Eötvös Loránd University
Faculty of Science

Zsombor Várkonyi

Binary quadratic forms and quadratic number fields

Diploma Thesis
BSc in Mathematics

Supervisor:
Dr. Gergely Zábrádi

Budapest, 2024

Contents

Acknowledgements

I am extremely grateful to my supervisor, Gergely Zábrádi, for his inspiring lectures, practices and exciting personal consultations. His lectures sparked my interest in algebra from my first semester, helping me explore this beautiful branch of mathematics. He suggested a very interesting topic and has always been available and helpful thoughout the entire year.

I am also grateful to my family for their support and belief in my abilities. My love for mathematics certainly started at a young age with solving problems with my father. I would like to mention my friends and girlfriend as well who have all been patient and supportive with me and helped making this BSc course an unforgettable experience.

Chapter 1

Introduction

The main goal of my thesis is to understand the connection between two seemingly unrelated topics of algebra: quadratic forms and quadratic number fields. Binary quadratic forms are simply homogeneous polynomials of degree two with integer coefficients in two variables. Quadratic number fields are the extensions of the field of rationals ($\mathbb{Q}$) by the square root of one of its elements. The motivation to study this topic partly comes from the fact that both are taught in undergraduate courses to some extent and no advanced tools are required to understand their deep-lying connection. Another source of motivation is the book of Cox titled *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication* [1] which solves the problem of classifying the primes represented by the form $x^2 + ny^2$. My thesis concentrates on only a small part of this book which I recommend for those interested.

In the shortest chapter, Preliminaries, we list the concepts and theorems the remainder of the thesis uses but are not neccessarily taught in undergraduate courses. This includes a characterisation of algebraic integers and a theorem stating that $\mathrm{SL}_2(\mathbb{R})$ acts on the complex upper half plane in a certain way.

Chapter 3 has another goal besides laying the foundations for the final chapter. The reason for this is that general quadratic forms are rarely taught and studied despite some important results of the binary case generalise nicely to the general case. One important source is the lecture notes of Maga [5], however we state and prove some results not listed there. Our results are certainly not new, however they may not have been in the centre of attention. For the second part of Chapter 3 studying binary quadratic forms, we follow the book of Cox [1] again besides the author's notes from the lectures of his supervisor, Zábrádi.

In the final part of the thesis, Chapter 4, we heavily use the results of the previous chapters to prove our main result. This is to be done in several steps as usual in algebra. Firstly we carefully construct two maps, then we factorise by some equivalences and in the end, we manage to show that the two maps are inverses of each other, showing the connection between quadratic forms and number fields. In this part we assume some knowledge in abstract algebra, especially familiarity with field extensions. Good books to learn more about these topics are Marcus [6] and Fröhlich-Taylor [3]. Here we don't follow a single source throughout the entire chapter, but our most important sources are once again the notes from the lectures of Zábrádi and the book of Cox [1].

Chapter 2

Preliminaries

In this chapter, we go through the concepts and theorems we are going to use later and assume that the reader is familiar with. Most of the topics covered in this chapter should normally be familiar to someone with a mathematics degree.

2.1 Algebra and number theory in general

We assume that the reader is familiar with algebra and number theory at the level of undergraduate courses. For those interested, I recommend the books of Cox [1], Kiss [2], and Ireland and Rosen [4] for reading. However, the most important concepts will be redefined.

As we will be working on many different algebraic structures, to avoid confusion, it is important to always be sure about the meaning of certain letters. We try to use the most common notations everywhere, but for the sake of completeness, we also define these ourselves.

Definition 2.1.1. Let us define the following usual notations for the notable sets of numbers:

- $\mathbb{N}$ stands for the set of the natural numbers, i.e. $\mathbb{N} = \{0, 1, 2, \dots\}$.
- $\mathbb{Z}$ is the notation for the set of integers.
- $\mathbb{Q}$ denotes the rationals: $\mathbb{Q} = \left\{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\right\}$.
- $\mathbb{R}$ denotes the set of real numbers.
- $\mathbb{C}$ stands for the set of complex numbers.

- The upper half plane of $\mathbb{C}$ is denoted by $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$.
- $\mathbb{K}$ always stands for some field and $\mathcal{K}$ is a number field (a subfield of $\mathbb{C}$).

We present the first classical result here about the action of the group $\mathrm{SL}_2(\mathbb{R})$ (the two by two real matrices with discriminant 1) on $\mathbb{H}$.

Theorem 2.1.2. *Suppose we have $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, $z \in \mathbb{C}$, and a group action defined as*

$$\gamma(z) = \frac{az+b}{cz+d}$$

Then for every $\gamma \in SL_2(\mathbb{R})$ we have $\gamma(\mathbb{H}) \subseteq \mathbb{H}$.

Equivalently, we can say that $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$.

2.2 About algebraic integers

Definition 2.2.1. $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients.

We now present a theorem characterising algebraic integers. The proof is omitted as this theorem is classical and is also taught in undergraduate algebra course.

Theorem 2.2.2. *For any $\alpha \in \mathbb{C}$, the following statements are equivalent:*

- *α is an algebraic integer.*
- *The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.*
- *α is an element of a subring of $\mathbb{C}$ having a finitely generated additive group.*
- *All the coefficients of the minimal polynomial of α over $\mathbb{Q}$ are integers.*

This concludes the review of assumed prior knowledge.

Chapter 3

Quadratic forms

Quadratic forms play a central role in this thesis because they build a bridge between number theory and algebra in the sense that quadratic forms are purely algebraic objects, yet studying them gives answers to questions arising in number theory. Although this phenomenon might not be rare in mathematics, studying quadratic forms has proven to be very efficient in tackling number theoretical problems, and their theory dates back to Lagrange.

We first investigate quadratic forms of n variables and prove general statements about them and then focus on the more relevant binary case. In the general case, see Maga [5] for reference, and in the binary case, we follow the book of Cox [1] and the lectures of Zábrádi in Number Theory II from the spring semester of 2023. The solutions for some of the problems are the work of the author.

3.1 General quadratic forms

Firstly, we define quadratic forms over a finite-dimensional vector field over a field $\mathbb{K}$. Typically we work with fields $\mathbb{Q}$ or $\mathbb{R}$, yet we aim to prove deep and non-trivial statements about quadratic forms as generally as possible.

Definition 3.1.1. Let n be a positive integer, $\mathbb{K}$ be a field, and V be an n-dimensional vector field over $\mathbb{K}$. $q : V \to \mathbb{K}$ is called a quadratic form if

$$q(x_1, \dots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} x_i x_j$$

holds for all $(x_1, \dots, x_n) \in V$ for some fixed $((a_{i,j}))_{1 \le i,j \le n} \in \mathbb{K}^{n \times n}$.

It is an immediate consequence of the definition that two quadratic forms are the same if all their coefficients are pairwise equal. Thus, we have a set of $((a_{i,j}))_{1 \le i,j \le n}$

matrices which define the same quadratic form, namely A and B define the same form if $A + A^T = B + B^T$, so it is natural to choose the unique symmetric matrix from this set to represent it. From now on it is assumed that $a_{i,j} = a_{j,i}$ for all $i, j \in \{1, \dots, n\}$, i.e. the matrix $((a_{i,j}))_{1 \le i,j \le n}$ is symmetric. It is also natural to identify the quadratic form with its matrix, which is now uniquely defined. Let $\mathrm{Sym}(n, \mathbb{K})$ denote the set of symmetric, $n \times n$ matrices over $\mathbb{K}$.

If we have two quadratic forms whose matrices are similar in the sense that the two matrices can be transformed into each other via a base change (by conjugating with an element of $\mathrm{GL}_n(\mathbb{K})$), it is natural to assume that the two quadratic forms behave similarly. This similarity will be called equivalence and is formalised by Definition 3.1.2.

Definition 3.1.2. Let $A, B \in \mathrm{Sym}(n, \mathbb{K})$. The quadratic forms defined by A and B are said to be *equivalent* if there exists $C \in \mathrm{GL}_n(\mathbb{K})$ such that $B = C^T AC$.

Proposition 3.1.3. The equivalence of quadratic forms is an equivalence relation.

Proof. Let $P, Q, R \in \mathrm{Sym}(n, \mathbb{K})$ and p, q, r be their corresponding quadratic forms.
Reflexivity: $p \cong p$ holds trivially with $C = I$.
Symmetry: $p \cong q \Rightarrow q \cong p$ holds with the choice of C^{-1}.
Transitivity: $p \cong q$, $q \cong r \Rightarrow Q = C_1^T PC_1$, $R = C_2^T QC_2 \Rightarrow R = C_2^T (C_1^T PC_1)C_2 = (C_2^T C_1^T)P(C_1C_2) = (C_1C_2)^T P(C_1C_2)$ which shows $p \cong r$ with the choice of C_1C_2. □

One may also consider quadratic forms over a ring R. This formally means that the quadratic form maps a free n-dimensional R-module into R. In this case, the entries of the quadratic form's representing matrix are not necessarily elements of R, but their doubles are. This follows from the convention of the representing matrix being chosen to be symmetric. The most important case here, in fact the only one we will consider is the case $R = \mathbb{Z}$. These are called *integral* quadratic forms. Any base change in $\mathbb{Z}^n$ is defined by a matrix in $\mathrm{GL}_n(\mathbb{Z})$. We recall that $\mathbb{Z}$-invertible matrices have determinants ± 1 and we deduce an immediate consequence of this below:

Proposition 3.1.4. If A and B are equivalent integral quadratic forms, then $\det A = \det B$.

Proof. We know by 3.1.2 that there is a $C \in \mathrm{GL}_n(\mathbb{Z})$ such that $B = C^T AC$. As a consequence, $\det B = (\det C)^2 \cdot \det A = (\pm 1)^2 \cdot \det A = \det A$. □

Our next goal is to prove a general theorem about the finiteness of the number of equivalence classes and we need some preparation for this. We first define the concept of reducedness and then, based on a strong theorem due to Hermite, show that every positive semidefinite quadratic form is equivalent to a reduced one.

Definition 3.1.5. A positive semidefinite quadratic form $A = ((a_{i,j}))_{1\leq i,j\leq n}$ is said to be *Minkowski reduced* (or *reduced* in short) if $x^T Ax \geq a_{k,k}$ holds for all vectors $x = (x_1, \dots x_n) \in \mathbb{Z}^n$ such that the entries $x_k, \dots x_n$ are relatively prime and $a_{k,k+1} \geq 0$ holds for all $k = 1, \dots n-1$.

