Representation of prime numbers by quadratic forms

Bachelor thesis in Mathematics

by

Simon Hasenfratz

Supervisor: Prof. R. Pink

ETH Zurich

Summer term 2008

Introduction

One of the most famous theorems in elementary number theory is the following, first conjectured by Fermat and then proved by Euler:

An odd prime p can be written as $p = x^2 + y^2$ where $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$.

Euler proved this theorem using infinite descent, and he also considered the similiar problems $p = x^2 + 2y^2$, $p = x^2 + 3y^2$ and so on. For each of these cases he had to work out completely new proofs and it took him years until he realized that in fact quadratic residues were at the heart of the matter. These problems led Euler finally to the discovery of quadratic reciprocity.

Unfortunately, the methods Euler used to tackle these problems hardly generalize. What one needs is a more powerful language to formulate the problem: Consider the number field $K = \mathbb{Q}(\sqrt{-n})$ with ring of integers $\mathcal{O}_K$. Furthermore, let $\mathcal{O}$ be the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ and denote the conductor of the order by $f := [\mathcal{O}_K : \mathcal{O}]$. Then it can be shown that for odd primes p not dividing f the following are equivalent:

(i) $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

(ii) $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ are prime ideals of $\mathcal{O}_K$ and $\mathfrak{p} = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}$.

Now consider the case $n = 1$. Then the equivalence above becomes

$$p = x^2 + y^2 \Leftrightarrow p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}}.$$

But this just says that p splits completely in K, which in turn is equivalent to the Legendre symbol $(\frac{1}{p})$ being equal to 1. Using the law of quadratic reciprocity, we deduce that $p = x^2 + y^2 \Leftrightarrow (\frac{1}{p}) = 1 \Leftrightarrow \frac{p-1}{2} = 2k \Leftrightarrow p = 4k + 1$.

Unfortunately, if $n > 0$ is arbitrary, various problems may arise. For instance, the quadratic number field $\mathbb{Q}[\sqrt{-n}]$ may have class number greater than 1 and $\mathcal{O}$ needs not to be the equal to the ring of integers in general. To resolve these difficulties, we will introduce ring class fields. The ring class field of an order $\mathcal{O}$ is defined to be the unique abelian extension L/K satisfying:

(i) All ramified primes of L/K divide $f\mathcal{O}_K$.

(ii) $\mathrm{Gal}(L/K) \cong C(\mathcal{O})$, where $C(\mathcal{O})$ is the ideal class group of $\mathcal{O}$.

The main point then will be to show that for odd primes not dividing n we have

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow p \text{ splits completely in } L.$$

This gives already a complete, but rather abstract answer to the problem. However, if we denote the minimal polynomial of a real primitve element of L over K by f_n, one can show that for any odd prime p neither dividing n nor the discriminant of f_n, the follwing are equivalent:

(i) $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

(ii) The Legendre symbol $(\frac{-n}{p})$ is equal to one and the equation $f_n(x) \equiv 0 \mod p$ has a solution in $\mathbb{Z}$.

This in fact is the main theorem of the whole thesis, and we will apply it by exploring which primes can be written as $x^2 + 14y^2$. Furthermore, we will show how the developped tools can be used to make more general statements about representation of prime numbers by quadratic forms.

In chapter 1 we will give a short introduction to the basic theory of quadratic forms. Chapter 2 will cover orders in imaginary quadratic number fields and we will show how they relate to quadratic forms. A brief introduction to class field theory will be given in chapter 3. Having developped these necessary tools, we will apply them in chapter 4 to give an abstract but complete solution to the general problem of which primes can be written as $x^2 + ny^2$. Finally, chapter 5 is dedicated to the proof that a primitive positive definite form always represents infinitely many primes.

I would like to thank Prof. Richard Pink and Patrik Hubschmid for their assistance.

Zurich, November 15, 2008
Simon Hasenfratz

Contents

Chapter 1

Quadratic forms

1.1 Proper equivalence

In this section we shall give a brief introduction to the theory of (integral) quadratic forms, ie. functions of the form

$$f(x,y) = ax^2 + bxy + cy^2, \quad \text{where } a,b,c \in \mathbb{Z}.$$

We choose a very classical approach here; all results we need are known since the 19th century. Nevertheless we will be able to relate them to class field theory, which will allow us to prove in chapter 5 that a primitive positive definite quadratic form always represents infinitely many primes. First we need some definitions:

Definition 1.1.1 (Primitive form) *A quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is primitive if its coefficients a,b,c are relatively prime.*

Note that every quadratic form is an integer multiple of a primitive quadratic form. Following Gauss, we now introduce an equivalence relation on the set of quadratic forms:

Definition 1.1.2 (Proper equivalence) *Two quadratic forms $f(x,y)$ and $g(x,y)$ are said to be properly equivalent if there exist integers p,q,r,s such that*

$$f(x,y) = g(px+qy, rx+sy) \text{ and } ps - qr = 1. \tag{1.1}$$

One can check that this really defines an equivalence relation. Note furthermore that condition (1.1) can be rewritten as

$$f\begin{pmatrix} x \\ y \end{pmatrix} = g\left(M\begin{pmatrix} x \\ y \end{pmatrix}\right) \quad \text{and } M \in SL_2(\mathbb{Z}).$$

Now consider the identity

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

where $D = b^2 - 4ac$ is the **discriminant**. Since we will be interested in quadratic forms which only take positive integers values, it is natural to make the following definition:

Definition 1.1.3 (Positive definite form) *A quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is called positive definite if one of the following equivalent conditions holds:*

(i) $f(x,y)$ *takes only positive values for* $(x,y) \neq (0,0)$.

(ii) Its discriminant $D = b^2 - 4ac$ is negative and the leading term a is positive.

Before we can formulate our first theorem, we need one last definition:

Definition 1.1.4 (Reduced form) *A primitive positive definite form $ax^2+bxy+cy^2$ is called reduced if its coefficients satisfy:*

(i) $|b| \leq a \leq c$

(ii) $(|b| = a \text{ or } a = c) \Rightarrow b \geq 0.$

Note also that a and c are always positive, since the form is positive definite. Now we can state our first result:

Theorem 1.1.5 *Every primitive positive definite form is properly equivalent to a unique reduced form.*

Proof: Theorem 2.8 in [1]. □

A straightforward calculation shows that properly equivalent forms have the same discriminant. Therefore Theorem 1.1.5 tells us that the number of equivalence classes of primitive positive definite forms of a given discriminant $D < 0$ is equal to the number of reduced forms of discriminant D. We shall refer to this number as $h(D)$.

Our aim is now to endow the set $C(D)$ of classes of primitive positive definite forms of discriminant $D < 0$ with the structure of a finite abelian group. While we postpone the construction of the group structure to the next section, we will now prove the finiteness of $h(D)$:

Lemma 1.1.6 *Let $D < 0$ and $h(D)$ be the number of reduced forms of discriminant $D < 0$. Then $h(D)$ is finite.*

Proof: Suppose $ax^2 + bxy + cy^2$ is a reduced form of discriminant $D < 0$. Then it follows by definition that

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

and thus

$$a \leq \sqrt{-D/3}.$$

Hence there are only finitely many choices for a. Since $|b| \leq a$ and $c = \frac{b^2-D}{4a}$, the same is true for b and c. □

1.2 Form class group

To define the **Dirichlet composition** of two quadratic forms, which will induce the group structure on $C(D)$ later on, we first need a technical lemma:

Lemma 1.2.1 *Suppose $f(x,y) = a_1x^2 + b_1xy + c_1y^2$ and $g(x,y) = a_2x^2 + b_2xy + c_2y^2$ are forms of discriminant D that satisfy $\gcd(a_1, a_2) = 1$. Then there is a unique integer B modulo $2a_1a_2$ such that*

(i) $B \equiv b_1 \bmod 2a_1$

(ii) $B \equiv b_2 \bmod 2a_2$

(iii) $B^2 \equiv D \bmod 4a_1a_2$.

