University of Groningen

Bachelor's Project Mathematics

Computing class numbers of orders in imaginary quadratic fields

July 12, 2019

Author:
Floor Dogger

First supervisor:
Pınar Kılıçer

Second assessor:
Jaap Top

Abstract

The connection between binary quadratic forms and imaginary quadratic number fields is studied with the aim of computing class numbers of orders in imaginary quadratic fields. The form class group is constructed and we define the Dirichlet composition of two primitive positive definite forms of the same discriminant. We prove in detail that the operation induced by Dirichlet composition is well-defined and provides an Abelian structure on the form class group. Algorithms to compute the class number of the form class group are implemented in Sage. The construction of the ideal class group is discussed next. We prove that every form class group is isomorphic to an ideal class group of a unique order in an imaginary quadratic field. The implemented algorithms are used to compute class numbers of orders in imaginary quadratic fields. We finish with computing class numbers of the ring of integers in imaginary quadratic fields to check whether they are unique factorization domains.

Contents

1 Introduction

1.1 History

One of the first problems related to quadratic forms is finding integers that can be the value of a certain quadratic form over the integers. An example is finding Pythagorean triples, which was already studied before the era. Another example is finding integer solutions of equations of the form $x^2 - ny^2 = 1$, where n is a given positive nonsquare integer, called Pell's equations. This problem was studied by the Indian mathematician Brahmagupta (598-668). In the previous century, Fermat (1607-1665) worked on similar problems resulting in for example his theorem on sums of two squares. A general theory of binary quadratic forms appeared in the book Disquisitiones Arithmeticae (1801) by Gauss (1777-1855). He developed an equivalence relation on the set of binary quadratic forms that share their discriminant and proved that some sets of equivalence classes form an Abelian group. We will study the link between binary quadratic forms and imaginary quadratic fields that is due to Kummer (1810-1893), Kronecker (1823-1891) and Dedekind (1831-1916).

1.2 Outline

The aim of the thesis is to understand the connection between binary quadratic forms and imaginary quadratic number fields. We will first study integral binary quadratic forms, which are of the form

$$ax^2 + bxy + cy^2, \text{ where } a, b, c \in \mathbb{Z}.$$

For simplicity, we will often write "quadratic form" or just "form" to refer to an integral binary quadratic form. The *discriminant* of a quadratic form with notation as above is defined to be

$$D = b^2 - 4ac.$$

A quadratic form is called *primitive* if its coefficients are relatively prime and *positive definite* if it represents only positive integers. Two quadratic forms f and g are equivalent if there exist integers p, q, r and s such that

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

We call f and g *properly equivalent* if $ps - qr = 1$. Both equivalence and proper equivalence are equivalence relations, as is described in [11, Remark 1.22]. Proper equivalent forms have the same discriminant and a form properly equivalent to a primitive positive definite form is itself a primitive positive definite form, see [11, Proposition 1.16, Corollary 1.19, Corollary 1.20]. The set of equivalence classes of primitive positive definite forms of discriminant D with respect to proper equivalence forms a group $C(D)$, called

the form class group, see [7, Theorem 3.9]. The form class group will play an important role in the computation of the class number of orders in imaginary quadratic fields.

In section 3, we will construct the ideal class group of orders in quadratic fields, which are degree two extensions of the rational numbers. A complex number is called an *algebraic integer* if it is a root of a monic polynomial with integer coefficients. The algebraic integers in a quadratic field form a ring called the *ring of integers*, see [9, Corollary 1]. The ring of integers in a quadratic field K is an example of an *order*, which is a subring of K containing 1 and moreover a free $\mathbb{Z}$-module of rank two.

The construction of the ideal class group is based on fractional ideals. A *fractional ideal* of an order $\mathcal{O}$ in a quadratic field K is a subset of K which is a nonzero finitely generated $\mathcal{O}$-module and has the form αI, where $\alpha \in K^\times$ and I is a nonzero ideal of $\mathcal{O}$, see [6, Theorem 2.3]. A fractional ideal J of $\mathcal{O}$ is called *proper* if $\mathcal{O} = \{\beta \in K : \beta J \subset J\}$. The set of proper fractional ideals of an order forms an Abelian group under multiplication and is denoted by $I(\mathcal{O})$, see [7, §7A]. The set of principal fractional $\mathcal{O}$-ideals, which are of the form $\alpha\mathcal{O}$ with $\alpha \in K^\times$, forms a subgroup $P(\mathcal{O}) \subset I(\mathcal{O})$, as is stated in [7, §7A]. We can therefore form the quotient

$$C(\mathcal{O}) \coloneqq I(\mathcal{O})/P(\mathcal{O}),$$

which is called the *ideal class group* of the order $\mathcal{O}$. This group is finite, which follows from [7, Theorem 7.7 (ii), Theorem 2.13].