Theorem 3.1.6 (Hermite)**.** *For any positive semidefinite symmetric $n \times n$ real matrix A, the following inequalities hold:*

$$0 < m(A) := \min_{x\in\mathbb{Z}^n\setminus\{0\}} x^T Ax \leq \left(\frac{4}{3}\right)^{\overline{\frac{n-1}{2}}} (\det A)^{\overline{\frac{1}{n}}}$$

Proof (from [5]). Since A is positive semidefinite and symmetric, due to the Principal Axis Theorem, there exists an orthogonal real matrix K such that $K^T AK$ is diagonal with positive eigenvalues $\rho_1 \geq \dots \geq \rho_n > 0$. Now we have a lower bound for $x^T Ax$ for any $x \in \mathbb{R}^n$:

$$x^T Ax = (x^T K^{-T})(K^T AK)(K^{-1}x) \geq \rho_n \|K^{-1}x\|^2 = \rho_n \|x\|^2$$

For every non-zero $x \in \mathbb{Z}^n$ we have $\|x\| \geq 1$, which implies $x^T Ax \geq \rho_n$ and proves the positiveness of $m(A)$. We also need to show that $m(A)$ is really a minimum. For any fixed non-zero vector $y \in \mathbb{Z}^n$, the value $d = y^T Ay$ is some finite positive real number. For any integer vector z with $\|z\| > \sqrt{\frac{d}{\rho_n}}$, $z^T Az \geq \rho_n \|z\|^2 > d$ holds, consequently we only need to consider lattice points with norm less than or equal to $\sqrt{\frac{d}{\rho_n}}$. There are only a finite number of lattice points in the n-dimensional ball $\bar{B}(0, \sqrt{\frac{d}{\rho_n}})$, so the minimum must be attained.

The last inequiality, the upper bound of $m(A)$ is to be proven by induction with base case $n = 1$ being obvious. Now let $n \geq 2$ and assume that the statement is true up to $n-1$ and fix a positive semidefinite symmetric $n \times n$ matrix A. Let $a_1 := m(A)$ and $x = (x_1, \dots, x_n)^T \in \mathbb{Z}^n \setminus \{0\}$ be one vector where the minimum is reached: $x^T Ax = a_1$. We observe that $\gcd(x_1, \dots, x_n) = 1$ as if it were $c > 1$, x/c would still be a nonzero integer vector that produces a smaller number $(x/c)^T A(x/c) = a_1/c^2 < a_1$ contradicting with the minimality of a_1.

Based on the previous observation, we know that there exists an integer matrix $\gamma \in \mathrm{GL}_n(\mathbb{Z})$ such that its first column is x itself and consequently, matrix $B = \gamma^T A\gamma$ has a_1 as its upper-left corner entry.

Now let us define a real vector $b \in \mathbb{R}^{n-1}$ and a matrix $A_1 \in \mathbb{R}^{(n-1)\times(n-1)}$ such that the following equality holds:

$$B = \begin{pmatrix} a_1 & a_1 b^T \\ b a_1 & b a_1 b^T + A_1 \end{pmatrix}$$

One can notice that vector b is well-defined by the first column of B and matrix A_1 is also uniquely defined by the lower-right $(n-1)\times(n-1)$ block of B. The motivation of defining b and A_1 in such a way is that now the following identity holds:

$$\begin{pmatrix} 1 & 0 \\ b & \mathrm{id}_{n-1} \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & A_1 \end{pmatrix} \begin{pmatrix} 1 & b^T \\ 0 & \mathrm{id}_{n-1} \end{pmatrix} = \begin{pmatrix} a_1 & a_1 b^T \\ b a_1 & b a_1 b^T + A_1 \end{pmatrix} = B$$

Since B is symmetric, A_1 also has to be symmetric and A_1 is also positive semidefinite because $\begin{pmatrix} a_1 & 0 \\ 0 & A_1 \end{pmatrix}$ is equivalent to B.

The next step is to obtain a useful upper bound for $m(A)$ using the previous decomposition. For any $y \in \mathbb{Z}^n$, we can decompose it as $(y_1, y_2) \in \mathbb{Z} \times \mathbb{Z}^{n-1}$ and now we perform calculations to have a better understanding of what $y^T B y$ is:

$$y^T B y = \begin{pmatrix} y_1 & y_2^T \end{pmatrix} \begin{pmatrix} a_1 & a_1 b^T \\ b a_1 & b a_1 b^T + A_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} =$$

$$= \begin{pmatrix} y_1 a_1 + y_2^T b a_1 & y_1 a_1 b^T + y_2^T b a_1 b^T + y_2^T A_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} =$$

$$= a_1 (y_1^2 + y_{,,}^T b y_1 + y_{,} b^T y_2 + y_2^T b b^T y_2) + y_2^T A_1 y_2 = a_1 (y_1 + y_2^T b)^2 + y_2^t A_1 y_2$$

We now may choose y_2 to be a nonzero vector such that $m(A_1) = y_2^T A_1 y_2$ based on the definiton of $m(A_1)$ and since y_1 can be any integer, we are able to set its value such that $|y_1 + y_2^T b|$ is minimal, namely at most $\frac{1}{2}$. Consequently, $a_1 \leq y^T B y \leq \dfrac{a_1}{4} + m(A_1)$ holds, from which $a_1 \leq \dfrac{4}{3} \cdot m(A_1)$ follows.

From the induction hypothesis, we know that

$$m(A_1) \leq \left(\frac{4}{3}\right)^{\dfrac{n-2}{2}} (\det A_1)^{\dfrac{1}{n-1}}$$

From the equivalence of A and $\begin{pmatrix} a_1 & 0 \\ 0 & A_1 \end{pmatrix}$ we get $a_1 \det A_1 = \det A$. Combining the above two statements together, we obtain

$$a_1 \leq \left(\frac{4}{3}\right)^{\dfrac{n}{2}} \cdot \frac{(\det A)^{1/(n-1)}}{a_1^{1/(n-1)}}$$

Multiplying with the denominator on the right-hand side and raising to the $\frac{n-1}{n}$-th power, the proof is complete by

$$m(A) = a_1 \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det A)^{\frac{1}{n}}$$

□

Turning our attention towards reducedness, our next aim is to prove that there is an equivalent reduced form for any given one. Since the second property of reducedness is easier to handle, we first show that for a quadratic form fulfilling the first property, a reduced equivalent quadratic form can be found in the following statement.

Proposition 3.1.7. For any quadratic form A, there is a quadratic form $B = ((b_{i,j}))_{1\leq i,j\leq n}$ such that A and B are equivalent and B satisfies the following requirements:

- $b_{k,k+1} \geq 0$ for all $k = 1, \ldots n-1$,
- For any given k, the minimum of expressions $x^T Ax$ and $x^T Bx$ are equal to each other where the minimum is taken over all $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ vectors satisfying $\gcd(x_k, \ldots, x_n) = 1$.

Proof (from [5]). Let E_k be the matrix which is diagonal with all its diagonal entries being 1 except for the k-th diagonal entry, which is -1. Note that conjugating a matrix with E_k multiplies its k-th row and k-th column by -1 leaving the k-th diagonal entry unchanged.

We conjugate A by E_k if the $(k, k+1)$-th entry is negative for every k one after another. This way, we obtain a matrix B. B is clearly equivalent to A and also has its close-to-diagonal entries set to nonnegative values. For every vector $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ define y as the vector where the absolute value of every entry is equal to those of x and the sign of y_k is changed if and only if during the previous algorithm, E_k was used to conjugate. Clearly, for every k, $\gcd(x_k, \ldots, x_n) = \gcd(y_k, \ldots, y_n)$ and hence the simple observation $x^T Ax = y^T By$ confirms the claim.

□

Theorem 3.1.8. *For every positive semidefinite quadratic form A, there is a reduced quadratic form B such that A and B are equivalent.*

Proof (from [5]). The proof will heavily rely on both the statement and the proof of 3.1.6. First set $A_0 = A$ and as before, select a matrix $\gamma_1 \in \mathrm{GL}_n(\mathbb{Z})$ such that the upper-left corner entry of $A_1 = \gamma_1^T A \gamma_1$ is minimal. We will make n such steps and in the k-th step, we want the upper-left corner $(k-1) \times (k-1)$ block of A_{k-1} to remain unchanged. As a consequence, we need to set the first $k-1$ columns of γ_k to the first $k-1$ unit vectors.

In the k-th step, $\gamma_k = \begin{pmatrix} \mathrm{id}_{k-1} & * \\ 0 & * \end{pmatrix}$ is chosen such that the k-th diagonal entry of $A_k = \gamma_k^T A_{k-1} \gamma_k$ is minimal. The existence of such a matrix γ_k is also a consequence of the proof presented above for 3.1.6.

After the n-th step, we get a matrix $A_n = B = ((b_{i,j}))_{1 \leq i,j \leq n}$ which is equivalent to A since it was conjugated n times. Alternatively, one can view it as if it were conjugated once with the matrix $\prod_{i=1}^n \gamma_i \in \mathrm{GL}_n(\mathbb{Z})$.

We claim that B fulfills the first property of reducedness, namely that $x^T B x \geq b_{k,k}$ holds for all $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ if entries $x_k, \ldots, x_n$ are relatively prime. Because x is linearly independent of the first $k-1$ basis vectors (which need to remain unchanged in the k-th step), any such x vector was taken into account when we took minimum in the k-th step and selected γ_k. As a consequence, if there were an x' vector with $x'^T B x < b_{k,k}$, the $n-k+1$ lowest entries of the k-th column of γ_k would have been selected to be x', contradicting with the minimality of $b_{k,k}$.

All in all, we managed to construct a matrix B equivalent to A satisfying the first property of being reduced, so Proposition 3.1.7 finishes the proof of the theorem. □

Definition 3.1.9. Given a quadratic form represented by the matrix A, its discriminant is defined to be $-4 \cdot \det A$.

Proposition 3.1.10. Equivalent quadratic forms have equal discriminants.

Proof. Based on the definition above, this statement is straightforward from 3.1.4. □

We need a final statement before we can prove our main theorem.

Proposition 3.1.11. If $A = ((a_{i,j}))_{1 \leq i,j \leq n}$ is Minkowski reduced quadratic form, then we have:

- $0 < a_{1,1} \leq \ldots \leq a_{n,n}$
- $2 \cdot |a_{k,l}| \leq \min(a_{k,k}, a_{l,l})$ for every $1 \leq k, l \leq n$.

Proof (from [5]). Let e_k be the unit vector with 1 at the k-th entry and 0-s elsewhere, the k-th element of the standard basis. Firstly, we know that $a_{k,k} \leq e_{k+1}^T A e_{k+1} = a_{k+1,k+1}$ for any $1 \leq k \leq n-1$. Also, $0 < e_1^T e_1 = a_{1,1}$. Concerning the second claim, for any $1 \leq k < l \leq n$ we have $a_{l,l} \leq (e_k \pm q_l)^T A(e_k \pm e_l) = a_{k,k} \pm 2_{k,l} + a_{l,l}$. □

Theorem 3.1.12. *Let $D < 0$ and $n \in \mathbb{N}$ be fixed. We claim that there is a finite collection of integral n-ary quadratic forms with discriminant D such that every integral n-ary quadratic form with discriminant D is equivalent to at least one of them.*

Proof. Let $R_n(D)$ denote the set of Minkowski reduced integral n-ary quadratic forms with discriminant D. By Theorem 3.1.8, it is enough to show that $R_n(D)$ is finite.