Proof: Lemma 3.2 in [1]. □

Now we can make the following definition:

Definition 1.2.2 (Dirichlet composition) *Let $f(x,y) = a_1x^2 + b_1xy + c_1y^2$ and $g(x,y) = a_2x^2 + b_2xy + c_2y^2$ be two primite positive definite forms of discriminant $D < 0$ satisfying $\gcd(a_1, a_2) = 1$. Then the Dirichlet composition of $f(x,y)$ and $g(x,y)$ is defined to be the form*

$$F(x,y) = a_1a_2x^2 + 2Bxy + \frac{B^2 - D}{4a_1a_2}y^2, \tag{1.2}$$

where B is the integer determined by Lemma 1.2.1.

One now can show that F is again primitive and positive definite of discriminant D (see [1], p.49). As the following theorem shows, $C(D)$ becomes a group via $[f(x,y)]\cdot[g(x,y)] := [F(x,y)]$, called the **form class group**.

Theorem 1.2.3 *Let $D < 0$ and let $C(D)$ be the set of classes of primitive positive definite forms of discriminant D. Then Dirichlet composition induces a group structure on $C(D)$,* *which makes $C(D)$ into a finite abelian group of order $h(D)$. In particular, the identity element of $C(D)$ is the class containing*

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

whereas the inverse of the class containing $ax^2 + bxy + cy^2$ is given by the opposite class, i.e. the class containing $ax^2 - bxy + cy^2$.

Sketch of proof: We only give the main ideas here; a more complete proof can be found in [1], p.51. So let $f(x, y) = a_1x^2 + b_1xy + c_1y^2$ and $g(x, y)$ be forms of the given type. Then one can show that $g(x, y)$ is properly equivalent to a form $h(x, y) = a_2x^2 + b_2xy + c_2y^2$ satisfying $\gcd(a_1, a_2) = 1$, and therefore Dirichlet composition is defined for any pair of classes in $C(D)$. Now one must check that this operation is indeed well-defined on the level of classes, and that we get a group structure out of this. This can be done directly by using the definition of Dirichlet composition, but the argument gets much easier if we use ideal class groups as shown in Theorem 2.2.3. Finally, to show that the identity and the inverse are of the given form, one has to note that $B = b_1$ fulfills the conditions of Lemma 1.2.1 and use the formula (1.2). □

Chapter 2

Orders in quadratic number fields

2.1 Definitions and motivation

Definition 2.1.1 (Order) *An order $\mathcal{O}$ in a number field K is a subset $\mathcal{O} \subset K$ such that*

(i) *$\mathcal{O}$ is a subring of K.*

(ii) *$\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.*

(iii) *$\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.*

Equivalently, one can define an order to be a subring of K, which is finitely generated as an abelian group and has maximal rank $n = [K : \mathbb{Q}]$. For instance, the ring of integers $\mathcal{O}_K$ in number field K is an order. It is even a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.
Recall from the theory of integral ring extensions that any ring $R \supseteq \mathbb{Z}$ which is finitely generated as a $\mathbb{Z}$-module is integral over $\mathbb{Z}$ (see [5], p.118 and p.122). Therefore, for any order $\mathcal{O}$ we find that $\mathcal{O} \subset \mathcal{O}_K$, because $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. Hence $\mathcal{O}_K$ is the **maximal order** in K.

Having introduced the general notion of an order, one can carry over many things that we know already about the maximal order $\mathcal{O}_K$. As an example, we can generalize the well-known fact that in a quadratic number field of discriminant d_K, the ring of integers can be written as

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot w_K, \text{where } w_K = \frac{d_K + \sqrt{d_K}}{2}.$$

For this purpose, let $f := [\mathcal{O}_K : \mathcal{O}]$ be the index of $\mathcal{O}$ in $\mathcal{O}_K$. Since $\mathcal{O}$ and $\mathcal{O}_K$ are both free $\mathbb{Z}$-modules of rank 2, f is finite and called the **conductor** of the order $\mathcal{O}$. It is now easy to show that $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z} \cdot f w_K$, and hence we have a generalization of the case $f = 1$ (consult [1], p.133 for details).

Using this integral basis, we can calculate an important invariant of $\mathcal{O}$: As for the maximal order $\mathcal{O}_K \subset K$ in a quadratic number field K, the **discriminant** of any order $\mathcal{O} \subset K$ of conductor f is defined to be

$$D = \left(\det\begin{pmatrix} 1 & fw_K \\ 1 & f\overline{w_K} \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & \frac{f}{2}(d_K + \sqrt{d_K}) \\ 1 & \frac{f}{2}(d_K - \sqrt{d_K}) \end{pmatrix}\right)^2 = f^2 d_K.$$

Therefore, an order in a quadratic number field is uniquely determined by its discriminant. The most important case for us is the order $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{Q}[\sqrt{-n}]$, where $n \in \mathbb{N}$. Here we can choose $\{1, \sqrt{-n}\}$ as an integral basis, and therefore its discriminant can be computed to be $D = -4n$. Alltogether we get $-4n = f^2 d_K$, which shall be useful later on.

Now let $\mathcal{O}$ be an arbitrary order. As in the case where $\mathcal{O} = \mathcal{O}_K$, one can show that $\mathcal{O}$ is noetherian and that all ideals have finite index in $\mathcal{O}$, called the **Norm** of the ideal. Therefore prime ideals are maximal. Nevertheless, $\mathcal{O}$ is *not* a Dedekind domain in general, since $\mathcal{O}$ is obviously not integrally closed in K when $f > 1$.

Our aim for the next section is now to develop a new ideal theory for orders in quadratic fields. To do this, we will exploit a rather astonishing connection between orders in imaginary quadratic fields and quadratic forms.

2.2 Orders and quadratic forms

The main idea is to generalize the notion of the ideal class group of $\mathcal{O}_K \subset K$ to arbitrary orders $\mathcal{O} \subset K$ in quadratic number fields. As in the case when $\mathcal{O}$ is the maximal order, a fractional ideal of $\mathcal{O}$ is defined to be a non-zero subset of K which is a finitely generated $\mathcal{O}$-module. But to introduce the ideal class group $C(\mathcal{O})$, we first need to restrict ourselves a certain class of fractional $\mathcal{O}$-ideals:

Definition 2.2.1 (Proper fractional ideal) *A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is called proper if $\mathcal{O} = \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}$.*

Note that "$\subset$" always holds, but "$\supset$" does not have to hold if $\mathcal{O}$ is not the maximal order: For example, consider the order $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ in $K = \mathbb{Q}[\sqrt{-3}]$. Then the $\mathcal{O}$-ideal $\mathfrak{a}$ generated by 2 and $1 + \sqrt{-3}$ satisifies

$$\{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K,$$

but $\mathcal{O} \neq \mathcal{O}_K$.