The last section discusses the relation between the form class group and the ideal class group. Let $C(D)$ be the form class group of a negative discriminant D. Just like quadratic forms, orders also have discriminants, as is described in [7, §7A]. It is proven in [7, Exercise 7.3] that there exists a unique order $\mathcal{O}$ in an imaginary quadratic field with discriminant D. The ideal class group $C(\mathcal{O})$ of this order and the form class group $C(D)$ are isomorphic by [7, Theorem 7.7 (ii)]. It follows that $C(\mathcal{O})$ and $C(D)$ have the same number of elements, which we call the *class number*. Computing the class number is, in general, a difficult problem. Computing the number of elements in the form class group however, is much easier, see for example [5, Algorithm 5.3.5]. This algorithm is discussed in 2.18. The implementation of the algorithm in Sage is given in Appendix A.

1.3 Motivation

Computing the class number of the ring of integers measures how far the ring of integers is from being a unique factorization domain. This is not true for orders that are not maximal. The reason is that the ring of integers is a Dedekind domain, as stated in [7, Theorem 5.5], which is not true for an order that is not maximal, see [7, §7A]. Dedekind domains have the property that they are unique factorization domains if and only if they are principal ideal domains, see [9, Theorem 18]. Dedekind domains are the subject of subsection 3.4.

The ring of integers in a quadratic field K is denoted by $\mathcal{O}_K$. If the class number of $\mathcal{O}_K$ is one, then $I(\mathcal{O}_K) = P(\mathcal{O}_K)$, which implies that all proper fractional ideals of $\mathcal{O}_K$ are principal. Since the ideals of $\mathcal{O}_K$ are proper fractional ideals, see [7, Exercise 7.6(b)], we conclude that $\mathcal{O}_K$ is a principal ideal domain. Hence, $\mathcal{O}_K$ is a unique factorization domain if the corresponding ideal class group is trivial. In the final section, we will compute the class number of the ring of integers in multiple imaginary quadratic fields, to determine whether the ring of integers is a unique factorization domain.

2 Integral binary quadratic forms

An integral binary quadratic form

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

is called *primitive* if its coefficients a, b and c are relatively prime. An integer m is represented by $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y. In case x and y of the integer solution are relatively prime, we say that m is properly represented by $f(x, y)$.

2.1 Equivalent forms

We can define an equivalence relation on the set of binary integral quadratic forms.

Definition 2.1. The quadratic form $f(x, y)$ is equivalent to the form $g(x, y)$ if there exist integers p, q, r and s such that

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

We use $f \sim g$ to denote that f is equivalent to g.

To prove that this indeed defines an equivalent relation, we have to show that it is reflexive, symmetric and transitive. Before we give this proof, we will first see how equivalence is defined in terms of matrices.

Let $f(x, y) = ax^2 + bxy + cy^2$ be an arbitrary quadratic form. The form f has the following matrix representation:

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}}_{M_f} \begin{pmatrix} x \\ y \end{pmatrix}.$$

This leads us to the following definition.

Definition 2.2. The matrix M_f of a quadratic form f is the unique 2×2 symmetric matrix such that

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} M_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

Let f and g be arbitrary quadratic forms. Let M_f be the matrix of f and M_g be the matrix of g. Assume that f is equivalent to g, so there exist integers p, q, r and s such

that $f(x,y) = g(px+qy, rx+sy)$ and $ps - qr = \pm 1$. We can rewrite this as follows:

$$\begin{aligned}
\begin{pmatrix} x & y \end{pmatrix} M_f \begin{pmatrix} x \\ y \end{pmatrix} &= f(x,y) \\
&= g\left(\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} \right) \\
&= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} M_g \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} M_g \begin{pmatrix} p & r \\ q & s \end{pmatrix}^T \begin{pmatrix} x \\ y \end{pmatrix},
\end{aligned} \tag{1}$$

where $\det \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \pm 1$.

We are now ready to prove that the relation in Definition 2.1 is indeed an equivalence relation.

Proof. It is clear that $f \sim f$ for every quadratic form f. Namely, pick $p = s = 1$ and $q = r = 0$, then $f(x,y) = f(px+qy, rx+sy)$ and $ps - qr = 1$. Therefore, the relation is reflexive.