To prove that $R_n(D)$ is finite, we will use Hermite's 3.1.6 Theorem repeatedly. We will construct all matrices in $R_n(D)$ entry-by-entry and conclude that because every entry could only be chosen from a finite set of numbers, the entire set $R_n(D)$ is finite. The matrix we will construct is denoted by $A = ((a_{i,j}))_{1 \leq i,j \leq n}$. By the link between the determinant and the discriminant (3.1.9), we know that $\det A = \dfrac{-D}{4} > 0$. Since $A = ((a_{i,j}))_{1 \leq i,j \leq n}$ is an integral quadratic form, $a_{i,i} \in \mathbb{Z}$ holds for all $1 \leq i \leq n$ and $2 \cdot a_{i,j} \in \mathbb{Z}$ also holds for all $1 \leq i, j \leq n$.

From Theorem 3.1.6 we know that $0 < a_{1,1} \leq \left(\dfrac{4}{3}\right)^{\dfrac{n-1}{2}} (\det A)^{\dfrac{1}{n}}$ and as a consequence, $a_{1,1}$ can only take a finite number of values. It is a positive integer upper-bounded by some function of n and $\det A$. In the next step, $a_{2,2}$ will be $m(A_1)$ where A_1 is defined by

$$B = \begin{pmatrix} a_1 & a_1 b^T \\ b a_1 & b a_1 b^T + A_1 \end{pmatrix}$$

Here b is a vector whose entries have to be integer multiples of $\dfrac{1}{2 \cdot a_{1,1}}$ and as a consequence, the entries of A_1 are integer multiples of $\dfrac{1}{4 \cdot a_{1,1}}$. Reffering again to the proof of 3.1.6, we also have $\det A_1 = \dfrac{\det A}{a_{1,1}}$. Thus $a_{2,2}$ is a positive number, namely at least $a_{1,1}$, is an integer multiple of $\dfrac{1}{4 \cdot a_{1,1}}$ and is upper-bounded by $\left(\dfrac{4}{3}\right)^{\dfrac{n-2}{2}} (\det A_1)^{\dfrac{1}{n-1}}$. So we can conclude that $a_{2,2}$ can only take finitely many different values regardless of the choice of $a_{1,1}$. (The number of values it can take depend on the choice of $a_{1,1}$ but is finite in every case.)

We will repeat the same to prove that $a_{k,k}$ can take a finite number of values. In step k, a matrix A_{k-1} is defined only depending on the choices of $a_{1,1}, \ldots, a_{k-1,k-1}$. The entries in matrix A_{k-1} are integer multiples of $\dfrac{1}{2^k \cdot a_{1,1} \cdot \ldots \cdot a_{k-1,k-1}}$. And again, we have $a_{k,k} \leq \left(\dfrac{4}{3}\right)^{\dfrac{n-k}{2}} (\det A_{k-1})^{\dfrac{1}{n+1-k}}$ where $\det A_{k-1} = \dfrac{\det A}{a_{1,1} \cdot \ldots \cdot a_{k-1,k-1}}$. This confirms the claim that the value of $a_{k,k}$ comes from a finite set for every $1 \leq k \leq n$.

To finish the proof of the theorem, we only need Proposition 3.1.11 which claims that if we already have the diagonal entry fixed, every other entry's absolute value is upper-bounded, consequently, the value of $a_{k,l}$ also comes from a finite set for every $1 \leq k, l \leq n$.

During the construction of all Minkowski reduced integral quadratic forms with disciminant D, we had a finite number of choices for each of the n^2 entries, hence the number of reduced forms with discriminant D is finite. □

This concludes the discussion of general quadratic forms and now we turn our attention towards integral binary quadratic forms.

3.2 Binary quadratic forms

In line with the literature, when we say binary quadratic form, we mean integral binary ones as the results for the case when the coefficients are not necessarily integers are usually not specific to the binary case and are discussed in Section 3.1.

Definition 3.2.1. We say that $q(x, y) \in \mathbb{Z}[x, y]$ is a *binary quadratic form* if $q(x, y) = ax^2 + bxy + cy^2$ holds for some $a, b, c \in \mathbb{Z}$. A binary quadratic form is said to be *primitive* if $(a, b, c) = 1$ holds.

Proposition 3.2.2. Any quadratic form is an integer multiple of a primitive one.

Proof. For any quadratic form $q(x, y) = ax^2 + bxy + cy^2$, let $n = (a, b, c)$. Now $q = n \cdot \dfrac{q}{n}$ holds, where n is an integer and $\dfrac{q}{n}$ is primitive. □

From now on, we will mainly focus on primitive binary quadratic forms. Some of the concepts discussed above in Section 3.1 will be redefined here as in some cases, the definitions extend the ones in the general case.

Definition 3.2.3. For a quadratic form $q(x, y) = ax^2 + bxy + cy^2$ we define its matrix, denoted by A_q as the following:

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

Note that this matrix A_q is the natural matrix identified with the quadratic form which is also used in Section 3.1. Also, we have $q(x, y) = \begin{pmatrix} x & y \end{pmatrix} A_q \begin{pmatrix} x \\ y \end{pmatrix}$. The entries matrix A_q might not all be integers as the elements in the antidiagonal are equal to $\frac{b}{2}$ and as b can be any integer, its half can have fractional part of one half.

Definition 3.2.4. Two quadratic forms, $q(x, y)$ and $r(x, y)$, are said to be *equivalent* if there exists $S \in \mathrm{GL}_2(\mathbb{Z})$ such that $A_r = S^T A_q S$. The two forms are *properly equivalent* if $S \in \mathrm{SL}_2(\mathbb{Z})$ also holds.

From Section 3.1 we know that the equivalence of quadratic forms is an equivalence relation. The proper equivalence is also an equivalence relation and the proof presented above in 3.1 works for this case as well.

Definition 3.2.5. An integer m is *represented* by a quadratic form q if there are integers x_0, y_0 such that $m = q(x_0, y_0)$. m is said to be *properly represented* by q if x_0 and y_0 can be chosen to be relatively prime.

Proposition 3.2.6. Equivalent quadratic forms represent the same subset of integers.

Proof. By the equivalence of forms q and r, we have $A_r = S^T A_q S$ for some $S \in \mathrm{GL}_2(\mathbb{Z})$. Suppose that we have an integer k which is represented by r, so we have $x, y \in \mathbb{Z}$ such that $r(x, y) = k$. We now have

$$k = r(x, y) = \begin{pmatrix} x & y \end{pmatrix} A_r \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} S^T A_q S \begin{pmatrix} x \\ y \end{pmatrix}$$

Let us define $\begin{pmatrix} u \\ v \end{pmatrix} = S \begin{pmatrix} x \\ y \end{pmatrix}$. u and v are also relatively prime since x and y are relatively prime and $S \in \mathrm{GL}_2(\mathbb{Z})$. By the identity above, we have $k = q(u, v)$ which finishes the proof. □

Lemma 3.2.7. *A primitive quadratic form q properly represents $m \in \mathbb{Z}$ if and only if there are numbers $b, c \in \mathbb{Z}$ such that q is properly equivalent to the quadratic form $mx^2 + bxy + cy^2$.*

Proof. $\Leftarrow$: Plugging $x = 1$, $y = 0$ into $mx^2 + bxy + cy^2$ gives m, so m is properly represented by the latter quadratic form. By their proper equivalence, m is also properly represented by q.

$\Rightarrow$: Let $q(u, v) = m$. We need a matrix $S \in \mathrm{SL}_2(\mathbb{Z})$ whose first column is $(u, v)^T$. This can be achieved by the Eucledian Algorithm since $(u, v) = 1$. Now $S^T A_q S$ has upper-left entry m and so the proof is finished. □

Definition 3.2.8. For a binary quadratic form $q(x, y) = ax^2 + bxy + cy^2$, the *discriminant* of the form, denoted by $\mathcal{D}$, is defined to be $b^2 - 4ac$.

Proposition 3.2.9. Equivalent forms have the same discriminant.

Proof. We first observe that for any quadratic form q with discriminant $\mathcal{D}$, $\mathcal{D} = -4 \det A_q$ holds. Now let q and r be two equivalent quadratic forms such that $A_r = S^T A_q S$. Using the multiplicativity of the determinant of square matrices, $\det A_r = (\det S)^2 \det A_q$ follows. Since $S \in \mathrm{GL}_2(\mathbb{Z})$, $(\det S)^2 = 1$ holds, which confirms the claim. □

Definition 3.2.10. The sign of $\mathcal{D}$ and a determine which numbers can be represented by the form:

- If $\mathcal{D} > 0$, both positive and negative numbers are represented and the form is called *indefinite.*
- If $\mathcal{D} < 0$ and $a > 0$, only positive numbers are represented by the form and we call it *positive definite.*
- If $\mathcal{D} < 0$ and $a < 0$, only negative numbers are represented by the form and it is called *negative definite.*

Proposition 3.2.11. For any q binary quadratic form, its discriminant $\mathcal{D}$ is congruent to either 0 or 1 modulo 4. Also, all such numbers are discriminants of some quadratic form.

Proof. Recall that $\mathcal{D} = b^2 - 4ac$, so the remainder modulo 4 indeed needs to be either 0 or 1. For a given $\mathcal{D} = 4k + 1$, $a = b = 1$, $c = -k$ fulfills the requirements and similarly, for $\mathcal{D} = 4k$, $a = 1$, $b = 0$ and $c = -k$ defines an appropiate quadratic form. □

Lemma 3.2.12. *If $D \equiv 0,\ 1 \bmod 4$ and m is an odd integer, m is properly represented by a primitive quadratic form q with discriminant D if and only if D is a quadratic residue modulo m.*

Proof. If q properly represents m, then $q(x, y) = mx^2 + bxy + cy^2$ can be assumed based on Lemma 3.2.7. Consequently we have $D = b^2 - 4mc$, from which $D \equiv b^2 \bmod m$ follows.

On the other hand, if we have $D \equiv b^2 \bmod m$, it can be assumed that D and b have the same parity as otherwise, b can be replaced by $m + b$. Consequently we have $D \equiv b^2 \bmod 4m$ since the congruence holds true for both m and 4 and they are relatively prime. Thus D can be written in the following form using an integer c: $D = b^2 - 4mc$. Considering the quadratic form $q(x, y) = mx^2 + bxy + cy^2$, we immediately see that it has discriminant D and it is primitive. q also properly represents m trivially with $x = 1$, $y = 0$ and the proof is complete. □

We now turn our attention towards the reducedness of positive definite binary quadratic forms. Recall that reducedness was defined for general quadratic forms in Definition 3.1.5 and let us examine what this definition means for the binary case. It means that a binary quadratic form $q(x, y) = ax^2 + bxy + cy^2$ is reduced if and only if all of the following conditions are met:

- All the integers properly represented by q are greater than or equal to a,
- If $x_2 = \pm 1$ and $x_1 \in \mathbb{Z}$, then $q(x_1, x_2) \geq c$.
- b is non-negative.