Now we can state the following result:

Lemma 2.2.2 *Let $\mathcal{O} \subset K$ be an order in a quadratic field K, and $\mathfrak{a} \subset K$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible, i.e. if there is a fractional ideal $\mathfrak{b} \subset K$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.*

Proof: Prop. 7.4 in [1]. □

This lemma implies especially that the set of proper fractional $\mathcal{O}$-ideals is a group under multiplication, which will be called $I(\mathcal{O})$. If $P(\mathcal{O})$ denotes the subgroup of *principal* fractional ideals lying in $I(\mathcal{O})$, one can form the **ideal class group**

$$C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$$

of the order $\mathcal{O}$. Using geometric methods as in the case where $\mathcal{O}$ is the maximal order, one can prove that $C(\mathcal{O})$ is a *finite* abelian group. But we choose a different approach here, which only uses basic facts about quadratic forms, and leads to a broader characterization of $C(\mathcal{O})$. Recall from Chapter 1 that $C(D)$ is the set of (proper) equivalence classes of primitive positive definite quadratic forms of discriminant D, endowed with a group structure by Dirichlet composition. Then we can state the following beautiful result:

Theorem 2.2.3 *Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic number field K.*

(i) If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite form of discriminant D, then $span_{\mathbb{Z}}\{a, \frac{-b+\sqrt{D}}{2}\}$ is a proper ideal of $\mathcal{O}$.

(ii) The map $f(x,y) \mapsto span_{\mathbb{Z}}\{a, \frac{-b+\sqrt{D}}{2}\}$ induces an isomorphism $C(D) \cong C(\mathcal{O})$.

(iii) A positive integer m is represented by a primitive positive definite form $f(x,y)$ if and only if m is the norm $N(\mathfrak{a})$ of some ideal $\mathfrak{a}$ in the corresponding ideal class in $C(\mathcal{O})$.

Proof: Theorem 7.7 in [1] □

Remark: Theorem 2.2.3 does not hold for real quadratic number fields, see [1], p.142 for a counterexample.

Corollary 2.2.4 *Let $\mathcal{O}$ be an order in an imaginary quadratic number field, and let $n \in \mathbb{N}$ be a positive integer. Then every ideal class in $C(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal whose norm is relatively prime to n.*

Sketch of proof: One can show that for any given primitive positive definite form $f(x,y)$ and any given $n \in \mathbb{N}$, the form $f(x,y)$ represents integers relatively prime to n (see [1], p.35). The result then follows immediately from Theorem 2.2.3, (iii). □

2.3 From orders to class field theory

Now let $\mathfrak{a}$ be a non-zero ideal in an order $\mathcal{O}$ of conductor f. Then $\mathfrak{a}$ is said to be **prime to** f whenever

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O}$$

holds. It is straightforward to show that an $\mathcal{O}$-ideal $\mathfrak{a}$ is prime to f if and only if its norm $N(\mathfrak{a})$ is prime to f and that $\mathcal{O}$-ideals prime to f are proper. For a proof of these basic results, consult [1], Lemma 7.18. Note that these two facts together imply that the $\mathcal{O}$-ideals prime to f lie in $I(\mathcal{O})$ and are closed under multiplication. The subgroup of $I(\mathcal{O})$ they generate is denoted by $I(\mathcal{O}, f)$. Furthermore, we denote by $P(\mathcal{O}, f)$ be the subgroup of $I(\mathcal{O}, f)$ generated by the *principal* ideals prime to f. As the following lemma shows, the quotient of these two groups is again the ideal class group:

Lemma 2.3.1 *There is a natural isomorphism $I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O})$ induced by the inclusion.*

Sketch of proof: Consider the natural map $I(\mathcal{O}, f) \to C(\mathcal{O})$. Its kernel is $I(\mathcal{O}, f) \cap P(\mathcal{O})$, which can easily be shown to be equal to $P(\mathcal{O}, f)$ (see [1], p.144). The proof now reduces to showing that this map is in fact surjective. But this follows directly from Corollary 2.2.4. □

To make our considerations so far available to class field theory, we need to translate the developed tools into the language of ideals of the maximal order $\mathcal{O}_K$ instead of $\mathcal{O}$. For this purpose, let I_K be the group of fractional $\mathcal{O}_K$-ideals and let $I_K(f)$ denote the subgroup of I_K generated by the $\mathcal{O}_K$-ideals prime to f. Then one can prove the following result:

Lemma 2.3.2 *Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic number field K. The mapping $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ is a bijection between the $\mathcal{O}_K$-ideals prime to f and the $\mathcal{O}$-ideals prime to f, and its inverse is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. Furthermore, this bijection preserves the norm of the ideals. By extension, we get an isomorphism $I_K(f) \cong I(\mathcal{O}, f)$.*

Sketch of proof: Let $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal prime to f. The canonical projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$ induces an injection $\iota : \mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \hookrightarrow \mathcal{O}_K/\mathfrak{a}$, and since $N(\mathfrak{a})$ is prime to f, so is $N(\mathfrak{a} \cap \mathcal{O})$. Therefore $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal prime to f. Now $\mathfrak{a}$ is prime to f, and hence multiplication by f is an automorphism of $\mathcal{O}_K/\mathfrak{a}$. But $f\mathcal{O}_K \subset \mathcal{O}$, so that ι is surjective and $N(\mathcal{O}/(\mathfrak{a} \cap \mathcal{O})) = N(\mathcal{O}_K/\mathfrak{a})$ follows. Similarly, one can show that if $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal which is also prime to f and of the same norm.
The next step is to prove that these maps are in fact inverse, ie. that $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a}$ if $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f and $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$ if $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f. This tedious calculations will be omitted here, but the interested reader can find them in [1], Prop.7.20.
To finish the proof we have to show the multiplicativity of this map, for we want to extend it to an isomorphism $I_K(f) \cong I(\mathcal{O}, f)$. But the inverse map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ obviously does respect multiplication, and therefore we are finished. □

Now recall that $I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong C(\mathcal{O})$. The isomorphism from Lemma 2.3.2 tells us now that there is a subgroup $P_{K,\mathbb{Z}}(f) \subset I_K(f)$ such that

$$I_K(f)/P_{K,\mathbb{Z}}(f) \cong C(\mathcal{O}).$$

The following result tells us explicitly how $P_{K,\mathbb{Z}}(f)$ looks like:

Lemma 2.3.3 *$P_{K,\mathbb{Z}}(f)$ is the subgroup of $I_K(f)$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer a relatively prime to f.*

Sketch of proof: The main point is to show the following equivalence: For $\alpha \in \mathcal{O}_K$ we have

$$\alpha \equiv a \text{ mod } f\mathcal{O}_K \text{ for some } a \in \mathbb{Z} \text{ satisfying } \gcd(a, f) = 1 \Leftrightarrow \alpha \in \mathcal{O},\ \gcd(N(\alpha), f) = 1. \quad (2.1)$$

The proof of this can be found in [1], Prop 7.22. Now $P(\mathcal{O}, f)$ is generated by the ideals $\alpha\mathcal{O}$, where $\alpha \in \mathcal{O}$ and $\gcd(N(\alpha), f) = 1$. Using the inverse map of Lemma 2.3.2, we see that $P_{K,\mathbb{Z}}(f)$ is generated by the ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies the left hand side of (2.1). □

To sum up, we found natural isomorphisms

$$C(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbb{Z}}(f), \quad (2.2)$$

which will be of heavy use in the next sections.