Suppose that for two quadratic forms f and g it holds that $f \sim g$. Let M_f be the matrix for f and M_g be the matrix for g. There exist integers p, q, r and s such that $f(x,y) = g(px+qy, rx+sy)$ and $ps - qr = \pm 1$. It follows from (1) that

$$M_f = \begin{pmatrix} p & r \\ q & s \end{pmatrix} M_g \begin{pmatrix} p & r \\ q & s \end{pmatrix}^T.$$

Moreover $\det \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \pm 1$, so the matrix $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$ is invertible. Hence, we get

$$\begin{aligned}
M_g &= \pm \begin{pmatrix} s & -r \\ -q & p \end{pmatrix} \cdot M_f \cdot \pm \begin{pmatrix} s & -r \\ -q & p \end{pmatrix}^T \\
&= \begin{pmatrix} s & -r \\ -q & p \end{pmatrix} M_f \begin{pmatrix} s & -r \\ -q & p \end{pmatrix}^T
\end{aligned}$$

This shows that

$$\begin{aligned}
g(x,y) &= f\left(\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} s & -r \\ -q & p \end{pmatrix} \right) \\
&= f(sx - qy, -rx + py).
\end{aligned}$$

Note that $\det \begin{pmatrix} s & -r \\ -q & p \end{pmatrix} = ps - qr = \pm 1$. Hence, we have that $g \sim f$. This proves that the relation is symmetric.

Suppose we have three quadratic forms f, g and h for which it holds that $f \sim g$ and $g \sim h$. Let M_f be the matrix of f, M_g be the matrix of g and M_h be the matrix of h. There exist $p, q, r, s, t, u, v, w \in \mathbb{Z}$ such that

$$f(x,y) = g\Big(\begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} p & r \\ q & s \end{pmatrix}}_{A} \Big) \qquad \text{and} \qquad g(x,y) = h\Big(\begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} t & v \\ u & w \end{pmatrix}}_{B} \Big),$$

with $\det A = \pm 1$ and $\det B = \pm 1$. Following (1), we get two equations:

$$M_f = A^T M_g A \qquad \text{and} \qquad M_g = B^T M_h B,$$

so $M_f = A^T B^T M_h B A = (BA)^T M_h BA$. Note that $\det BA = \det B \cdot \det A = \pm 1$. This shows that $f \sim h$ and hence the relation is transitive. □

Definition 2.3. The equivalence in Definition 2.1 is called *proper equivalence* if $ps - qr = 1$ and *improper equivalence* if $ps - qr = -1$.

Remark 2.4. The matrices with integer entries and unit determinant form a group called $SL(2, \mathbb{Z})$. Specifically, $SL(2, \mathbb{Z})$ is closed under matrix multiplication and taking inverses. This is the reason that proper equivalence is also an equivalence relation and the same proof as for equivalence can be used to prove it. The set of matrices with integer entries and determinant -1 is not a group, since this set is not closed under matrix multiplication. Therefore transitivity does not hold for improper equivalence, so improper equivalence is not an equivalence relation.

Theorem 2.5 ([11, Proposition 1.17])**.** Equivalent forms represent the same set of integers.

Proof. Let f and g be two arbitrary quadratic forms and assume that $f \sim g$. Furthermore, assume that m is an integer that is represented by f. Then there exist integers p, q, r and s with $f(x,y) = g(px + qy, rx + sy)$ and $ps - qr = \pm 1$. Moreover, the equation $m = f(x,y)$ has an integer solution in x and y, so there exist $a, b \in \mathbb{Z}$ such that $m = f(a,b)$. Then it follows that

$$m = f(a,b) = g(pa + qb, ra + sb),$$

where $pa + qb, ra + sb \in \mathbb{Z}$. Hence m is represented by g. Since $f \sim g$ is symmetric, we also have that $g \sim f$. Then the same proof shows that if the integer n is represented by g, then n is represented by f. □

Corollary 2.6 ([11, Corollary 1.20])**.** Any quadratic form equivalent to a primitive form is itself primitive.

Proof. Let $f = kx^2 + lxy + my^2$ be a primitive quadratic form and let $g = ax^2 + bxy + cy^2$ be an arbitrary quadratic form such that $f \sim g$. Suppose g is not primitive. Then

$d \coloneqq \gcd(a,b,c) > 1$. It follows that $d|ax^2+bxy+cy^2$ for all $x,y \in \mathbb{Z}$. So for all integers m that are represented by g, it holds that $d|m$. It follows from Theorem 2.5 that $d|m$ for all integers m that are represented by f. But this implies that $d|\gcd(k,l,m)$ and hence $\gcd(k,l,m) > 1$, which contradicts the assumption that f is primitive. □

Lemma 2.7 ([7, Lemma 2.3])**.** An integer m is properly represented by a quadratic form f if and only if there exist $B, C \in \mathbb{Z}$ such that f is properly equivalent to the form $mx^2+Bxy+Cy^2$.