We will use a different definition here in the binary case presented below:

Definition 3.2.13. A primitive positive definite form $q(x, y) = ax^2 + bxy + cy^2$ is said to be *reduced* if $|b| \leq a \leq c$ holds and either $a = c$ or $a = |b|$ implies $b \geq 0$.

We first notice that the two definitions are quite similar, in fact if a binary quadratic form is reduced by one of the definitions, then the quadratic form possibly conjugated by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (flipping the sign of b) is reduced by the other definiton. This matrix is in $\mathrm{GL}_2(\mathbb{Z})$ but is not in $\mathrm{SL}_2(\mathbb{Z})$, hence we can say that the difference between the two definitons can be fixed by equivalence, but not necessarily a proper equivalence.

Our next theorem may seem as a special case of Theorem 3.1.8, but it is stronger as it demands proper equivalence and also states uniqueness, two important properties which weren't true in the general case.

Theorem 3.2.14. *Every primitive positive definite form is properly equivalent to a unique reduced form.*

Proof. As for the existence part of the theorem, we use Theorem 3.1.8. By the notes above on the two different definitions, we conclude that for any binary quadratic form q we have another quadratic form p which is reduced by our new definition and they are equivalent, but not necessarily properly equivalent. This means that the determinant of the base change between the A_q and A_p can be ±1 and we want it to be +1. If it is +1, we leave it unchanged and are done. If it is −1 and none of $a = c$ or $a = |b|$ hold, we can swap the sign of b by conjugating with $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and the equivalence will become proper.

Our last two cases are when either $a = c$ or $a = |b|$ hold, but the equivalence is improper. Based on the definiton of reducedness, in these cases we also know that $b \geq 0$, from which $a = b$ follows in the second case which will be very useful for us. If $a = c$ holds, we conjugate by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to swap a and c and the equivalence is proper again. If $a = b$ holds, the matrix we conjugate with is $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. Its determinant is −1 but leaves our specific matrix unchanged, making the equivalence proper again.

We tackle uniqueness next, the statement is that any two reduced positive definite quadratic forms are properly inequivalent. We assume to the contrary that we have two reduced binary quadratic forms $q(x, y) = ax^2 + bxy + cy^2$ and $r(x, y) = a'x^2 + b'xy + c'y^2$ which are properly equivalent, i.e. we have $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_q = \gamma^T A_r \gamma$.

Since q is reduced, we have $|b| \leq a \leq c$ and thus $q(x, y) \geq (a - |b| + c) \cdot \min(x^2, y^2)$. Specifically, if none of x or y is zero, $q(x, y) \geq a - |b| + c$, so a is the smallest non-zero value of q, represented by exactly $x = \pm 1$, $y = 0$. Since equivalent forms represent the same set of integers (see Proposition 3.2.6), we have showed that $a = a'$.

To finish the proof, we need to examine three cases based on the possible equalities between the coefficients of q:

1. $\mathbf{|b| < a < c}$. Here we have c as the second smallest integer properly represented by q as $c < a - |b| + c$. We want to show that $c = c'$. $c' \geq a$ holds surely and if $c' = a$, then we have four solutions to $r(x, y) = a$ in $(\pm 1, 0)$ and $(0, \pm 1)$ contradicting to only having two solutions to $q(x, y) = a$ in $(\pm 1, 0)$. So we can conclude that $c' > a$, meaning that c' is second smallest integer properly represented by r, hence we have $c = c'$ by using Proposition 3.2.6 again. Since the discriminants of the two forms are equal, we deduce $b = \pm b'$. We now consider the matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ which conjugates

A_q into A_r. Suppose $\gamma = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$ and we have $a_0d_0 - b_0c_0 = 1$. Now $a = q(1,0) = r(a_0, b_0)$ and $c = q(0,1) = r(c_0, d_0)$ are proper represantations, meaning that $(a_0, b_0) = \pm(1,0)$ and $(c_0, d_0) = \pm(0,1)$, from which $\gamma = \pm I$ follows. This means that $q = r$.

2. $\mathbf{a = c.}$ (implying $b \geq 0$) Here we have four solutions to $q(x, y) = a$ meaning that there should also exist four solutions to $r(x, y) = a$, meaning that $c' = a$ also holds. By the equality of discriminants, we have $b = \pm b'$ again. This case is easier however, since $b, b' \geq 0$ is forced by reducedness, hence $q = r$ holds.

3. $\mathbf{|b| = a < c.}$ (implying $c > a = b > 0$) The smallest integer properly represented by q is a again, also being represented only by $(\pm 1, 0)$. But c is now properly represented not only by $(0, \pm 1)$ but also by $\pm(1, -1)$. Hence, there should also be four proper solutions to $r(x, y) = c'$, meaning that there are solutions besides $(0, \pm 1)$. Any vector including a number of absolute value at least 2 will result in a number larger than c, so we also need to have $r(\pm 1, \mp 1) = c$, meaning again that $b' = b = a$ and from this we deduce $c = c'$ and $p = q$ again.

We arrived at a contradiction in each of the cases, so the proof is complete. □

Definition 3.2.15. Two quadratic form of discriminant $\mathcal{D}$ belong to the same *class* if they are properly equivalent to each other. The number of these classes for a given $\mathcal{D}$ is denoted by $h(\mathcal{D})$.

Theorem 3.2.16. *$h(\mathcal{D})$ is finite for all $\mathcal{D} < 0$.*

Proof. This follows directly from Theorems 3.2.14 and 3.1.12. □

So we have shown that the class number is finite for all negative discriminants D. Note that for every $n \in \mathbb{N}$, the quadratic form $x^2 + ny^2$ is always reduced and its discriminant is $-4n$. To show that $h(\mathcal{D}) \not\equiv 1$, we give two reduced properly inequivalent quadratic forms with $\mathcal{D} = -20$ as an example: One is $x^2 + 5y^2$ and the other is $2x^2 + 2xy + 3y^2$. One can easily check that they are indeed both reduced and have discriminant -20 and the simple observation that 3 is properly represented by the latter form but not represented by the former form shows that they are not equivalent.

We conclude Chapter 3 by defining a special set of discriminants.

Definition 3.2.17. An integer $\mathcal{D}$ is called a *fundamental discriminant* if it is a discriminant of a binary integral quadratic form (see Proposition 3.2.11) and satisfies one of the followings:

- $\mathcal{D} \equiv 1 \pmod 4$ and $\mathcal{D}$ is square-free.
- $\mathcal{D} = 4d$, where $d \equiv 2, 3 \pmod 4$ and d is square-free.

We will learn more about fundamental discriminants and their connection to quadratic number fields later in Chapter 4.

Chapter 4

Quadratic number fields

In this chapter, we study the quadratic extensions of $\mathbb{Q}$, the field of the rational numbers. An interesting question to study is what will the ring of integers look like in $\mathbb{Q}(\sqrt{d})$ for different integers d. For example, for which values d does the Fundamental Theorem of Number Theory hold in the ring of integers of $\mathbb{Q}(\sqrt{d})$? At the end of the chapter, we will be able to prove our main result, which builds the strong connection between the ideal classes of quadratic number fields and the quadratic binary forms.

We again follow the book of Cox [1] and author's notes from the lectures of Zábrádi.

4.1 Ring of algebraic integers of number fields

We begin by defining number fields in general which are the primary objects we will be working with. We will focus on the specific case where the degree of the field extension is 2, this will be highlighted in Definition 4.1.2 and characterised by Proposition 4.1.3.

Definition 4.1.1. $\mathcal{K}$ is a number if field if it is a subfield of $\mathbb{C}$ and has a finite degree over $\mathbb{Q}$.

Definition 4.1.2. Let $\mathcal{K}$ denote $\mathbb{Q}(\sqrt{d})$, the extension of the field of rationals by $\sqrt{d}$ for some integer d.

Proposition 4.1.3.

$$\mathbb{Q}(\sqrt{d}) = \{p + q\sqrt{d} : p, q \in \mathbb{Q}\}$$

Proof. It is sufficient to show that $H = \{p + q\sqrt{d} : p, q \in \mathbb{Q}\}$ is a field, since all numbers of the form $p+q\sqrt{d}$ are clearly elements of $\mathbb{Q}(\sqrt{d})$ because they are exactly the $\mathbb{Q}$-linear combinations of 1 and $\sqrt{d}$. The only interesting part is to check that division does not lead outside the set H. This holds because

$$\frac{p+q\sqrt{d}}{r+s\sqrt{d}} = \frac{p+q\sqrt{d}}{r+s\sqrt{d}} \cdot \frac{r-s\sqrt{d}}{r-s\sqrt{d}} = \frac{pr-qsd}{r^2-ds^2} + \frac{qr-ps}{r^2-ds^2}\sqrt{d} \in H$$

The above equality confirms that H is indeed a field and concludes the proof. □

We recall a few well-known notations concerning elements of $\mathbb{Q}(\sqrt{d})$. For $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, where $a, b \in \mathbb{Q}$, we say that the *conjugate* of α, denoted by $\bar{\alpha}$ is $a - b\sqrt{d}$, the *trace* of α, denoted by $Tr(\alpha)$ is $\alpha + \bar{\alpha} = 2a$ and the *norm* of α is denoted by $N(\alpha)$ and defined to be $\alpha\bar{\alpha} = a^2 - db^2$. Note that the norm of the elements is indeed a norm in the usual sense.

One of the most important and fundamental concepts of this chapter is the algebraic integer. Similarly to the usual integers, $\mathbb{Z}$, the algebraic integers contained inside a number field turn out to form a ring with addition and multiplication, as pointed out by Corollary 4.1.4.

Corollary 4.1.4. *The set of algebraic integers in* $\mathbb{C}$ *form a ring.*

Proof. We have to show that α and β being algebraic integers imply $\alpha \pm \beta$ and $\alpha \cdot \beta$ also being algebraic integers. By 2.2.2, we know that the rings $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ have finitely generated additive groups, so lets suppose that $\{a_1, \dots a_n\}$ and $\{b_1, \dots b_m\}$ generate them, respectively. Then, $\mathbb{Z}[\alpha, \beta]$ is generated by $\{a_i b_j | 1 \leq i \leq n, 1 \leq j \leq m\}$, so it is also finitely generated. Finally, $\alpha \pm \beta$ and $\alpha \cdot \beta$ are elements of $\mathbb{Z}[\alpha, \beta]$, so by the third characterization of 2.2.2, they are also algebraic integers. □

After having a basic knowledge of algebraic integers in general, we move on to examine the set of algebraic integers contained in a number field $\mathcal{K}$. Unsurprisingly, they also form a ring, and in the case of $\mathcal{K} = \mathbb{Q}(\sqrt{d})$, we will also have an explicit charachterization by 4.1.7.