Chapter 3

Class field theory

3.1 Artin symbol

Lemma 3.1.1 *Let L/K be a finite Galois extension, $\mathfrak{p} \subset \mathcal{O}_K$ a prime which is unramified in L and $\mathfrak{P} \subset \mathcal{O}_L$ be a prime lying above $\mathfrak{p}$, i.e. satisfying $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then there is a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that*

$$\forall \alpha \in \mathcal{O}_L : \ \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

Proof: Lemma 5.19 in [1]. □

Definition 3.1.2 (Artin symbol) *The unique element from Lemma 3.1.1 is denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$ and called the Artin symbol of the extension L/K at $\mathfrak{P}$.*

We say that a prime $\mathfrak{p} \subset \mathcal{O}_K$ **splits completely** in a Galois extension L/K if the ramification index $e(\mathfrak{P}|\mathfrak{p})$ and the inertial degree $f(\mathfrak{P}|\mathfrak{p})$ both are equal to 1 for all primes $\mathfrak{P}$ satisfying $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. In this case, there are exactly $[L : K]$ primes lying above $\mathfrak{p}$. The following Lemma relates this property to the Artin symbol just defined:

Lemma 3.1.3 *An unramified prime $\mathfrak{p} \in \mathcal{O}_K$ splits completely in a Galois extension L if and only if*

$$\left(\frac{L/K}{\mathfrak{P}}\right) = \mathrm{Id}$$

for some prime $\mathfrak{P}$ lying over $\mathfrak{p}$.

Proof: To prove this lemma, we first need to review some standard facts about ramification. The **decomposition group** of $\mathfrak{P}$ is defined by

$$D_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

whereas the **inertia group** of $\mathfrak{P}$ is given by

$$I_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \forall \alpha \in \mathcal{O}_L : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}\}.$$

A first result is that $I_\beta \subset D_\beta$ and that any $\sigma \in \ D_\beta$ induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}$, which is given by $\overline{\sigma}(\alpha + \mathfrak{P}) = \sigma(\alpha) + \mathfrak{P}$ and therefore is the identity on $\mathcal{O}_K/\mathfrak{p}$. Hence we have a homomorphism $D_\beta \to \widetilde{G} := \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p})$. It is easy to show that this homomorphism is surjective with kernel I_β, and that $|I_\beta|$ is equal to the ramification index of $\mathfrak{p}$ in $\mathfrak{P}$, i.e. we have $|I_\beta| = e(\mathfrak{P}|\mathfrak{p})$. In particular, it follows $D_\beta/I_\beta \cong \widetilde{G}$. Consult e.g. [2], Chapter I.5 for a proof of these standard facts.

Now we can proceed with the actual proof. Since $\mathfrak{p}$ is unramified in L, we have $|I_\beta| = 1$ and therefore $D_\beta \cong \widetilde{G}$. But we know from Galois theory of finite fields that $\widetilde{G}$ is a cyclic group of order $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f(\mathfrak{P}|\mathfrak{p})$. Moreover, we know that $\widetilde{G}$ is generated by the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$, where $N(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}]$.

Lemma 3.1.1 shows that the Artin Symbol maps to the Frobenius element under $D_\beta \to \widetilde{G}$, and therefore its order is equal to $f(\mathfrak{P}|\mathfrak{p})$. Now $\mathfrak{p}$ splits completely in L iff $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$. For unramified primes $\mathfrak{p}$, this reduces to $f(\mathfrak{P}|\mathfrak{p}) = 1$, which in turn is equivalent to ord $\left(\frac{L/K}{\mathfrak{P}}\right) = 1$, i.e. $\left(\frac{L/K}{\mathfrak{P}}\right) = \mathrm{Id}$. □

Now we want to extend our definition of the Artin symbol to get a dependence on the underlying prime $\mathfrak{p}$. In order to do this, we need the following basic properties:

Lemma 3.1.4 *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime of a number field K, and let L/K be a Galois extension. Then we have:*

(i) $\mathrm{Gal}(L/K)$ *acts transitively on the primes lying above* $\mathfrak{p}$.

(ii) *For any $\sigma \in \mathrm{Gal}(L/K)$, one has* $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$.

Proof: See [2], p.12 and p.198. □

Lemma 3.1.4 shows that for any prime $\mathfrak{P}$ lying above $\mathfrak{p}$, the corresponding Artin symbols lie in the same conjugacy class of $\mathrm{Gal}(L/K)$. In fact, they form a complete conjugacy class of $\mathrm{Gal}(L/K)$. This leads to the following definition:

Definition 3.1.5 *Let L/K be a Galois extension, $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ be any prime of L lying above p. Then we can define the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ as follows:*

(i) *If L/K is abelian, then* $\left(\frac{L/K}{\mathfrak{p}}\right) := \left(\frac{L/K}{\mathfrak{P}}\right)$.

(ii) *If L/K is non-abelian, then* $\left(\frac{L/K}{\mathfrak{p}}\right) := \langle\left(\frac{L/K}{\mathfrak{P}}\right)\rangle$, *where $\langle\cdot\rangle$ denotes the conjugacy class of an element in* $\mathrm{Gal}(L/K)$.

3.2 Existence Theorem

Given a number field K, prime ideals of $\mathcal{O}_K$ are often called **finite primes**, whereas infinite primes are given by the embeddings $K \hookrightarrow \mathbb{C}$. More precisely, a **real infinite prime** is an embedding $\sigma : K \hookrightarrow \mathbb{R}$, while a **complex infinite prime** is a pair of complex conjugate embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$.

Now we can introduce the notion of a modulus in a number field K:

Definition 3.2.1 (Modulus) *A modulus $\mathfrak{m}$ is a formal product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ is a product of real infinite primes of K.*

Remark: If $K = \mathbb{Q}[\sqrt{-n}]$ for some integer $n \in \mathbb{N}$, the notions of moduli and $\mathcal{O}_K$-ideals coincide.

Given a modulus $\mathfrak{m}$, we define $I_k(\mathfrak{m}) \subset I_k$ to be the subgroup of I_k generated by the prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}_0$. In other words, $I_k(\mathfrak{m})$ is the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{m}_0$.

Furthermore, let $P_{K,1}(\mathfrak{m}) \subset I_k(\mathfrak{m})$ be the subgroup of $I_k(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ obeys

$$\alpha \equiv 1 \bmod \mathfrak{m}_0 \text{ and } \sigma(\alpha) > 0 \text{ for all } \sigma \text{ dividing } m_\infty.$$

The subgroups H of $I_k(\mathfrak{m})$ containing $P_{K,1}(\mathfrak{m})$, i.e. satisfying

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_k(\mathfrak{m})$$

are called **congruence subgroups**. If H is a congruence subgroup, then the quotient $I_k(\mathfrak{m})/H$ is called a **generalized ideal class group** for $\mathfrak{m}$. It can be shown that this quotient is in fact a finite abelian group. Moreover, as Theorem 3.2.4 below will show, this group can be realized as the Galois group of some finite abelian extension L/K.

To justify the name, consider the case $\mathfrak{m} = \mathcal{O}_K$. Then, using $P_{K,1}(\mathfrak{m}) = P_K$ and $I_K(\mathfrak{m}) = I_K$, it follows immediately that the ideal class group $C(\mathcal{O}_K) = I_K/P_K$ is in fact a generalized ideal class group.

Now we want to extend the notion of ramification to infinite primes:

Definition 3.2.2 (Ramification for infinite primes) *Given an extension L/K, an infinite prime σ of K ramifies in L if σ is real but has an extension to L which is complex.*

It is clear by definition that there are only finitely many infinite primes that ramify in a given extension L/K. Less obvious is the fact that also only finitely many finite primes of K ramify in

L. More precisely, the ramified finite primes of L/K are exactly those dividing the discriminant ideal $\Delta(\mathcal{O}_L/\mathcal{O}_K)$ (see [3], p.213).