Proof. Assume that the integer m is properly represented by the form $f(x,y) = ax^2 + bxy + cy^2$. Then there exist integers p and q, relatively prime, such that $m = f(p,q)$. By Bézout's identity, we can find $r, s \in \mathbb{Z}$ such that $ps - qr = 1$. Then we obtain

$$\begin{aligned} f(px+ry, qx+sy) &= a(px+ry)^2 + b(px+ry)(qx+sy) + c(qx+sy)^2 \\ &= (ap^2+bpq+cq^2)x^2 + (2apr+bps+brq+2cqs)xy \\ &\quad + (ar^2+brs+cs^2)y^2 \\ &= f(p,q)x^2 + Bxy + Cy^2 \\ &= mx^2 + Bxy + Cy^2. \end{aligned}$$

Next assume that f is properly equivalent to the form $g(x,y) = mx^2+Bxy+Cy^2$. Since $g(1,0) = m$, we have that g properly represents m. By Theorem 2.5, we get that f represents m. It remains to show that f represents m properly. We can find integers p, q, r and s such that $g(x,y) = f(px+qy, rx+sy)$ and $ps - qr = 1$. Then

$$m = g(1,0) = f(p,r).$$

Since $ps - qr = 1$, it follows from Bézout's identity that $\gcd(p,r) = 1$ and hence m is properly represented by f. □

Corollary 2.8 ([11, Corollary 1.26])**.** Properly equivalent forms properly represent the same set of integers.

Proof. Let f and g be two arbitrary quadratic forms with f properly equivalent to g. Assume that m is an integer that is properly represented by f. Then it follows from Theorem 2.5 that m is represented by g. We still have to prove that g represents m properly. By Lemma 2.7, we know that there exist $B, C \in \mathbb{Z}$ such that f is properly equivalent to the form $mx^2+Bxy+Cy^2$. Using the symmetry and transitivity of proper equivalence, we obtain that g is properly equivalent to $mx^2+Bxy+Cy^2$. Then Lemma 2.7 implies that m is properly represented by g. □

Definition 2.9. Let $f(x,y) = ax^2+bxy+cy^2$ be a quadratic form. Then we define the *discriminant* D of f to be $D = b^2 - 4ac$.

Theorem 2.10 ([11, Proposition 1.16])**.** Equivalent forms have the same discriminant.

Proof. Let f and g be two arbitrary quadratic forms with $f \sim g$. Write $g(x,y) = ax^2+bxy+cy^2$ so that the discriminant D_g is b^2-4ac. There exist integers p, q, r and s such that $f(x,y) = g(px+qy, rx+sy)$ and $ps-qr = \pm 1$. A simple computation shows

$$f(x,y) = (ap^2+bpr+cr^2)x^2 + (2apq+bps+bqr+2crs)xy + (aq^2+bqs+cs^2)y^2$$

We can then compute the discriminant D_f of f. This is an easy, but long computation, so we will not do it in detail. We find

$$\begin{aligned} D_f &= (2apq+bps+bqr+2crs)^2 - 4(ap^2+bpr+cr^2)(aq^2+bqs+cs^2) \\ &= (ps-qr)^2(b^2-4ac) \\ &= D_g. \end{aligned}$$

□

The sign of the discriminant D of a quadratic form $f(x,y) = ax^2+bxy+cy^2$ tells us something about the sign of the integers that are represented by f. This is clear from the following identity:

$$\begin{aligned} 4af(x,y) &= 4a(ax^2+bxy+cy^2) \\ &= 4a^2x^2+4abxy+4acy^2 \\ &= 4a^2x^2+4abxy+b^2y^2-b^2y^2+4acy^2 \\ &= (2ax+by)^2 - Dy^2. \end{aligned} \tag{2}$$

If $D > 0$, then the right-hand side of (2) can be positive or negative. This means that f represents both positive and negative integers. In this case, we call f *indefinite*. If $D < 0$, then we see that the right-hand side of (2) is positive. The sign of the integers that f represents then corresponds to the sign of a. We call f *positive definite* if a is positive, and *negative definite* if a is negative. The notions of indefiniteness, positive definiteness and negative definiteness are invariant under equivalence. This follows directly from Theorem 2.10 and Theorem 2.5, which state that equivalent forms have the same discriminant and represent the same set of integers.

The discriminant D of a form $f(x,y) = ax^2+bxy+cy^2$ also gives information about the sign of the middle coefficient b of f. Namely, $D = b^2-4ac \equiv b^2 \mod 4$, so b is even when $D \equiv 0 \mod 4$ and b is odd when $D \equiv 1 \mod 4$.