Definition 4.1.5. Let $\mathcal{O}_\mathcal{K}$ denote the set of algebraic integers in $\mathcal{K}$:

$$\mathcal{O}_\mathcal{K} = \{\alpha \in \mathcal{K} \mid \exists f \in \mathbb{Z}[x] \text{ monic} : f(\alpha) = 0\}$$

Proposition 4.1.6. $\mathcal{O}_\mathcal{K}$ is a subring of $\mathbb{C}$.

Proof. $\mathcal{O}_\mathcal{K}$ is defined to be the intersection of the ring of algebraic integers in $\mathbb{C}$ and $\mathcal{K}$, which are both rings. As a consequence, $\mathcal{O}_\mathcal{K}$ is a ring itself. □

Proposition 4.1.7. Let d be a square-free integer, and $\mathcal{K} = \mathbb{Q}(\sqrt{d})$. $\mathcal{O}_\mathcal{K}$ is:

- $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$.
- $\mathbb{Z}\left[\dfrac{\sqrt{d}+1}{2}\right]$ if $d \equiv 1 \pmod 4$.

Proof. For an arbitrary element $\alpha = a + b\sqrt{d} \in \mathcal{K}$, we need a necessary and sufficient condition on a and b for α to be an algebraic integer. By the fourth statement in 2.2.2, we know that $m_\alpha(x) = (x - a - b\sqrt{d})(x - a + b\sqrt{d}) = x^2 - 2ax + a^2 - b^2 d \in \mathbb{Z}[x]$.

So $\alpha \in \mathcal{O}_\mathcal{K} \iff -2a$ and $a^2 - b^2 d$ are both integers. We first examine the $d \equiv 1 \pmod 4$ case, let us denote $d = 4d' + 1$ where $d' \in \mathbb{Z}$. Clearly, $2a$ needs to be an integer, let $2a = a' \in \mathbb{Z}$. We have

$$\frac{(a')^2}{4} - b^2(4d' + 1) = a^2 - b^2 d \in \mathbb{Z}$$

Since $(a')^2$ gives remainder 0 or 1 modulo 4, $4b^2(4d' + 1) = (2b)^2(4d' + 1)$ needs to give the same remainder meaning that $2a = a'$ and $2b$ have the same parity. This confirms that the ring of algebraic integers in this case is indeed $\mathbb{Z}\left[\dfrac{\sqrt{d}+1}{2}\right]$.

Concerning the $d \equiv 2, 3 \pmod 4$ case, if a were not an integer but the half of one, a^2 would be an integer $+\frac{1}{4}$, so $b^2 d$ is also an integer $+\frac{1}{4}$. Since $d \equiv 2, 3 \pmod 4$, it follows that b is irrational, a contradiction. Thus a needs to be an integer and as a consequence, b also. So the ring of algebraic integers in this case is $\mathbb{Z}[\sqrt{d}]$. □

It is important that by examining the minimal polynomials of $\sqrt{d}$ and $\frac{\sqrt{d}+1}{2}$ in the two cases of 4.1.7 respectively, we can obtain primitive integral binary quadratic forms with a fundamental discriminant.

In the case of $d \equiv 2, 3 \pmod 4$, the minimal polynomial of $\sqrt{d}$ is $x^2 - d$ which corresponds to the quadratic form $q(x, y) = x^2 - dy^2$. It is easy to see that q is primitive. The discriminant of q is $4d$ which is a fundamental discriminant by 3.2.17.

If $d \equiv 1 \pmod 4$, we are looking for the minimal polynomial of $\frac{\sqrt{d}+1}{2}$, which turns out to be $x^2 + x - \frac{d-1}{4}$. The correspondng quadratic form is $r(x, y) = x^2 + xy + \frac{d-1}{4}y^2$ which is also primitive. Its discriminant is d itself, which is also fundamental by 3.2.17.

Definition 4.1.8. If $\mathcal{K} = \mathbb{Q}(\sqrt{d})$, let $d_\mathcal{K}$ denote the discriminant of the minimal polynomial of the primitive element of $\mathcal{O}_\mathcal{K}$.

Proposition 4.1.9. $d_\mathcal{K} = \begin{cases} 4d & \text{if } d \equiv 2, 3 \bmod 4, \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$

Proof. This is a direct consequence of Proposition 4.1.7 and the discussion of the minimal polynomials above. □

We now understand the motivation behind the definition of fundamental discriminants earlier. As a next step, we would like to decide if the Fundamental Theorem of Arithmetic holds in $\mathcal{O}_{\mathcal{K}}$ for a given negative $d_{\mathcal{K}}$. To answer this question, we need to study the ideals of $\mathcal{O}_{\mathcal{K}}$.

4.2 Assigning ideals to quadratic forms

The main goal of the remainder of the thesis is to prove that there is a bijection between the reduced binary quadratic forms of discriminant d and the ideal classes of the ring of algebraic integers of a field extension $\mathbb{Q}(\sqrt{d})$ where d is a negative fundamental discriminant. This is to be shown in several steps: we first need to assign an ideal to each quadratic form, then assign a quadratic form to each ideal and finally show that these two functions are the inverses of each other.

Some statements in the paragraph above are intentionally not precise as some concepts are yet to be defined (for example, we will assign a quadratic form to ideal classes, not ideals). The goal of this paragraph is to give an overview of what is described below precisely.

In this section we will construct a function from the set of reduced quadratic forms to the set of ideals of $\mathcal{O}_{\mathcal{K}}$. The converse is discussed in Section 4.3.

Proposition 4.2.1. Let us suppose we have a binary integral positive definite quadratic form $q(x, y) = ax^2 + bxy + cy^2$ with discriminant $d_{\mathcal{K}} < 0$. Then we have $\dfrac{-b + \sqrt{d_{\mathcal{K}}}}{2} \in \mathcal{O}_{\mathcal{K}}$.

Proof. Our first observation is that $d_{\mathcal{K}} = b^2 - 4ac \equiv b^2 \pmod 4$. Consequently, if $d_{\mathcal{K}}$ is odd, then $d_{\mathcal{K}} \equiv 1 \pmod 4$ and b is also odd. In this case, we have $\dfrac{-b + \sqrt{d_{\mathcal{K}}}}{2} = -\dfrac{b+1}{2} + \dfrac{1 + \sqrt{d_{\mathcal{K}}}}{2} \in \mathcal{O}_{\mathcal{K}}$.

On the other hand, if $d_{\mathcal{K}}$ is even, then it is also divisible by 4 and b is also even. Thus, $\dfrac{-b + \sqrt{d_{\mathcal{K}}}}{2} = \dfrac{-b}{2} + \dfrac{\sqrt{d_{\mathcal{K}}}}{2} \in \mathbb{Z}[\sqrt{d_{\mathcal{K}}}] = \mathcal{O}_{\mathcal{K}}$ □

As a next step, we will show that a certain set of numbers defined by the quadratic form q indeed forms an ideal of $\mathcal{O}_{\mathcal{K}}$.

Lemma 4.2.2.

$$I_q = a \cdot \mathbb{Z} + \frac{-b + \sqrt{d_{\mathcal{K}}}}{2} \cdot \mathbb{Z} \lhd \mathcal{O}_{\mathcal{K}}$$

Proof. The sum and difference of elements of I_q are clearly also in I_q. Also, if we multiply an element of I_q with an integer, it stays in I_q. The only interesting part is to show that multiplication by other elements of $\mathcal{O}_\mathcal{K}$ also do not lead out of I_q.

Let us introduce the notation $\tau = \dfrac{-b+\sqrt{d_\mathcal{K}}}{2a}$ which is one of the roots of the polynomial ax^2+bx+c. Now $I_q = a(\mathbb{Z}+\tau\cdot\mathbb{Z})$ so it is sufficient to prove that $\mathbb{Z}+\tau\cdot\mathbb{Z}$ is closed to multiplication by elements of $\mathcal{O}_\mathcal{K}$ since we have seen that I_q is a subset of $O_\mathcal{K}$.

Our next observation is that it would suffice to show that $\mathcal{O}_\mathcal{K} = \mathbb{Z}+a\tau\cdot\mathbb{Z}$, since $(\mathbb{Z}+\tau\cdot\mathbb{Z})(\mathbb{Z}+a\tau\cdot\mathbb{Z}) \subseteq \mathbb{Z}+\tau\cdot\mathbb{Z}+a\tau^2\cdot\mathbb{Z}$ where we can calculate $a\tau^2 = \frac{b^2+d_\mathcal{K}-2b\sqrt{d_\mathcal{K}}}{4a} = \frac{2b^2-4ac-2b\sqrt{d_\mathcal{K}}}{4a} = -c-b\frac{-b+\sqrt{d_\mathcal{K}}}{2a} = -c-b\tau \in \mathbb{Z}+\tau\cdot\mathbb{Z}$.

We know that $\mathcal{O}_\mathcal{K}$ can either be equal to $\mathbb{Z}+\dfrac{\sqrt{d_\mathcal{K}}}{2}\cdot\mathbb{Z}$ or $\mathbb{Z}+\dfrac{1+\sqrt{d_\mathcal{K}}}{2}\cdot\mathbb{Z}$, but since we have $b\equiv d_\mathcal{K} \pmod 4$, it indeed follows that $\mathcal{O}_\mathcal{K} = \mathbb{Z}+\dfrac{-b+\sqrt{d_\mathcal{K}}}{2}\cdot\mathbb{Z}$ and the proof is finished. □

So far we have constructed function which assigns an ideal to each quadratic form. A natural question arising here is if we could also construct the inverse of this function. This is what we are going to study from now on.

4.3 Assigning quadratic forms to ideals

Suppose we have an ideal $I \lhd \mathcal{O}_\mathcal{K}$. We would like to somehow define a quadratic form only depending on I, but we need some preparation for that.

Definition 4.3.1. The norm of an ideal, denoted by $N(I)$ is defined to be $|O_\mathcal{K} : I|$.

Proposition 4.3.2. If $I = \alpha\cdot\mathcal{O}_\mathcal{K}$ is a principal ideal, then $N(I) = N(\alpha)$.

Proof. $\mathcal{O}_\mathcal{K}$ can be naturally identified with $\mathbb{Z}^2$ as an Abelian group.

If $\alpha\in\mathbb{Z}$, then $\alpha\cdot\mathcal{O}_\mathcal{K} \cong (\alpha\cdot\mathbb{Z})^2$ and its index is $\alpha^2 = N(\alpha)$.

