of the polynomial $f(x) = x^6 - 2x^5 - 4x^4 + 8x^3 + 17x^2 - 22x + 34$ of

discriminant $-2^{22}23^279^2$. So for $p \neq 2, 23, 79$:

$$p = x^2 - 79y^2 \Leftrightarrow \begin{cases} \left(\frac{79}{p}\right) = 1 \text{ and,} \\ x^6 - 2x^5 - 4x^4 + 8x^3 + 17x^2 - 22x + 34 \text{ has a root modulo } p \end{cases}$$

The forms $x^2 - 79y^2$ and $-x^2 + 79y^2$ correspond to the subgroup $H_1 = \{1, r^3\}$ of the narrow class group. The corresponding class group is the fixed field $L^{H_1} = K(\beta)$, where β is a root of $g(x) = x^3 - 12x^2 + 41x - 34$ of discriminant 2^479. Complete splitting of (p) in L^{H_1} means that p is represented by $x^2 - 79y^2$ or $-x^2 + 79y^2$. Excluding the primes represented by $x^2 - 79y^2$ gives for $p \neq 2, 23, 79$:

$$p = -x^2 + 79y^2 \Leftrightarrow \begin{cases} \left(\frac{79}{p}\right) = 1 \text{ and,} \\ x^3 - 12x^2 + 41x - 34 \text{ has a root modulo } p \text{ and,} \\ x^6 - 2x^5 - 4x^4 + 8x^3 + 17x^2 - 22x + 34 \text{ has no roots modulo } p \end{cases}$$

The forms x^2-79y^2, $-3x^2+16xy+5y^2$ and $-3x^2-16xy+5y^2$ correspond to the subgroup $H_2 = \{e, r^2, r^4\}$ of the narrow class group. The corresponding class field is the fixed field $L^{H_2} = K(\gamma)$, where γ is a root of $h(x) = x^2 + 1$. Complete splitting of (p) in L^{H_2} means that p is represented by one of these forms. Excluding those primes represented by $x^2 - 79y^2$ gives the criterion for $p \neq 2, 23, 79$:

$$-3x^2 \pm 16xy + 5y^2 \Leftrightarrow \begin{cases} \left(\frac{79}{p}\right) = 1 \text{ and,} \\ x^2 + 1 \text{ has a root modulo } p \text{ and,} \\ x^6 - 2x^5 - 4x^4 + 8x^3 + 17x^2 - 22x + 34 \text{ has no roots modulo } p \end{cases}$$

Lastly we are left with the forms $3x^2+14xy-10y^2$ and $3x^2-14xy-10y^2$. We have determined when a prime is represented by any of the other forms. The Legendre symbol tells us when a prime is represented by some form, excluding all other forms give the criterion for $p \neq 2, 23, 79$:

$$3x^2 \pm 14xy - 10y^2 = \begin{cases} \left(\frac{79}{p}\right) = 1 \text{ and,} \\ x^2 + 1 \text{ has no roots modulo } p \text{ and,} \\ x^3 - 12x^2 + 41x - 34 \text{ has no roots modulo } p \end{cases}$$

6.3 The Genus Field

The class field L corresponding to the subgroup $\mathcal{C}^+(K)^2$ of squares in the narrow class group $\mathcal{C}^+(K)$ of a quadratic field K detects whether the class of a prime ideal $\mathfrak{p}$ lies in this subgroup. In terms of quadratic forms, complete splitting in L happens if and only if a prime p can be represented by some quadratic form corresponding to the subgroup of squares.

We know from genus theory that the genus containing the principal form is exactly the subgroup of squares, and so complete splitting in this class field detects that p is represented by some form in the principal genus. This link to genera of quadratic forms motivates calling L the genus field of the quadratic field K, and gives a class field theoretic interpretation of genus theory for fundamental discriminants.

A more general definition of the genus field of a number field is given in Ishida [13, p. 1] for which the previous becomes a special case:

Definition 6.10. Let K be an algebraic number field. The genus field L if K is the maximal abelian extension of K which is the composite of an absolute abelian and K, and is unramified at all the finite primes.

As stated in Ishida [13, p. 3–5] the genus field of a quadratic number field can be explicitly described as follows.

Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic number field, where m is a square-free integer. For a prime divisor p of m, define:

$$p^* = \begin{cases} (-1)^{(p-1)/2} & \text{if } p \text{ is odd} \\ -4 & \text{if } p = 2 \text{ and } m \equiv 3 \pmod 4 \\ 8 & \text{if } p = 2 \text{ and } m \equiv 2 \pmod 8 \\ -8 & \text{if } p = 2 \text{ and } m \equiv 6 \pmod 8 \end{cases}$$

which is the discriminant of the quadratic field $\mathbb{Q}(\sqrt{p^*})$.

If $p_1, p_2, \ldots, p_t$ are the prime divisors of Δ_K, then $\Delta_K = \prod p_i^*$, and the genus field of K is given by:

$$L = \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \ldots, \sqrt{p_t^*})$$

Complete splitting of q in this field means that q is represented by some quadratic form in the principal genus. This is equivalent to splitting in each of the quadratic fields $\mathbb{Q}(\sqrt{p_i^*})$, which can be explicitly described in terms of the Legendre symbols $\left(\frac{p_i^*}{q}\right) = 1$. Using quadratic reciprocity we can transform this into a congruence condition.

This turns out to be very closely related to Gauss's definition of genera in terms of assigned characters, and here reduces to the condition that a form is in same genus as the principal form. For this see Lemma 3.20 and Section 6 of Cox [7, p. 57, pp. 121-127]. Thus we can formulate genus theory in terms of class field theory.

Bibliography

[1] Emil Artin and John Tate. *Class Field Theory*. Advanced Book Classics Series. Addison-Wesely, 1990.

[2] Matthew H. Baker. *An Introduction to Class Field Theory*. URL: `http://www.math.umass.edu/~dhayes/CFT.ps`.

[3] J. W. S. Cassels. *Rational Quadratic Forms*. Vol. 13. LMS Monographs. Academic Press, 1987.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Vol. 138. Graduate Texts in Mathematics. Springer, 1996.

[5] Henri Cohen. *Advnced Topics in Computational Number Theory*. Vol. 193. Graduate Texts in Mathematics. Springer, 2000.

[6] Harvey Cohn. *Advanced Number Theory*. Dover, 1980.

[7] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*. John Wiley & Sons, 1989.

[8] Daniel E. Flath. *Introduction to Number Theory*. Wiley, 1989.

[9] G. Frei. "Leonhard Euler's Convenient Numbers". In: *Math. Intell.* 7 (3 1985), pp. 55–58, 64.

[10] A. Fröhlich and M. J. Taylor. *Algebraic Nmber Theory*. Vol. 27. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1991.

[11] Robert Guralnick, Murray M. Schacher, and Jack Sonn. "Irreducible Polynomials Which Are Locally Reducible Everywhere". In: *Proceedings of the American Mathematical Society* 133.11 (2005), pp. 3171–3177. URL: `http://www.jstor.org/stable/4097570`.

[12] Helmut Hasse. *Number Theory*. Vol. 229. Grundlehren der mathematischen Wissenschaften. Springer, 1980.

[13] Makato Ishida. *The Genus Fields of Algebraic Number Fields*. Vol. 555. Lecture Notes in Mathematics. Springer, 1976.

[14] Gerald J. Janusz. *Algebraic Number Fields*. Academic Press, 1973.

[15] Edmund Landau. "Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante". In: *Mathematische Annalen* 56 (4 1903), pp. 671–676.

[16] Serge Lang. *Algebraic Number Theory*. Addison-Wesley Series in Mathematics. Addison-Wesley, 1970.

[17] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein*. Springer Monographs in Mathematics. Springer, 2000.

[18] Daniel A. Marcus. *Number Fields*. Universitext. Springer, 1995.

[19] Keith Matthews. *Some BCMath/PHP number theory programs*. URL: `http://www.numbertheory.org/php/`.

[20] James S. Milne. *Algebraic Number Theory (v3.03)*. 2011. URL: `www.jmilne.org/math/`.

[21] James S. Milne. *Class Field Theory (v4.01)*. 2011. URL: `www.jmilne.org/math/`.

[22] James S. Milne. *Fields and Galois Theory (v4.30)*. 2012. URL: `www.jmilne.org/math/`.

[23] H. M. Stark. "A Complete Determination of the Complex Quadratic Fields of Class-Number One". In: *Michigan Math. J.* 14 (1 1967), pp. 1–27.

[24] Ian Stewart. *Galois Theory*. Chapman & Hall/CRC, 2004.

[25] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. AK Peters, 2002.

[26] Computational Algebra Group at the University of Sydney. *Magma Computational Algebra System*. URL: `http://magma.maths.usyd.edu.au/magma/`.