Lemma 2.11 ([7, Lemma 2.5])**.** Let D be an integer satisfying $D \equiv 0, 1 \mod 4$ and m an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if $D \equiv b^2 \mod m$ for some $b \in \mathbb{Z}$.

Proof. Assume that m is properly represented by a primitive form f of discriminant D. By Lemma 2.7, there exist $b, c \in \mathbb{Z}$ such that f is properly equivalent to $mx^2+bxy+cy^2$. Then the discriminant D of f is b^2-4mc, because equivalent forms have the same discriminant. It follows that $D = b^2 \mod m$.

Next assume that $D \equiv b^2 \mod m$ for some $b \in \mathbb{Z}$. Then there exists $k \in \mathbb{Z}$ such that $D = b^2 + mk$. We will show that we can pick b in such a way that D and b have the same parity. First suppose that D is even. Then b^2 and mk are either both even or both odd. If b^2 is even, and hence b is even, b has the same parity as D. If b^2 is odd, and hence b is odd, we can replace b by the even integer $b + m$. We can do this because $(b+m)^2 \mod m = b^2 \mod m$. Next suppose that D is odd. Then either b^2 is odd and mk is even or vice versa. If b^2 is odd, and hence b is odd, b has the same parity as D. If b^2 is even, and hence b is even, then we can replace b by the odd integer $b + m$. Hence, we can assume that D and b have the same parity.

The next step is to show that $D \equiv b^2 \mod 4m$. Suppose that D is even, so $D = b^2 + mk \equiv 0 \mod 4$. Then also b is even, which implies that $b^2 \equiv 0 \mod 4$. It follows that $mk \in 4\mathbb{Z}$ and hence $D \equiv b^2 \mod 4m$. Now suppose that D is odd, so $D = b^2 + mk \equiv 1 \mod 4$. Then also b is odd, which implies that $b^2 \equiv 1 \mod 4$. It follows that $mk \in 4\mathbb{Z}$ and hence $D \equiv b^2 \mod 4m$.

Since $D \equiv b^2 \mod 4m$, there exists $c \in \mathbb{Z}$ such that $D = b^2 - 4mc$. The form $mx^2 + bxy + cy^2$ has discriminant D and properly represents m. To show that $mx^2 + bxy + cy^2$ is primitive, suppose that n divides m, b and c. Then we also have that n divides D. Since m and D are relatively prime, we must have that $n = \pm 1$. Hence, the form $mx^2 + bxy + cy^2$ is primitive. □

2.2 Reduced forms

For the rest of this paper, we restrict ourselves to primitive positive definite forms. The following definition applies to these forms.

Definition 2.12. We call a primitive positive definite form $ax^2 + bxy + cy^2$ reduced if

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

Lemma 2.13 ([11, Proposition 1.39])**.** Let $f = ax^2 + bxy + cy^2$ be a primitive positive definite form that is reduced. Then the smallest nonzero integer that is represented by f is a.

Proof. Since $f(1, 0) = a$, the integer a is represented by f. Suppose that x and y are

nonzero. Using that $|b| \leq a \leq c$, we can make the estimation

$$\begin{aligned} f(x,y) &= ax^2 + bxy + cy^2 \\ &\geq ax^2 - |bxy| + ay^2 \\ &= a(x^2+y^2) - |bxy| \\ &\geq 2a|xy| - |bxy| \qquad (3) \\ &\geq a|xy| \\ &\geq a, \end{aligned}$$

where in (3) we have used that $(|x|-|y|)^2 = x^2 - 2|xy| + y^2 \geq 0$ and therefore $x^2+y^2 \geq 2|xy|$. Moreover, we have that

$$\begin{aligned} f(0,y) &= cy^2 \geq ay^2 \geq a \text{ for all nonzero integers } y, \\ f(x,0) &= ax^2 \geq a \text{ for all nonzero integers } x. \end{aligned}$$

This proves that a is the smallest nonzero integer that is represented by f. □

The proof of the following theorem consists of three steps. Step 1 and 2 follow the proof of [7, Theorem 2.8] and step 3 follows the proof of [10, Theorem 3.1].

Theorem 2.14. Every primitive positive definite form is properly equivalent to a unique reduced form.

Proof. Let f be an arbitrary primitive positive definite form. In the first two steps we will show that there exists a reduced form such that f is properly equivalent to this form. In the final step we will show that this reduced form is unique.