Now let $\mathfrak{m}$ be a modulus divisible by all (finite or infinite) ramified primes of an abelian extension L/K. If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal not dividing $\mathfrak{m}$, then $\mathfrak{p}$ is unramified in L and therefore $(\frac{L/K}{\mathfrak{P}})$ is defined for $\mathfrak{p}$. More generally, if $\mathfrak{a} \in I_k$ is any fractional ideal whose prime factors do not divide $\mathfrak{m}$, say $\mathfrak{a} = \prod_{i=1}^k \mathfrak{p}_i^{r_i}$, we can define the Artin symbol of $\mathfrak{a}$ to be

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \prod_{i=1}^{k} \left(\frac{L/K}{\mathfrak{p}}\right)^{r_i}.$$

Therefore, we can extend the Artin symbol to give us a group homomorphism

$$\Phi_\mathfrak{m} : I_K(\mathfrak{m}) \rightarrow \mathrm{Gal}(L/K)$$

called the **Artin map**, which is omnipresent in class field theory. A first characterization is given by the following theorem:

Theorem 3.2.3 *Let $\mathfrak{m}$ be a modulus divisible by all (finite or infinite) ramified primes of an abelian extension L/K. Then the Artin map $\Phi_\mathfrak{m}$ is surjective.*

Proof: See [4], p.197. □

To introduce the notion of a ring class field in the next section, we need the famous existence theorem of class field theory:

Theorem 3.2.4 (Existence Theorem) *Let $\mathfrak{m}$ be a modulus of K and H be a congruence subgroup for $\mathfrak{m}$, i.e. $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$. Then there is a unique abelian extension L/K such that*

(i) *All (finite or infinite) primes of K that ramify in L divide $\mathfrak{m}$, i.e. we can define the Artin map $\Phi_\mathfrak{m} : I_k(\mathfrak{m}) \rightarrow \mathrm{Gal}(L/K)$.*

(ii) $\ker(\Phi_\mathfrak{m}) = H$.

Proof: See [4], p.209. □

Remarks:

(i) Theorems 3.2.3 and 3.2.4 together imply, that there is an abelian extension L/K satisfying

$$I_k(\mathfrak{m})/H \cong \mathrm{Gal}(L/K).$$

In particular, every generalized ideal class group is isomorphic to the Galois group of some abelian extension L/K.

(ii) The converse is also true (this is the so-called Artin reciprocity Theorem, see [4], p.197): If L/K is an abelian extension, then there is a modulus $\mathfrak{m}$ divisible by all (finite or infinite) ramified primes of K such that

$$P_{K,1}(m) \subset \ker(\Phi_{\mathfrak{m}}) \subset I_K(\mathfrak{m})$$

and therefore $\mathrm{Gal}(L/K) \cong I_k(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}})$ is isomorphic to a generalized ideal class group for $\mathfrak{m}$.

3.3 Ring class fields

Let $\mathcal{O} \subset K$ be an order of conductor f in an imaginary quadratic number field. In the previous sections we have seen that

$$C(\mathcal{O}) = I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbb{Z}}(f).$$

Until this point, the subgroup $P_{K,\mathbb{Z}}(f) \subset I_K(f)$ seemed like a rather unnatural construction. Therefore it is nice to have the following lemma:

Lemma 3.3.1 *$P_{K,\mathbb{Z}}(f)$ is a congruence subgroup for the modulus $f\mathcal{O}_K$, i.e. we have*

$$P_{K,1}(f\mathcal{O}_K) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f\mathcal{O}_K).$$

Proof: By definition, we find that $P_{K,1}(f\mathcal{O}_K)$ is generated by the principal ideals

$$\{\alpha\mathcal{O}_K \mid \alpha \in \mathcal{O}_K, \alpha \equiv 1 \bmod f\mathcal{O}_K\}.$$

Furthermore, Lemma 2.3.3 shows that $P_{K,\mathbb{Z}}$ is generated by the principal ideals

$$\{\alpha\mathcal{O}_K \mid \alpha \in \mathcal{O}_K, \alpha \equiv a \bmod f\mathcal{O}_K \text{ for some } a \in \mathbb{Z} \text{ satisying } \gcd(a, f) = 1\}.$$

The first inclusion is therefore obvious.
Again by definition, $I_K(f\mathcal{O}_K)$ is generated by the prime ideals not dividing $f\mathcal{O}_K$. Recall from chapter 2 that $I_K(f)$ is the subgroup of I_K generated by the $\mathcal{O}_K$-ideals prime to f. Since we know already that $P_{K,\mathbb{Z}} \subset I_K(f)$, it suffices to show that $I_K(f) \subset I_K(f\mathcal{O}_K)$. Now let $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal prime to f, i.e. $\mathfrak{a} + f\mathcal{O}_K = \mathcal{O}_K$. If $\mathfrak{p}$ is any prime divisor of $\mathfrak{a}$, it follows directly that $\mathfrak{p}$ does not divide $f\mathcal{O}_K$, because otherwise one would have $\mathfrak{p}|\mathcal{O}_K$ and hence a contradiction. Therefore we find $\mathfrak{a} \in I_K(f\mathcal{O}_K)$ and the lemma is proved. □

The first remark after Theorem 3.2.4 tells us now, that there is a unique abelian extension L/K, all of whose ramified primes divide $f\mathcal{O}_K$, such that

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(L/K). \tag{3.1}$$

This leads to the following definition:

Definition 3.3.2 (Ring class field) *Let $\mathcal{O}$ be an order of conductor f in a number field K. Then the ring class field of $\mathcal{O}$ is defined to be the unique abelian extension L/K satisfying:*

(i) *All ramified primes of L/K divide $f\mathcal{O}_K$.*

(ii) $\mathrm{Gal}(L/K) \cong C(\mathcal{O})$*, where $C(\mathcal{O})$ is the ideal class group of $\mathcal{O}$.*

In the case where K is imaginary quadratic, one can show that L is always galois over $\mathbb{Q}$. What one has to verify is that L is invariant under complex conjugation (see [1], p.181). Furthermore, the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ relates to $\mathrm{Gal}(L/K)$ in the follwing way:

Lemma 3.3.3 *Let L be the ring class field of an order in an imaginary quadratic field K. Then $L/\mathbb{Q}$ is galois with Galois group*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L/K) \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z},$$

where $\varphi(1)(\sigma) = \sigma^{-1}$ for $\sigma \in \mathrm{Gal}(L/K)$.

Proof: Lemma 9.3 in [1]. □

3.4 Cebotarev density Theorem

There is one last Theorem that we shall require for our result about primes represented by quadratic forms in chapter 5. It is the famous Cebotarev density Theorem, which we will state without proof. But first we need to introduce the notion of Dirichlet density.

Definition 3.4.1 (Dirichlet density) *Let K be a number field, and $\mathcal{P}_K$ denote the set of prime ideals of $\mathcal{O}_K$. For any subset $\mathcal{S} \subset \mathcal{P}_K$ we define the Dirichlet density of $\mathcal{S}$ to be*

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

provided the limit exists.