If $\alpha\notin\mathbb{Z}$, then let S_α denote the multiplication by α, which is an Abelian group homomorphism. Let $\alpha = a + b\dfrac{d_\mathcal{K}+\sqrt{d_\mathcal{K}}}{2}$ where $a,b\in\mathbb{Z}$. We calculate the value of α^2 and write it up as a $\mathbb{Z}$-linear combination of 1 and α:

$$\alpha^2 = a^2 + 2ab\frac{d_\mathcal{K}+\sqrt{d_\mathcal{K}}}{2} + b^2\Big(\frac{d_\mathcal{K}+\sqrt{d_\mathcal{K}}}{2}\Big)^2 =$$

$$= a^2 - \frac{b^2 d_\mathcal{K}(d_\mathcal{K}-1)}{4} + (b^2 d_\mathcal{K} + 2ab)\frac{d_\mathcal{K}+\sqrt{d_\mathcal{K}}}{2} =$$

$$= -d_{\mathcal{K}}ab - a^2 - \frac{b^2 d_{\mathcal{K}}(d_{\mathcal{K}}-1)}{4} + (d_{\mathcal{K}} + 2a)\alpha$$

Both coefficients are integers as either $d_{\mathcal{K}}$ or $d_{\mathcal{K}} - 1$ is divisible by four because $d_{\mathcal{K}}$ is a fundamental discriminant. Now, let us write up the matrix of S_α in the basis $(1, \alpha)$:

$$\begin{pmatrix} 0 & -d_{\mathcal{K}}ab - a^2 - \dfrac{b^2 d_{\mathcal{K}}(d_{\mathcal{K}}-1)}{4} \\ 1 & (d_{\mathcal{K}} + 2a) \end{pmatrix}$$

The index $|\mathcal{O}_{\mathcal{K}} : I|$ is equal to the absolute value of the determinant of the matrix above, which is quite easy to compute: $d_{\mathcal{K}}ab + a^2 + \dfrac{b^2 d_{\mathcal{K}}(d_{\mathcal{K}}-1)}{4}$.

Our claim is equivalent to this value being equal to $N(\alpha)$ so we have to verify this by another computation:

$$N(\alpha) = \alpha\bar{\alpha} = \left(a + b\frac{d_{\mathcal{K}} + \sqrt{d_{\mathcal{K}}}}{2}\right)\left(a + b\frac{d_{\mathcal{K}} - \sqrt{d_{\mathcal{K}}}}{2}\right) =$$

$$= a^2 + abd_{\mathcal{K}} + \frac{b^2 d_{\mathcal{K}}^2}{4} - \frac{b^2 d_{\mathcal{K}}}{4} = d_{\mathcal{K}}ab + a^2 + \frac{b^2 d_{\mathcal{K}}(d_{\mathcal{K}}-1)}{4}$$

□

The next statement concerning the norm of elements included in a certain ideal follows from Proposition 4.3.2 and will have important consequences later.

Proposition 4.3.3. If $\alpha \in I \lhd \mathcal{O}_{\mathcal{K}}$, then we have $N(I)|N(\alpha)$.

Proof. Let I_α denote the principal ideal generated by α, which is $\alpha \cdot \mathcal{O}_{\mathcal{K}}$. We have $I_\alpha \subseteq I$ because $\alpha \in I$. Since I is a ring itself, also $I_\alpha \lhd I$ follows, from which we obtain $N(\alpha) = N(I_\alpha) = |\mathcal{O}_{\mathcal{K}} : I_\alpha| = |\mathcal{O}_{\mathcal{K}} : I| \cdot |I : I_\alpha| = N(I) \cdot |I : I_\alpha|$. Since $|I : I_\alpha|$ is an integer, the proof is finished. □

In the next definition we describe the binary quadratic form corresponding to the ideal I.

Definition 4.3.4. Suppose $I \lhd \mathcal{O}_{\mathcal{K}}$ and $I = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$ for some $\alpha, \beta \in \mathcal{O}_{\mathcal{K}}$. We define the *quadratic form of ideal I* as

$$f_I(x, y) = \frac{N(\alpha \cdot x - \beta \cdot y)}{N(I)}$$

Here we have a free choice because the ideals $\alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$ and $\beta \cdot \mathbb{Z} + \alpha \cdot \mathbb{Z}$ are the same but the quadratic forms assigned to them are not neccessarily equal formally, so we have to make an assumption to make this function well-defined. The assumption we make is that $\frac{\beta}{\alpha}$ is in the upper half plane, which is denoted by $\mathbb{H}$ (the complex numbers with positive imaginary part). This means that if we have an ideal where this ratio would have a negative imaginary part, we swap the order of the two numbers, making the ratio and element of $\mathbb{H}$. This way, the quadratic form assigned to the ideal is well-defined in every case.

Proposition 4.3.5. For $I = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z} \lhd \mathcal{O}_{\mathcal{K}}$ we have $N(I)^2 = \frac{(\alpha \cdot \bar{\beta} - \bar{\alpha} \cdot \beta)^2}{d_{\mathcal{K}}}$.

Proof. We know that $N(I) = |\mathcal{O}_{\mathcal{K}} : I|$, which is the ratio of the areas of the paralelogram spanned by α and β and the base paralelogram of the grid $\mathcal{O}_{\mathcal{K}}$. Since $\mathcal{O}_{\mathcal{K}}$ is either equal to $\mathbb{Z} + \frac{\sqrt{d_{\mathcal{K}}}}{2} \cdot \mathbb{Z}$ or $\mathbb{Z} + \frac{1+\sqrt{d_{\mathcal{K}}}}{2} \cdot \mathbb{Z}$, the square of the area of the base paralelogram of $\mathcal{O}_{\mathcal{K}}$ is $\frac{-d_{\mathcal{K}}}{4}$ (which is a positive number). The square of the area of the paralelogram spanned by α and β is $(\alpha \times \beta)^2 = \frac{-(\alpha \cdot \bar{\beta} - \bar{\alpha} \cdot \beta)^2}{4}$. As a conclusion, we get $N(I)^2 = \frac{(\alpha \cdot \bar{\beta} - \bar{\alpha} \cdot \beta)^2}{d_{\mathcal{K}}}$ as desired. □

We would like to show that f_I has some properties we could naturally expect.

Proposition 4.3.6. f_I is a positive definite quadratic form with discriminant $d_{\mathcal{K}}$.

Before proving Proposition 4.3.6, let us show an example together with Figure 4.1 to make it easier to understand and visualise the proof and the concepts we are examining.

Suppose we have $d = -5$, consequently $\mathcal{K} = \mathbb{Q}(i\sqrt{5})$, $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[i\sqrt{5}]$ and $d_{\mathcal{K}} = -20$. Stating otherwise $\mathcal{O}_{\mathcal{K}}$ is $\mathbb{Z} + i\sqrt{5} \cdot \mathbb{Z}$. This is the black dotted rectangular grid in Figure 4.1. The square of the area of the base paralelogram (in this case, rectangle) of $\mathcal{O}_{\mathcal{K}}$ is $(1 \cdot \sqrt{5})^2 = 5 = \frac{-d_{\mathcal{K}}}{4}$ as shown by Proposition 4.3.5.

Let us examine the ideal spanned by $\alpha = 4 + i\sqrt{5}$ and $\beta = 1 + 2i\sqrt{5}$, $I = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$. The square of the area of the base paralelogram of ideal I is $(4 \cdot 1.75\sqrt{5})^2 = 245$. The square of the norm of I is 49, so we have $N(I) = 7$. The ideal is shown on Figure 4.1 in red with the two generating elements α and β highlighted in blue.

Now let us compute f_I for this specific ideal. We need to divide $N(\alpha \cdot x - \beta \cdot y)$ by 7. $N(\alpha \cdot x - \beta \cdot y) = (\alpha \cdot x - \beta \cdot y)\overline{(\alpha \cdot x - \beta \cdot y)} = \Big((4 + i\sqrt{5}) \cdot x - (1 + 2i\sqrt{5}) \cdot y\Big)\Big((4 - i\sqrt{5}) \cdot x - (1 - 2i\sqrt{5}) \cdot y\Big) = 21x^2 - 28xy + 21y^2$. So we have $f_I(x, y) = 3x^2 - 4xy + 3y^2$ whose discriminant is indeed $16 - 4 \cdot 3 \cdot 3 = -20 = d_{\mathcal{K}}$ and we also see that f_I is really positive definite in this case.

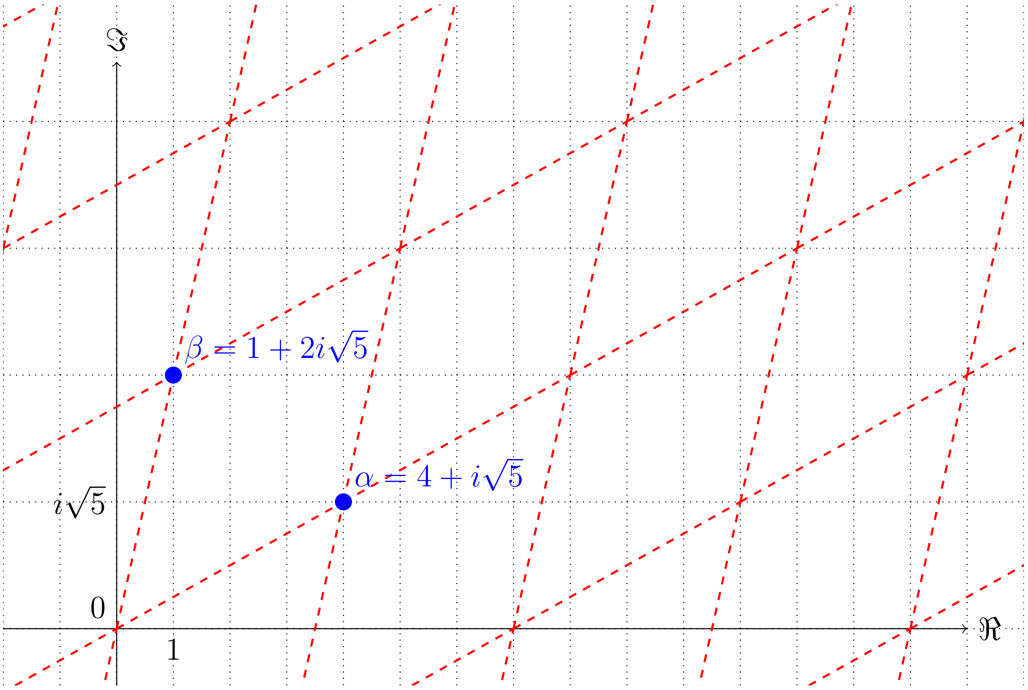

Figure 4.1: An ideal generated by two elements of $\mathcal{O}_{\mathcal{K}}$ for $d = -5$

One can also check which ideal will be assigned to this quadratic form f_I by the function defined in Section 4.2. Let $J = I_{f_I}$ denote this ideal defined in Lemma 4.2.2 as $J = 3 \cdot \mathbb{Z} + \dfrac{4 + \sqrt{-20}}{2} \cdot \mathbb{Z} = 3 \cdot \mathbb{Z} + (2 + i\sqrt{5}) \cdot \mathbb{Z}$. This is not exactly I, but we can compute that $I = J \cdot \dfrac{4 + i\sqrt{5}}{3}$ holds in this case. So we obtain $I_{f_I} = c \cdot I$ for some $c \in \mathbb{C}$. Now we see a reason to identify ideals which can be multiplied into each other and we will formalise exactly this property in Definition 4.3.7.