Step 1. We will first show that f is properly equivalent to a form $ax^2 + bxy + cy^2$ satisfying $|b| \leq a \leq c$. Consider the set of all forms properly equivalent to f and pick $g(x,y) = ax^2 + bxy + cy^2$ in this set so that $|b|$ is as small as possible. Suppose that $a < |b|$. Let m be any integer and define

$$\begin{aligned} h(x,y) &\coloneqq g(x+my, y) \\ &= a(x+my)^2 + b(x+my)y + cy^2 \\ &= ax^2 + (2am+b)xy + (am^2+bm+c)y^2. \end{aligned}$$

Then h is properly equivalent to g for all choices of m. Moreover, h is properly equivalent to f, which implies that h is positive definite. Thus, the integer a satisfies the following two properties: $a > 0$ and $a < |b|$. Note that $2am + b \equiv b \mod 2a$. We can therefore choose m in such a way that $|2am + b| \leq a < |b|$. This contradicts the minimality of $|b|$. Hence, we must have that $a \geq |b|$. Similarly, suppose that $c < |b|$ and define $k(x,y) \coloneqq g(x, nx+y)$ for any integer n. In the same way as before, we can pick n in

such a way that $|2cn + b| \leq c < |b|$ and get a contradiction with the minimality of $|b|$. It follows that $c \geq |b|$. Two cases remain: $a \leq c$ or $a > c$. In the first case, we obtain that g satisfies $|b| \leq a \leq c$. In the second case, we define the form g' to be

$$g'(x, y) = g(-y, x) = cx^2 - bxy + ay^2.$$

Then g' does satisfy $|b| \leq c \leq a$. Moreover, g' is properly equivalent to g, which implies that g' is properly equivalent to f.

Step 2. We have shown that there exists a form $g(x, y) = ax^2 + bxy + cy^2$ satisfying $|b| \leq a \leq c$ that is properly equivalent to f. We will show that g is properly equivalent to a reduced form. Except for the two cases which are $b < 0$ and $b = -a$, and $b < 0$ and $a = c$, the form g is itself reduced. In both cases, the form $h(x, y) = ax^2 - bxy + cx^2$ is reduced. In the first case, that is $b < 0$ and $b = -a$, we have

$$\begin{aligned} g(x + y, y) &= a(x + y)^2 - a(x + y)y + cy^2 \\ &= ax^2 + axy + cy^2 \\ &= ax^2 - bx^2 + cy^2 \\ &= h(x, y). \end{aligned}$$

This shows that g is properly equivalent to h. In the second case, that is $b < 0$ and $a = c$, we have

$$\begin{aligned} g(-y, x) &= ay^2 - bxy + cx^2 \\ &= ax^2 - bxy + cy^2 \\ &= h(x, y). \end{aligned}$$

This shows that g is properly equivalent to h in this case as well.

Step 3. In step 1 and 2, we have proven the existence of a reduced form h such that f is properly equivalent to h. In this step, we will prove the uniqueness of such a reduced form. We will do this by showing that different reduced forms cannot be properly equivalent. Suppose $g(x, y) = a'x^2 + b'xy + c'y^2$ is a reduced form properly equivalent to the reduced form $f(x, y) = ax^2 + bxy + cy^2$. By Theorem 2.5, f and g represent the same set of integers. It follows from Lemma 2.13 that $a = a'$.

Suppose that $c > c'$. Since g is reduced, we have that $c' \geq a' = a$, so it follows that $c > a$. There exist integers p, q, r and s such that $g(x, y) = f(px + qy, rx + sy)$ and $ps - qr = 1$. This results in the following equalities for the coefficients of g:

$$a' = ap^2 + bpr + cr^2, \tag{4}$$

$$b' = 2apq + bps + bqr + 2crs, \tag{5}$$

$$c' = aq^2 + bqs + cs^2. \tag{6}$$

Using that $c > a$, Equation (4) leads to the inequality

$$\begin{aligned} a' &= ap^2 + bpr + cr^2 \\ &> ap^2 - |bpr| + ar^2 \\ &= a(p^2 + r^2) - |bpr|. \end{aligned} \tag{7}$$

Note that $(|p| - |r|)^2 = p^2 - 2|pr| + r^2 \geq 0$ and therefore $p^2 + r^2 \geq 2|pr|$. It follows from (7) that $a' > 2a|pr| - |bpr|$. Since $|b| \leq a$, we have $a' > a|pr|$. We have already shown that $a' = a$, so this inequality can only hold when $|pr| = 0$. If $p = 0$, then (4) reduces to $a' = cr^2 > ar^2$, which again can only hold when $r = 0$. However, p and r cannot both be zero, because in that case $ps - qr = 0$. Hence, p must be nonzero. If $r = 0$, then $ps - qr = 1$ implies that $ps = 1$. Filling in $r = 0$ and $ps = 1$ in (5), we find that $b' = 2apq + b$. From the fact that f and g are reduced, we obtain

$$|b| \leq a \qquad \text{and} \qquad |b'| \leq a' = a.$$

These inequalities only hold if $2apq = 0$, which implies that $q = 0$. Hence, we find that $b' = b$.