The Dirichlet density has many interesting properties and applications. For our purposes we will need the following

Lemma 3.4.2 *The Dirichlet density has the following properties:*

(i) *If S is finite, then $\delta(S) = 0$.*

(ii) *If $\delta(S)$ exists and T differs from S by finitely many elements, then $\delta(T) = \delta(S)$.*

Proof: The proof of (i) can be found in [4], p.160. The implication (i)⇒(ii) is obvoius. □

Now we state the Theorem of Cebotarev, which provides some very useful information about the Artin map:

Theorem 3.4.3 (Cebotarev density Theorem) *Let L/K be galois, and let $\langle\sigma\rangle$ be the conjugacy class of an element $\sigma \in \mathrm{Gal}(L/K)$. Then the set*

$$\mathcal{S} = \{\mathfrak{p} \in \mathcal{P}_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and } \left(\frac{L/K}{\mathfrak{p}}\right) = \langle\sigma\rangle\}$$

has Dirichlet density

$$\delta(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(L/K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}.$$

Proof: Theorem 10, Chapter VIII in [2]. □

Chapter 4

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

4.1 A first characterization

After all these preparations, we are finally in the position to give a first characterization of the primes which can be written as $x^2 + ny^2$ for fixed $n \in \mathbb{N}$ and $x, y \in \mathbb{Z}$:

Theorem 4.1.1 *Let $n > 0$ be an integer and L be the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in $K = \mathbb{Q}[\sqrt{-n}]$. If $p > 2$ is a prime not dividing n, then*

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow p \text{ splits completely in } L.$$

Proof: We will divide the proof into several little lemmas, each of which is easy to prove. Throughout we will assume that p is an odd prime not dividing n, and $\mathcal{O}$ will denote the order $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{Q}[\sqrt{-n}]$, whereas $\mathcal{O}_K$ stands for the full ring of integers in K. As usual, we set the conductor f equal to $f = [\mathcal{O}_K : \mathcal{O}]$.

Lemma 4.1.2 *Let $n > 0$ be an integer and $K = \mathbb{Q}[\sqrt{-n}]$. Then the following are equivalent:*

(i) $p = x^2 + ny^2$ *for some* $x, y \in \mathbb{Z}$.

(ii) $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, *where* $\mathfrak{p} \neq \overline{\mathfrak{p}}$ *are prime ideals of* $\mathcal{O}_K$ *and* $\mathfrak{p} = \alpha\mathcal{O}_K$ *for some* $\alpha \in \mathcal{O}$.

Proof: Let us first assume (i). Then we can find $x, y \in \mathbb{Z}$ such that $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. If we set $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$, then it follows that directly that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} = \alpha\mathcal{O}_K$ and $\alpha = x + \sqrt{-n}y \in \mathcal{O}$. This already has to be the prime factorization of $p\mathcal{O}_K$, since by ramification theory there are at most 2 primes in $\mathcal{O}_K$ lying above p. It remains to prove that $\mathfrak{p} \neq \overline{\mathfrak{p}}$, or in other words, that p is unramified in K. It is a standard fact that a prime $p \in \mathbb{Z}$ ramifies in a quadratic number field K if and only if p divides its discriminant d_K (see [1], p.105). Now recall from chapter 2 the relation $-4n = f^2 d_K$. Since p does not

divide n and $p > 2$ by assumption, it follows that p does not divide d_K either, and therefore p is unramified in K.
Now assume that (ii) holds. Then we can find $x, y \in \mathbb{Z}$ such that $p\mathcal{O}_K = (x + \sqrt{-n}y)(x - \sqrt{-n}y)\mathcal{O}_K = (x^2 + ny^2)\mathcal{O}_K$. This in turn implies that p and $x^2 + ny^2$ are associated elements in the ring $\mathcal{O}_K$. But the only possible units in $\mathcal{O}_K$ are $\{\pm 1, \pm i, \pm\omega, \pm\omega^2\}$, where $\omega = \exp(\frac{2\pi i}{3})$. Therefore it follows that $p = x^2 + ny^2$. □

Now we want to reformulate the second condition from Lemma 4.1.2.

Lemma 4.1.3 *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ lying above p and satisfying $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Then we have:*

$$\mathfrak{p} = \alpha\mathcal{O}_K \text{ for some } \alpha \in \mathcal{O} \Leftrightarrow \mathfrak{p} \in \ P_{K,\mathbb{Z}}(f).$$

Proof: Recall from the proof of Lemma 2.3.3 that $P_{K,\mathbb{Z}}(f)$ is the subgroup of $I_K(f)$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}$ satisfies $\gcd(N(\alpha), f) = 1$. Therefore "$\Leftarrow$" follows directly be definition.
To see "$\Rightarrow$", let $\mathfrak{p} = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}$. Note first that $N(\mathfrak{p}) \mid N(p\mathcal{O}_K)$. Since $\mathfrak{p} \neq \overline{\mathfrak{p}}$, this implies $N(\mathfrak{p}) = p$. But we saw already that p does not divide $f^2 d_K$, so in particular p does not divide f. Using $N(\mathfrak{p}) = N(\alpha)$, we find that $\gcd(N(\alpha), f) = 1$ as desired. □

The next step is to express this result in terms of the ring class field L of $\mathcal{O}$.

Lemma 4.1.4 *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ and L be the ring class field of $\mathcal{O}$. Then we have:*

$$\mathfrak{p} \in P_{K,\mathbb{Z}}(f) \Leftrightarrow \mathfrak{p} \text{ splits completely in } L.$$

Proof: By definition of the ring class field, the Artin map Φ induces an isomorphism $I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(L/K)$. Therefore $\mathfrak{p} \in \ P_{K,\mathbb{Z}}(f)$ if and only if $\mathfrak{p} \in \ker\Phi$, or equivalently, iff $\left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{Id}$. Using Lemma 3.1.3 we get the desired result. □

So far we have shown that the following statements are equivalent:

(i) $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

(ii) $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ are prime ideals and $\mathfrak{p}$ splits completely in L.

The last step is now to show that this second condition is in fact equivalent to the situation where p splits completely in L. We already know from Lemma 3.3.3 that $L/\mathbb{Q}$ is galois. Therefore it suffices to state the following general lemma:

Lemma 4.1.5 *Let $K \subset M \subset L$ be number fields, and let L and M be galois over K. Then for any prime $\mathfrak{p} \subset \mathcal{O}_K$, the following are equivalent:*

(i) $\mathfrak{p} \subset \mathcal{O}_K$ *splits completely in L.*

(ii) $\mathfrak{p}$ *splits completely in* M *and some prime of* $\mathcal{O}_M$ *above* $\mathfrak{p}$ *splits completely in* L.

Sketch of proof: This follows directly from the fact that in a Galois extension L/K, all primes of $\mathcal{O}_L$ containing $\mathfrak{p} \subset \mathcal{O}_K$ have the same ramification index and the same inertial degree. □

4.2 Main theorem

In the last section, we found a theoretic answer to the question which primes can be written as $x^2 + ny^2$. The next step is now to translate the criterion given in Theorem 4.1.1 into a more elementary language.

For this purpose, we need some more information about how the primes $\mathfrak{P}$ lying above some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ look like. In the case of finite Galois extensions, we can state the following useful result:

Lemma 4.2.1 *Let* L/K *be a finite Galois extension, where* $L = K(\alpha)$ *for some* $\alpha \in \mathcal{O}_L$. *Furthermore, let* $f(x) \in \mathcal{O}_K[X]$ *be the minimal polynomial of* α *over* K, *and let* $\mathfrak{p}$ *be a prime in* $\mathcal{O}_K$ *such that* $f(x)$ *is separable mod* $\mathfrak{p}$. *Write* $f(x)$ *as* $f(x) \equiv f_1(x) \cdot \ldots \cdot f_g(x)$ *mod* $\mathfrak{p}$, *where the* f_i*'s are distinct and irreducible mod* $\mathfrak{p}$. *Then* $\mathfrak{p}$ *is unramified in* L *and the primes above* $\mathfrak{p}$ *are exactly* $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$. *Furthermore, all of the* f_i *have the same degree, which is the inertial degree* f.