After this brief side track of looking at an example, we continue by prooving our Proposition 4.3.6.

Proof of Proposition 4.3.6. By Proposition 4.3.3, we know that $N(I)|N(\alpha \cdot x - \beta \cdot y)$ holds for all $x, y \in \mathbb{Z}$ since $\alpha \cdot x - \beta \cdot y$ is an element in ideal I. Let us evaluate $N(\alpha \cdot x - \beta \cdot y)$:

$$N(\alpha \cdot x - \beta \cdot y) = (\alpha \cdot x - \beta \cdot y)(\bar{\alpha} \cdot x - \bar{\beta} \cdot y) = N(\alpha)x^2 + N(\beta)y^2 - Tr(\alpha \cdot \bar{\beta})xy$$

Substituting $x = 1, y = 0$ gives $N(I)|N(\alpha)$, $x = 0, y = 1$ gives $N(I)|N(\beta)$. If we substitute $x = y = 1$ into the equation, we get $N(I)|N(\alpha) + N(\beta) - Tr(\alpha \cdot \bar{\beta})$, which yields $N(I)|Tr(\alpha \cdot \bar{\beta})$ when combined with the previous two divisibilities. So all the coefficients of the $\dfrac{N(\alpha \cdot x - \beta \cdot y)}{N(I)} \in \mathbb{R}[x, y]$ are indeed integers, so we conclude that $f_I(x, y) \in \mathbb{Z}[x, y]$, the quadratic form is integral.

We need to calculate the discriminant of f_I using the identity proved in Proposition 4.3.5:

$$d_{f_I} = b^2 - 4ac = \frac{Tr(\alpha \cdot \bar{\beta})^2 - 4N(\alpha)N(\beta)}{N(I)^2} =$$

$$= \frac{(\alpha \cdot \bar{\beta} + \bar{\alpha} \cdot \beta)^2 - 4\alpha \cdot \bar{\alpha} \cdot \beta \cdot \bar{\beta}}{N(I)^2} = \frac{(\alpha \cdot \bar{\beta} - \bar{\alpha} \cdot \beta)^2}{N(I)^2} = d_{\mathcal{K}}$$

The form f_I is also positive definite because $f_I(1,0) > 0$ and the discriminant is negative. □

We now define an equivalence relation of the non-zero ideal of $\mathcal{O}_{\mathcal{K}}$ which is motivated by example worked through above:

Definition 4.3.7. Suppose $0 \neq I, J \lhd \mathcal{O}_{\mathcal{K}}$. We say I is equivalent to J, denoted by $I \sim J$ if there is a non-zero c element in $\mathcal{K}$ for which $c \cdot I = J$.

Proposition 4.3.8. The relation defined above is indeed an equivalence relation.

Proof. Reflexivity if clear with the choice of $c = 1 \in \mathcal{K}$. For symmetry, we need to take the inverse element of c which is also in $\mathcal{K}$ since it is a field. As for transitivity we need to multiply two elements, which again does not lead out of $\mathcal{K}$ and we are done. □

Once we know that this is an equivalence relation, it would be natural to consider the equivalence classes of ideals up to this relation. This is also motivated by the example worked through above showing that it can happen that $I_{f_I} \neq I$, but $I_{f_I} \sim I$ holds.

Definition 4.3.9. The *class group* of $\mathcal{K}$ is defined to be $C_{\mathcal{K}} = {}^{\{I \lhd \mathcal{O}_{\mathcal{K}} \,:\, I \neq 0\}}\big/_{\sim}$, the set of the non-zero ideals of $\mathcal{O}_{\mathcal{K}}$ factorised by the equivalence relation defined above.

We would also like to show that this set called the class group also has a group structure. To prepare this, we define the multiplication of ideals and show some basic properties.

Definition 4.3.10. If we have $I, J \lhd \mathcal{O}_{\mathcal{K}}$, then their product is

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k : n \in \mathbb{N}, i_k \in I, j_k \in J \right\}$$

As we are preparing to show that $C_{\mathcal{K}}$ is a group, we want to prove that this multiplication is well-defined on the elements of $C_{\mathcal{K}}$, i.e. the equivalence classes of ideals.

Proposition 4.3.11. If we have $I \sim I'$ and $J \sim J'$, then $IJ \sim I'J'$ holds.

Proof. By the definition of equivalence (4.3.7), we have $I = c_1 \cdot I'$ and $J = c_2 \cdot J'$ for some $c_1, c_2 \in \mathcal{O}_{\mathcal{K}}$. For each choice of $n \in \mathbb{N}, i_k \in I', j_k \in J'$ in $I'J'$, we can choose $n \in \mathbb{N}, c_1 i_k \in I, c_2 j_k \in J$ which will form an element of IJ with $c_1c_2 \cdot I'J' \ni c_1c_2 \cdot \sum_{k=1}^{n} i_k j_k = \sum_{k=1}^{n}(c_1 i_k)(c_2 j_k) \in IJ$. So we have $IJ \sim I'J'$. □

Proposition 4.3.12. For an ideal $0 \neq I \lhd \mathcal{O}_{\mathcal{K}}$ we have: $I \sim \mathcal{O}_{\mathcal{K}} \iff I$ is principal.

Proof. $\Rightarrow$: From $I \sim \mathcal{O}_{\mathcal{K}}$ we have $I = c \cdot \mathcal{O}_{\mathcal{K}}$ for some $c \in \mathcal{O}_{\mathcal{K}}$ by Definiton 4.3.7. So we have $I = \{c \cdot \alpha : \alpha \in \mathcal{O}_{\mathcal{K}}\} = \langle c \rangle$, as a consequence, I is principal.

$\Leftarrow$: We now have $I = \langle c \rangle$ for some $c \in \mathcal{O}_{\mathcal{K}}$, consequently, $I = c \cdot \mathcal{O}_{\mathcal{K}}$. □

We define the conjugate of an ideal as it will be needed to invert elements in group $C_{\mathcal{K}}$:

Definition 4.3.13. For any $I \lhd \mathcal{O}_{\mathcal{K}}$, let us define its conjugate $\bar{I} = \{\bar{\alpha} : \alpha \in I\}$.

Proposition 4.3.14. For any $0 \neq I \lhd \mathcal{O}_{\mathcal{K}}$, $I\bar{I} = N(I) \cdot \mathcal{O}_{\mathcal{K}}$ is a principal ideal.

Proof. Suppose we have $\alpha, \beta \in I$. We observe that $N(I)|N(\alpha) = \alpha \cdot \bar{\alpha}$ and $N(I)|N(\beta) = \beta \cdot \bar{\beta}$. Since $\alpha + \beta \in I$ also holds, we deduce $N(I)|N(\alpha+\beta) = N(\alpha) + N(\beta) + \alpha \cdot \bar{\beta} + \bar{\alpha} \cdot \beta = N(\alpha) + N(\beta) + Tr(\alpha \cdot \bar{\beta})$. Consequently, both the trace and the norm of $\dfrac{\alpha \cdot \bar{\beta}}{N(I)}$ are integers since they are $\dfrac{Tr(\alpha \cdot \bar{\beta})}{N(I)}$ and $\dfrac{N(\alpha)N(\beta)}{N(I)^2}$, respecively. If we consider the polynomial $x^2 - Tr\left(\dfrac{\alpha \cdot \bar{\beta}}{N(I)}\right) \cdot x + N\left(\dfrac{\alpha \cdot \bar{\beta}}{N(I)}\right)$, we see immediately that its coefficients are integers with the leading coefficient being one, so its roots are elements of $\mathcal{O}_{\mathcal{K}}$. But $\dfrac{\alpha \cdot \bar{\beta}}{N(I)}$ is a root itself as the polinomial was exactly constructed that way. We conclude that $\alpha \cdot \bar{\beta} \in N(I) \cdot \mathcal{O}_{\mathcal{K}}$, i.e. $I\bar{I} \subseteq N(I) \cdot \mathcal{O}_{\mathcal{K}}$.

Conversely, we need to show that $N(I)$ itself is an element of $I\bar{I}$. For all $\alpha \in I$, we have $N(\alpha) = \alpha \cdot \bar{\alpha} \in I\bar{I}$. And since $I\bar{I}$ is an ideal, it is specifically a subgroup for addition, so a $\mathbb{Z}$-linear combination of elements in I is also in $I\bar{I}$. Now we investigate the coefficients of the quadratic form assigned to I: $f_I(x, y) = \dfrac{N(x \cdot \alpha - y \cdot \beta)}{N(I)} =: ax^2 + bxy + cy^2$. Here we can calculate the coefficients: $a = \dfrac{N(\alpha)}{N(I)}$, $c = \dfrac{N(\beta)}{N(I)}$ and $b = \dfrac{N(\alpha+\beta) - N(\alpha) - N(\beta)}{N(I)}$. The discriminant of f_I has been shown to be $d_{\mathcal{K}}$ which is a square-free integer. $(a, b, c)^2 | b^2 - 4ac = d_{\mathcal{K}}$, so we conclude that $(a, b, c) = 1$, i.e. the three coefficients are relatively prime. If the coefficients are relatively prime together, it means that $N(I)$ is expressable as a $\mathbb{Z}$-linear combination of $N(\alpha)$, $N(\beta)$ and $N(\alpha + \beta)$, all of which are elements of $I\bar{I}$, hence $N(I) \in I\bar{I}$. □

After this showing some important properties of the ideal class group and principal ideals, we are prepared to prove that $C_{\mathcal{K}}$ is really a group.

Lemma 4.3.15. *$C_{\mathcal{K}}$ is an Abelian group for the multiplication of ideals.*

Proof. We have shown earlier that multiplication is well-defined. Associativity and commutativity follows from the associativity and commutativity of the usual multiplication and addition of numbers.