Similarly, suppose that $c < c'$. Then there exist integers p, q, r and s such that $f(x, y) = g(px + qy, rx + sy)$ and $pq - rs = 1$. This equation results in the equalities (4), (5) and (6) for the coefficients of f, where a, b and c are replaced by a', b' and c' respectively, and vice versa. In this way, the roles of the coefficients of f and g are reversed and using the same proof as above, we conclude that $b = b'$.

Since equivalent forms have the same discriminant and we proved that $a' = a$ and $b' = b$, it follows that also $c' = c$. Hence, we have that $g = f$. This shows that if two reduced forms are properly equivalent, they must be equal. □

We restricted ourselves to the set of primitive positive definite quadratic forms. Remember that the discriminant of these forms is always negative. Fix an integer $D < 0$ and consider the set of primitive positive definite forms of discriminant D. We can split this set into equivalence classes by saying that two forms belong to the same equivalence class if and only if they are properly equivalent. The number of equivalence classes in the set of primitive positive definite forms of discriminant D is called the *class number* and is denoted by $h(D)$. Theorem 2.14 implies that every equivalence class contains exactly one reduced form and hence $h(D)$ is equal to the number of reduced forms of discriminant D.

Theorem 2.15 ([7, Theorem 2.13])**.** Let the integer $D < 0$ be fixed. Then $h(D)$ is finite and the number of reduced forms of discriminant D is equal to $h(D)$.

Proof. We have already argued that Theorem 2.14 implies that $h(D)$ is equal to the number of reduced forms of discriminant D. It remains to show that $h(D)$ is finite.

This follows from the following observation. Suppose that $f(x, y) = ax^2 + bxy + cy^2$ is a reduced form of discriminant D. Then the coefficients of f satisfy $|b| \leq a \leq c$ and $b^2 \leq a^2$. These inequalities lead to

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

and hence

$$a \leq \sqrt{\frac{-D}{3}}. \tag{8}$$

The integer D is fixed. Thus, the inequality $|b| \leq a$ and Equation (8) imply that there are finitely many choices for the coefficients a and b of f. Since c is uniquely determined by a and b, we also have finitely many options for the coefficient c of f. Hence, there are finitely many reduced forms of discriminant D. Since the number of reduced forms of discriminant D is equal to $h(D)$, we have shown that $h(D)$ is finite. □

2.3 Algorithms

We will look at two algorithms. The first algorithm finds and lists all the reduced forms of a given negative discriminant. Counting the number of reduced forms gives the class number. The goal of the second algorithm is to compute the class number in an efficient way. Both algorithms are constructed using the theory discussed so far. We use the notation (a, b, c) for the form $ax^2 + bxy + cy^2$. This notation will come back in the next section.

In the previous section, we have seen that reduced forms satisfy the inequalities

$$a \leq \sqrt{\frac{-D}{3}} \qquad \text{and} \qquad |b| \leq a \leq c.$$

Moreover, $b \geq 0$ if $|b| = a$ or $a = c$. The input of the first algorithm is a negative discriminant D. Then for all values $a \in \left\{1, \ldots, \left\lfloor \sqrt{\frac{-D}{3}} \right\rfloor \right\}$, the algorithm checks for every value $b \in \{-a, \ldots, a\}$ whether (a, b, c) represents a reduced form. Note that once given the value of a and b, the value of c can be computed using the formula for the discriminant.

Algorithm 2.16 (Computing reduced forms)**.** Let D be a negative discriminant.

1. Set $a = 1$, $b = -a$, let $c = \frac{b^2 - D}{4a}$ and go to step 4.
2. Set $a = a + 1$. If $a \leq \sqrt{\frac{-D}{3}}$, set $b = -a$, let $c = \frac{b^2 - D}{4a}$ and go to step 4. Otherwise, output the number of reduced forms and end the algorithm.

3. Set $b = b + 1$. If $b \leq a$, let $c = \frac{b^2 - D}{4a}$ and go to the next step. Otherwise, go to step 2.

4. If c is an integer, $c \geq a$ and $\gcd(a, b, c) = 1$, then go to the next step. Otherwise, go to step 3.

5. If $|b| = a$ or $a = c$, go to the next step. Otherwise, go to step 7.

6. If $b \geq 0$, output (a, b, c). Then go to step 3.

7. Output (a, b, c) and go to step 3.

Example 2.17. Let $D = -12$. Set $a = 1$, $b = -1$ and let $c = \frac{b^2 - D}{4a} = \frac{13}{4}$. Then c is not an integer, so we set $b = 0$. It holds that $b \leq a$, so we compute $c = \frac{b^2 - D}{4a} = 3$. Then c is an integer, $c \geq a$ and $\gcd(a, b, c) = 1$. We have therefore found the reduced form $(1, 0, 3)$.