Proof: Proposition 5.11 in [1]. □

Corollary 4.2.2 *Let* L/K *be a finite Galois extension, where* $L = K(\alpha)$ *for some* $\alpha \in \mathcal{O}_L$. *Furthermore, let* $f(x) \in \mathcal{O}_K[X]$ *be the minimal polynomial of* α *over* K, *and let* $\mathfrak{p}$ *be a prime in* $\mathcal{O}_K$ *such that* $f(x)$ *is separable mod* $\mathfrak{p}$. *Then we find:*

$$\mathfrak{p} \text{ splits completely in } L \Leftrightarrow f(x) \equiv 0 \text{ mod } \mathfrak{p} \text{ has a solution in } \mathcal{O}_K.$$

Proof: We know already from Lemma 4.2.1 that $\mathfrak{p}$ is unramified, i.e. the ramification index e is 1. The lemma tells us also that the inertial degree f is equal to 1 if and only if some f_i has degree 1, i.e. is linear. But this in turn is equivalent to f having a root mod $\mathfrak{p}$ lying in $\mathcal{O}_K$. □

From now on, let L be the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}[\sqrt{-n}]$. Then we can state the following lemma:

Lemma 4.2.3 *There is a real algebraic integer* α *such that* $L = K(\alpha)$. *Its minimal polynomial* $f(x)$ *over* K *has integer coefficients, i.e.* $f(x) \in \mathbb{Z}[X]$.

Proof: Proposition 5.29 in [1]. □

The last result we will need is the following lemma, which gives an elementary criterion for when a prime $p \in \mathbb{Z}$ splits completely in L.

Lemma 4.2.4 *Given α as in Lemma 4.2.3, let $f(x) \in \mathbb{Z}[X]$ be its minimal polynomial over K. If $p \in \mathbb{Z}$ is a prime not dividing the discriminant of f, the following are equivalent:*

(i) *p splits completely in L.*

(ii) *The Legendre symbol $\left(\frac{d_K}{p}\right)$ is equal to one and the equation $f(x) \equiv 0 \bmod p$ has a solution in $\mathbb{Z}$.*

Proof: We know from the proof of Theorem 4.2.5 that the following are equivalent:

(i) p splits completely in L

(ii) $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ are prime ideals and $\mathfrak{p}$ splits completely in L.

Now $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ is equivalent to p splitting in K, and this in turn happens only if $\left(\frac{d_K}{p}\right) = 1$ (see [1], p.105). So the lemma is proved once we showed that

$$\mathfrak{p} \text{ splits completely in L } \Leftrightarrow f(x) \equiv 0 \bmod p \text{ has a solution in } \mathbb{Z}. \tag{4.1}$$

Note that both statements in the lemma imply that p splits completely in K. Therefore we may assume that

$$\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/\mathfrak{p}. \tag{4.2}$$

Furthermore, since p does divide the discriminant of f, we find that $f(x)$ is separable modulo p, or in other words, separable over $\mathbb{Z}/p\mathbb{Z}$. Using (4.2) we see that f is also separable mod $\mathfrak{p}$, and therefore Corollary 4.2.2 yields

$$\mathfrak{p} \text{ splits completely in } L \Leftrightarrow f(x) \equiv 0 \bmod \mathfrak{p} \text{ has a solution in } \mathcal{O}_K.$$

Using again (4.2), we get the desired equivalence of (4.1). □

Finally, we can state our main result:

Theorem 4.2.5 (Main Theorem) *Let $n > 0$ be an integer and L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}] \subset K = \mathbb{Q}[\sqrt{-n}]$. Furthermore, let α be a primitive element of L over K such that its minimal polynomial $f_n(x)$ over K lies in $\mathbb{Z}[X]$. Now assume that p is an odd prime which does neither divide n nor the discriminant of $f_n(x)$. Then the following are equivalent:*

(i) *$p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.*

(ii) *The Legendre symbol* $\left(\frac{-n}{p}\right)$ *is equal to one and the equation* $f_n(x) \equiv 0$ *mod* p *has a solution in* $\mathbb{Z}$.

Proof: Using the identity $\left(\frac{d_K}{p}\right) = \left(\frac{-n}{p}\right)$, this follows directly from Lemma 4.2.4 and Theorem 4.1.1. □

Remarks:

(i) By definition of the ring class field, we find that deg $f_n = [L : K] = |\mathrm{Gal}(L/K)| = |C(\mathcal{O})|$.

(ii) Note that the conditions of Theorem 4.2.5 exclude only finitely many primes p. Therefore, for any fixed $n > 0$, the Theorem tells us for almost all prime numbers, whether they can be written as $x^2 + ny^2$ or not. Once we have f_n, it is easy to calculate the Legendre symbol $\left(\frac{-n}{p}\right)$ (by using the Gauss reciprocity law) and to check (only finitely many possibilities) if f_n has a root mod p.
So the main problem is how to find f_n. If we want to give an explicit answer to the problem in this section, we therefore have to know how to find primitive elements of ring class fields. This can be done by using methods of complex conjugation, but unfortunately this is far beyond the reach of this thesis. For a complete treatment of this issue, consult [1], chapter 3.

(iii) There is a stronger version of Theorem 4.2.5, which can be proved with a little more work (see [1], p.183). Namely, if f_n is a monic integer polynomial of degree $|C(\mathcal{O})|$, for which the equivalence of the main theorem holds, then f_n has to be the minimal polynomial of a primitive element of the ring class field L of $\mathcal{O}$. Hence knowing f_n is equivalent to knowing the ring class field of $\mathbb{Z}[\sqrt{-n}]$.

4.3 An example: $n = -14$

To give a numerical example of the theory just developed, consider the case $n = -14$. Since $-14 \equiv 2 \bmod 4$, the order $\mathbb{Z}[\sqrt{-14}] \subset \mathbb{Q}[\sqrt{-14}]$ is in fact the maximal order. In this case, the ring class field L of $\mathbb{Z}[\sqrt{-14}]$ is called the **Hilbert class field** of $\mathbb{Q}[\sqrt{-14}]$. It can be characterized as follows:

Theorem 4.3.1 *Let* K *be a number field and* L *be its Hilbert class field, i.e. the ring class field of the order* $\mathcal{O}_K \subset K$. *Then* L *is the maximal unramified abelian extension of* K.

Proof: Theorem 8.10 in [1]. □

Returning to our numerical example, it can be shown by elementary means that the Hilbert class field of $K = \mathbb{Q}[\sqrt{-14}]$ is $L = K(\alpha)$, where $\alpha = \sqrt{2\sqrt{2} - 1}$. For this purpose, note that the class number of K is 4, and therefore it suffices to show that L/K is an unramified abelian extension of degree 4. The only tricky part is to show that L/K is indeed unramified; consult [1], p.114 for details.

Note that the minimal polynomial of α equals to $f_{14}(x) = (x^2+1)^2+8$. The discriminant of $f_{14}(x)$ can be shown to be equal to $-7 \cdot 2^{14}$. Therefore, Theorem 4.2.5 yields us to the following result:

Corollary 4.3.2 *If $p \neq 7$ is an odd prime, then*

$$p = x^2 + ny^2 \Leftrightarrow \left(\frac{-14}{p}\right) = 1 \text{ and } (x^2+1)^2 \equiv 8 \bmod p \text{ has a solution in } \mathbb{Z}.$$

Proof: □

Chapter 5

Primitive positive definite forms

5.1 Representation of prime numbers

The aim of this chapter is to show that a primitive positive definite form always represents infintely many prime numbers. This result was first stated by Dirichlet in 1840, but he was only able to prove it for a restricted class of discriminants. The first complete proof was given by Weber in 1882. The proof we will give below uses class field theory and the Cebotarev density theorem.