For an ideal I, its inverse is defined to be $\bar{I}$. We have seen in Proposition 4.3.14 that $I\bar{I}$ is principal and in Propostion 4.3.12 that principal ideals are equivalent to $\mathcal{O}_{\mathcal{K}}$. The class corresponding to $\mathcal{O}_{\mathcal{K}}$ (and all the other principal ideals) will be the identity element of the group. □

Note that the proof presented above holds for all Dedekind domains. A different proof of Lemma 4.3.15 and the previous statements can be found in [4]. This proof is due to Hurwitz and is specific to the number field case.

We have arrived to the most important point of this thesis, where we will prove that the two maps defined earlier are inverses of each other. This specifically shows that $C_{\mathcal{K}}$ is always a finite group since we know that $h(D) < \infty$ for all $D < 0$ by Theorem 3.2.16.

Theorem 4.3.16. *Let $d < 0$ be a square-free integer, $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ and $d_{\mathcal{K}}$ be the fundamental discriminant assigned to d (see Definition 3.2.17). The two functions $I \mapsto f_I$ and $f \mapsto I_f$ are inverses of each other. They are both bijections between $C_{\mathcal{K}}$ and the proper equivalence classes of quadratic forms with discriminant $d_{\mathcal{K}}$.*

Proof. Firstly we need to check that the function $I \mapsto f_I$ is also well-defined as a function from $C_{\mathcal{K}}$ to the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms. Equivalently, we need to verify that $I \sim J \implies f_I \sim_{\mathrm{SL}_2(\mathbb{Z})} f_J$. From $I \sim J$, $J = c \cdot I$ follows for some $c \in \mathcal{O}_{\mathcal{K}}$. Suppose that $I = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$, so we obtain $f_I(x, y) = {}^{N(\alpha \cdot x - \beta \cdot y)}/_{N(I)}$. The generating elements of J can be chosen to be $c \cdot \alpha$ and $c \cdot \beta$, so we can compute $f_J(x, y) = {}^{N(c \cdot \alpha \cdot x - c \cdot \beta \cdot y)}/_{N(c \cdot I)} = {}^{c^2 N(\alpha \cdot x - \beta \cdot y)}/_{c^2 N(I)} = {}^{N(\alpha \cdot x - \beta \cdot y)}/_{N(I)} = f_I(x, y)$.

On the other hand, we also need to verify that $f \sim_{\mathrm{SL}_2(\mathbb{Z})} g \implies I_f \sim I_g$. We assume that $f(x, y) = ax^2 + bxy + cy^2$, $g(x, y) = a_1x^2 + b_1xy + c_1y^2$ and the witness of their proper equivalence is $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ for which $f(x, y) = g(px + qy, rx + sy)$ holds. Let $\tau_f \in \mathbb{H}$ be one of the roots of the univariate polynomial $f(x, 1)$. Since $f(x, 1)$ has real coefficients, its two roots are conjugates of each other, so one of them is inside $\mathbb{H}$. Solving the equation we obtain $\tau_f = \dfrac{-b+\sqrt{d_{\mathcal{K}}}}{2a}$. Since we know that $I_f = a \cdot (\mathbb{Z} + \tau_f \cdot \mathbb{Z})$ we deduce that $\tau_f = {}^{\beta}\!/_{\alpha}$ using the usual notation $I_f = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$ (where ${}^{\beta}\!/_{\alpha} \in \mathbb{H}$). Now let us benefit from the $\mathrm{SL}_2(\mathbb{Z})$-equivalence of f and g:

$$0 = f(\tau_f, 1) = g(p \cdot \tau_f + q, r \cdot \tau_f + s) = (r \cdot \tau_f + s)^2 \cdot g\Big(\frac{p \cdot \tau_f + q}{r \cdot \tau_f + s}, 1\Big)$$

We are interested in what τ_g is, the solution of $0 = g(x,1)$ in $\mathbb{H}$. Based on the calculation above, it can either be $\dfrac{p \cdot \tau_f + q}{r \cdot \tau_f + s}$ or $\dfrac{p \cdot \bar{\tau_f} + q}{r \cdot \bar{\tau_f} + s}$, whichever is in $\mathbb{H}$. With the help of Theorem 2.1.2, we can decide that since $\dfrac{p \cdot \tau_f + q}{r \cdot \tau_f + s}$ is exactly $\gamma(\tau_f)$ by the group action defined there, so we deduce $\dfrac{p \cdot \tau_f + q}{r \cdot \tau_f + s} \in \mathbb{H}$, consequently, $\tau_g = \dfrac{p \cdot \tau_f + q}{r \cdot \tau_f + s}$. We want to show that $I_f = a \cdot (\mathbb{Z} + \tau_f \cdot \mathbb{Z})$ and $I_g = a_1 \cdot (\mathbb{Z} + \tau_g \cdot \mathbb{Z})$ are equivalent to each other. Since equivalence means same up to constant factor, it is enough to show the equivalence of $\mathbb{Z} + \tau_f \cdot \mathbb{Z}$ and $\mathbb{Z} + \tau_g \cdot \mathbb{Z}$:

$$\mathbb{Z} + \tau_g \cdot \mathbb{Z} = \mathbb{Z} + \frac{p \cdot \tau_f + q}{r \cdot \tau_f + s} \cdot \mathbb{Z} \sim (r \cdot \tau_f + s) \cdot \mathbb{Z} + (p \cdot \tau_f + q) \cdot \mathbb{Z}$$

Since $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ represents an orthogonal transformation in the vector field $\mathbb{R}^2$, the grid spanned by $\begin{pmatrix} \tau \\ 1 \end{pmatrix}$ is equivalent to the grid spanned by $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} p \cdot \tau + q \\ r \cdot \tau + s \end{pmatrix}$, which shows $I_f \sim I_g$.

So far we have shown that both functions are well-defined on the sets of $C_{\mathcal{K}}$ and the equivalence classes of quadratic forms, respectively. It remains to prove that these functions are really bijections and are the inverses of each other.

Suppose we have a quadratic form of discriminant $d_{\mathcal{K}}$ $f(x,y) = ax^2 + bxy + cy^2$. Then $I_f = a \cdot (\mathbb{Z} + \tau_f \cdot \mathbb{Z})$ holds as computed above. Let us evaluate f_{I_f} with the help of the identity $\tau_f = \dfrac{-b+\sqrt{d_{\mathcal{K}}}}{2a}$:

$$f_{I_f}(x,y) = \frac{N(a \cdot x - a\tau_f \cdot y)}{N(I_f)} = \frac{a^2(x - \frac{-b+\sqrt{d_{\mathcal{K}}}}{2a}y)(x - \frac{-b-\sqrt{d_{\mathcal{K}}}}{2a}y)}{N(I_f)} =$$

$$= \frac{a^2x^2 + abxy + \frac{b^2-d_{\mathcal{K}}}{4}y^2}{N(I_f)} = \frac{a(ax^2 + bxy + cy^2)}{N(I_f)} = \frac{a}{N(I_f)} f(x,y)$$

It remains to show that $a = N(I_f)$ holds. This is verified by the fact that the base paralelogram of the grid $I_f = a \cdot \mathbb{Z} + \frac{-b+\sqrt{d_{\mathcal{K}}}}{2} \cdot \mathbb{Z}$ has base a and height of $\frac{\sqrt{d_{\mathcal{K}}}}{2}$, i.e. the base length is a times the base length of grid $\mathcal{O}_{\mathcal{K}}$ with the height being the same, showing $N(I_f) = |\mathcal{O}_{\mathcal{K}} : I_f| = a$.

As a next step, suppose that $I = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$ is given with $\tau = {}^{\beta}\!/\!_{\alpha}$ being one of the roots of $f_I(x, 1)$. Now evaluate what this polynomial is: $f_I(x, 1) = \frac{N(\alpha \cdot x - \beta)}{N(I)}$. We see that τ is really a root: $N({}^{\beta}\!/\!_{\alpha} \cdot \alpha - \beta) = N(0) = 0$. Now $I_{f_I} = a(\mathbb{Z} + \tau \cdot \mathbb{Z}) = \frac{a}{\alpha}(\alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}) = \frac{a}{\alpha} \cdot I \sim I$, hence I_{f_I} and I are equivalent.

From the two functions being inverses of one another it follows that both of them are also bijections. We have showed every statement of the theorem, so the proof is complete. □

After proving the main theorem of the thesis, there are several questions arising. What is the use of this theorem apart from its beauty? Why are we only working with negative discriminants? What would break if we observed positive discriminants and how can it be fixed? In the final Section 4.4 we tackle some of these questions to some extent and prospose some good literature for those interested.

4.4 Conclusions

One immediate application of Theorem 4.3.16 within algebraic number theory is the classification of quadratic fields whose number rings are principal ideal domains. We have seen previously that the ideals equivalent to $\mathcal{O}_{\mathcal{K}}$ itself are exactly the principal ideals. Thus, $\mathcal{O}_{\mathcal{K}}$ is a PID if and only if $h(d_{\mathcal{K}}) = 1$. We have a classification for these numbers due to Baker, Stark and Heegner from the second half of the 20^{th} century:

Theorem 4.4.1 (Baker, Stark, Heegner). *Suppose D is a negative integer with $D \equiv 0, 1$ mod 4. Then*

$$h(D) = 1 \iff D \in \{-4, -8, -12, -16, -28, -3, -7, -11, -19, -27, -43, -67, -163\}$$

As a consequence, we have a finite list of negative disciminants D for which the Fundamental Theorem of Number Theory holds in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Concerning positive discriminants, things get harder right away as it can happen that two reduced binary quadratic forms are properly equivalent to each other. Even though both sets are finite, the correspondence between equivalence classes of binary quadratic forms and ideal classes also has to be slightly modified. In case $D > 0$

is a fundamental discriminant, one obtains a bijection with the so called *narrow class group* which is potentially twice as big as the ideal class group. As opposed to the above theorem, it is an open problem whether there are infinitely many $D > 0$ with $h(D) = 1$. A good reference to learn about the case of positive discriminants is Chapter VII.2. of the book of Fröhlich and Taylor. [3].

Bibliography

[1] David A Cox. *Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions*, volume 387. American Mathematical Soc., 2022.

[2] Kiss Emil. *Bevezetés az algebrába.* Typotex Kft, 2007.

[3] Albrecht Fröhlich and Martin J Taylor. *Algebraic number theory.* Number 27. Cambridge University Press, 1991.

[4] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.

[5] Péter Maga. Introduction to number theory. `https://users.renyi.hu/~magap/classes/bsm/18_summer_number_theory/introduction_to_number_theory.pdf`, 2019.

[6] Daniel A Marcus and Emanuele Sacco. *Number fields*, volume 1995. Springer, 1977.

NYILATKOZAT

Név: VÁRKONYI ZSOMBOR

ELTE Természettudományi Kar, szak: MATEMATIKA BSC

NEPTUN azonosító: J70VMX

Szakdolgozat címe: BINARY QUADRATIC FORMS AND QUADRATIC NUMBER FIELDS

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2024. 05. 29.

a hallgató aláírása