[27] Computational Algebra Group at the University of Sydney. *Magma Handbook*. URL: `http://magma.maths.usyd.edu.au/magma/handbook/`.

[28] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Vol. 83. Graduate Texts in Mathematics. Springer, 1997.

[29] Don Zagier. *Zetafunktionen und Quadratische Körper*. Springer, 1981.

Appendix A

Magma

Magma is a computer algebra system designed primarily for defining and performing computations on algebraic structures such as rings, fields and groups. It has many built in functions for performing the frequently occurring calculations the arise when working with algebraic structures.

I will give a brief overview of how these functions could be used to perform some of the calculations required in this report.

A number field is defined using the `NumberField` function. This function takes an irreducible polynomial as input, and returns the extension defined by adjoining a root of the polynomial to the coefficient field of the polynomial. To define a polynomial over $\mathbb{Q}$ use the `PolynomialRing` command with argument `Rationals()` and assign the generating element to the variable `x` as follows:

```
R<x> := PolynomialRing(Rationals());
```

Then the number $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^2 + 5$, is created as follows, where the generating elements α is assigned to the variable `s`:

```
K<s> := NumberField([x^2 + 5]);
```

Given a number field K, its Hilbert class field can be computed using the `HilbertClassField` command. The Hilbert class field is returned as a relative extension of K. The command outputs a description of this extension by giving the polynomial which generates it over K. In order to make the output more understandable, first define the polynomial ring over K, and assign its generator to a variable `y`:

```
S<y> := PolynomialRing(K);
HilbertClassField(K);

> Number Field with defining polynomial y^2 + 1 over K
```

This shows the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$ is given by $K(\beta)$, where β is a root of the polynomial $y^2 + 1$. That is, the Hilbert class field of K is $K(\mathrm{i})$.

If we need to view an extension of a number field as an extension of $\mathbb{Q}$, use the `AbsoluteField` command. This returns a relative extension of number fields as an absolute extension of $\mathbb{Q}$, and outputs a description by giving the polynomial which generates it over $\mathbb{Q}$:

```
L := HilbertClassField(K);
AbsoluteField(L);

> Number Field with defining polynomial x^4 + 12*x^2 + 16 over the Rational Field
```

So the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$ is also given by $\mathbb{Q}(\gamma)$, where γ is a root of the polynomial $x^4 + 12x^2 + 16$.

To compute the composite of two absolute number fields use the `Compositum` command. It returns the composite as an absolute extension of $\mathbb{Q}$, and outputs a description by giving the polynomial which generates it over $\mathbb{Q}$:

```
E := NumberField([x^2 - 2]);
F := NumberField([x^2 - 3]);
Compositum(E, F);

> Number Field with defining polynomial x^4 - 10*x^2 + 1 over the Rational Field
```

Magma can compute more general class field using the `RayClassField` command. It takes an ideal $\mathfrak{m}_0$ of a number field, and a list of real infinite primes as input, and returns the abelian extension arising from the modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ and the congruence subgroup $\mathcal{P}_{K,1}(\mathfrak{m})$. To compute the narrow class field of the quadratic $K = \mathbb{Q}(\sqrt{3})$ we could proceed as follows:

```
K<s> := NumberField([x^2 - 3]);
S<y> := PolynomialRing(K);
NumberField(RayClassField(1*MaximalOrder(K), [1, 2]));

> Number Field with defining polynomial y^2 + 1 over K
```

So the narrow class field of $K = \mathbb{Q}(\sqrt{3})$ is $K(\mathrm{i}) = \mathbb{Q}(\sqrt{3}, \mathrm{i})$.

The `SubfieldLattice` command is used to generate a list of all subfields of a given number field K. Using this we can find the intermediate fields of the extension L/K, and identify the class fields corresponding to subgroups of the class group. To list the subfields of $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\delta)$, where δ is a root of the polynomial $x^4 - 10x^2 + 1$, we would use:

```
K<s> := NumberField([x^4 - 10*x^2 + 1]);
SubfieldLattice(K);

> Subfield Lattice of K
> [1] Rational Field
> [2] Subfield generated by a root of x^2 - 8
> [3] Subfield generated by a root of x^2 + 10*x + 1
> [4] Subfield generated by a root of x^2 - 4*x - 8
> [5] Subfield generated by a root of x^4 - 10*x^2 + 1
```

A more detailed explanation of these commands and the other commands available in Magma, along with examples of their usage it available in the Magma Handbook [27].

Appendix B

List of Criteria