Theorem 5.1.1 *Let $ax^2 + bxy + cy^2$ be a primitive positive definite quadratic form of discriminant $D < 0$, and let $\mathcal{S}$ be the set of primes represented by this form, i.e.*

$$\mathcal{S} = \{p \text{ prime} \mid p = ax^2 + bxy + cy^2 \text{ for some } x, y \in \mathbb{Z}\}.$$

Then the Dirchlet density $\delta(\mathcal{S})$ exists and is positive, and hence $ax^2 + bxy + cy^2$ represents infintely many prime numbers.

Proof: Let $K = \mathbb{Q}(\sqrt{D})$ and let $\mathcal{O} \subset K$ be the order of discriminant D. The first step is to rewrite the set $\mathcal{S}$ in a suitable manner, so that we can apply class field theory. Consider the form class $[ax^2 + bxy + cy^2] \in C(D)$. By Theorem 2.2.3 (ii), this corresponds to an ideal class $[\mathfrak{a}\,] \in C(\mathcal{O})$ for some proper $\mathcal{O}$-ideal $\mathfrak{a}$. Then Theorem 2.2.3 (iii) implies that we can rewrite $\mathcal{S}$ as

$$\mathcal{S} = \{p \text{ prime} \mid p = N(\mathfrak{b}) \text{ for some } \mathfrak{b} \in [\mathfrak{a}\,]\}. \tag{5.1}$$

By Corollary 2.2.4, we may assume that $\mathfrak{a}$ is prime to the conductor f. In addition, equation (2.2) tells us that $\mathfrak{b} \in [\mathfrak{a}\,] \in C(\mathcal{O})$ corresponds to $\mathfrak{b}\mathcal{O}_K \in [\mathfrak{a}\mathcal{O}_K] \in I_K(f)/P_{K,\mathbb{Z}}(f)$.
From now on we will only consider prime numbers p not dividing f. Furthermore we introduce the following notation: if $\mathcal{S}$ and $\mathcal{T}$ are sets, we will write $\mathcal{S} =' \mathcal{T}$ whenever $\mathcal{S}$ and $\mathcal{T}$ differ only by finitely many elements. Similiarly, we write $\mathcal{S} \subseteq' \mathcal{T}$ if $\mathcal{S} \subseteq \mathcal{T} \cup \Sigma$ for some finite set Σ.

If $\mathfrak{b}$ is prime to f, then $\mathfrak{b}$ and $\mathfrak{b}\mathcal{O}_K$ have the same norm by Lemma 2.3.2, and therefore we can rewrite (5.1) as

$$\mathcal{S} =' \{p \text{ prime} \mid p \nmid f, p = N(\mathfrak{b}\mathcal{O}_K) \text{ for some } \mathfrak{b}\mathcal{O}_K \in [\mathfrak{a}\mathcal{O}_K]\}.$$

But the condition $p = N(\mathfrak{b}\mathcal{O}_K)$ forces $\mathfrak{b}\mathcal{O}_K$ to be prime, so that we finally get

$$\mathcal{S} =' \{p \text{ prime} \mid p \nmid f, p = N(\mathfrak{p}) \text{ for some prime ideal } \mathfrak{p} \in [\mathfrak{a}\mathcal{O}_K]\}. \tag{5.2}$$

Now let L be the ring class field of $\mathcal{O}$. From (3.1) we know that the Artin map induces an isomorphism

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(L/K).$$

Under this map, the class $[\mathfrak{a}\mathcal{O}_K]$ maps to some $\sigma \in \mathrm{Gal}(L/K)$, which we can regard as an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Let $\langle\sigma\rangle$ denote the conjugacy class of σ in $\mathrm{Gal}(L/\mathbb{Q})$ and let $\mathcal{T}$ be the set

$$\mathcal{T} := \left\{p \text{ prime } \mid p \text{ unramified in } L, \left(\frac{L/\mathbb{Q}}{p}\right) = \langle\sigma\rangle\right\}.$$

Now we claim: $\mathcal{S} =' \mathcal{T}$.

Proof: We first show that $\mathcal{T} \subseteq' \mathcal{S}$, i.e. that $\mathcal{S}$ contains $\mathcal{T}$ except finitely many elements. For this purpose, let $p \in \mathcal{T}$. This implies that $(\frac{L/\mathbb{Q}}{p}) = \langle\sigma\rangle$, and hence $(\frac{L/\mathbb{Q}}{\mathfrak{P}}) = \sigma$ for some prime $\mathfrak{P}$ of L lying above p. Now set $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. where $\mathfrak{p}$ is now a prime of K containing p. Note that for $\alpha \in \mathcal{O}_L$ we have

$$\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{P} \tag{5.3}$$

by definition of the Artin symbol. But σ even lies in $\mathrm{Gal}(L/K)$, so for $\alpha \in \mathcal{O}_K$ equation (5.3) implies that

$$\alpha \equiv \alpha^p \bmod \mathfrak{p}.$$

Therefore we have $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ and $N(\mathfrak{p}) = p$. So (5.3) implies that σ is the Artin symbol $(\frac{L/K}{\mathfrak{p}})$. Since the class $[\mathfrak{a}\mathcal{O}_K]$ corresponds to σ under the Artin map, we get $\sigma = (\frac{L/K}{\mathfrak{a}\mathcal{O}_K})$. On the other hand, we just saw that $\sigma = (\frac{L/K}{\mathfrak{p}})$, and hence $\mathfrak{p} \in [\mathfrak{a}\mathcal{O}_K]$ follows.
By (5.2) we find that $\mathcal{T} \subseteq' \mathcal{S}$.

Now let $p \in \mathcal{S}$. Note that $p = N(\mathfrak{p})$ implies that $\mathfrak{p} \subset \mathcal{O}_K$ lies above p. It follows directly by definition of the ring class field that all primes of K that ramify in L must divide $f\mathcal{O}_K$. But we know that p does not divide f, and therefore $\mathfrak{p}$ is unramified in L. Assume that p does not divide d_K. Then p does not divide the discriminant $D = f^2 d_K$ either, and therefore p is unramified in K. All in all we find that p is unramified in L.
Now let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime above $\mathfrak{p}$. By the Artin map we know that $\sigma = (\frac{L/K}{\mathfrak{a}\mathcal{O}_K}) = (\frac{L/K}{\mathfrak{p}})$. This means that for all $\alpha \in \mathcal{O}_L$ we have

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P},$$

which leads to

$$\forall \alpha \in \mathbb{Z} : \sigma(\alpha) \equiv \alpha^{N(p)} \bmod \mathfrak{P}.$$

Hence we find that $(\frac{L/\mathbb{Q}}{p}) = \langle\sigma\rangle$, and $\mathcal{S} \subseteq' \mathcal{T}$ follows.

Now we can apply the Cebotarev density theorem: Theorem 3.4.3 shows directly that $\mathcal{S}$ has Dirichlet density

$$\delta(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{[L:\mathbb{Q}]} > 0.$$

Therefore the set $\mathcal{S}$ is infinite by Lemma 3.4.2. □

Bibliography

[1] D. A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication* John Wiley & Sons, 1989.

[2] S. Lang. *Algebraic number theory* Springer, 1994.

[3] J. Neukirch. *Algebraische Zahlentheorie* Springer, 1992.

[4] G. Janusz. *Algebraic number fields* American Mathematical Society, 1996.

[5] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry* Springer, 1995.