We go back to step 3 and set $b = 1$. We still have $b \leq a$, so set $c = \frac{13}{4}$. Since this is not an integer, we set $b = 2$. Then $b \geq a$, so we set $a = 2$. Note that $a \leq \sqrt{\frac{-D}{3}} = 2$. Set $b = -2$ and let $c = 2$. Then $\gcd(a, b, c) = 2$, so we set $b = -1$. We have $b \leq a$, so let $c = \frac{13}{8}$, which is not an integer. Therefore, we set $b = 0$. Then $b \leq a$, but $\gcd(a, b, c) = 2$. We set $b = 1$ and find $c = \frac{13}{8}$, which is not an integer. Finally, we set $b = 2$, which implies that $\gcd(a, b, c) = 2$. Then we set $a = 3$. Since we have $a > \sqrt{\frac{-D}{3}} = 2$, we end the algorithm. We have found one reduced form $(1, 0, 3)$, so the class number is 1.

The second algorithm is obtained from [5, Algorithm 5.3.5]. It counts the number of reduced forms of a given negative discriminant.

Algorithm 2.18 (Counting reduced forms)**.** Let D be a negative discriminant.

1. If $D \equiv 0 \mod 4$, let $b = 0$ and if $D \equiv 1 \mod 4$, let $b = 1$. Let $B = \left\lfloor \sqrt{\frac{-D}{3}} \right\rfloor$ and set $h = 1$.

2. Set $q = \frac{b^2 - D}{4}$ and $a = b$. If $a \leq 1$, set $a = 1$ and go to step 4.

3. If $a | q$ and $\gcd(a, b, \frac{q}{a}) = 1$, set $h = h + 2$, unless it also holds that $a = b$, $a^2 = q$ or $b = 0$, then set $h = h + 1$.

4. Set $a = a + 1$. If $a^2 \leq q$, go to step 3.

5. Set $b = b + 2$. If $b \leq B$, go to step 2. Otherwise output h, which gives the class number of D.

Before proving this algorithm, we make the following observations.

(i) We showed in the proof of Theorem 2.15 that B is an upper bound for the coefficient a of a reduced form. Together with the inequality $|b| \leq a \leq c$, we obtain that $|b| \leq B$.

(ii) The integer q stands for the product of the coefficient a and c. Hence, we have that $a^2 \leq q$ if and only if $a \leq c$.

(iii) The integer h counts the number of reduced forms of discriminant D.

Proof. In step 1, we let b be the smallest nonnegative integer matching the parity of D. The inequality $|b| \leq a$ implies that the smallest integer that a can attain is b, so in step 2 we set $a = b$. The coefficient a must however be positive, because reduced forms are positive definite. Therefore, if $a \leq 1$, we set $a = 1$.

In step 3 and step 4, the algorithm checks for all values of a between b and c (observation (ii)) if (a, b, c) defines a reduced form. If in step 3, we have $a|q$ and $\gcd(a, b, \frac{q}{a}) = 1$, then both (a, b, c) and $(a, -b, c)$ define reduced forms, unless it also holds that $a = b$, $a^2 = q$ or $b = 0$ in which case only (a, b, c) defines a reduced form. The value of h is adjusted accordingly (observation (iii)).

In step 5, the value of b is changed to the next smallest integer having the same parity as D. If $b \leq B$, we go to step 2 and check again for all values of a between b and c if (a, b, c) defines a reduced form. Otherwise, the algorithm ends.

Since B is an upper bound for the coefficient b of a reduced form (observation (i)), there are only finitely many combination of coefficients (a, b, c) of which we have to check if they define a reduced form. Hence, the algorithm ends in finitely many steps. □

The implementation of Algorithm 2.16 and Algorithm 2.18 in Sage can be found in Appendix A.

2.4 The form class group

In this section, we fix a negative discriminant D and look at the set of primitive positive definite forms of discriminant D. Proper equivalence splits this set into equivalence classes. The set of equivalence classes of primitive positive definite forms of discriminant D is denoted by $C(D)$. We will study the operation that turns the set $C(D)$ into a finite Abelian group.

Definition 2.19. Let $f(x, y)$ and $g(x, y)$ be primitive positive definite forms of discriminant D. Then a primitive positive definite form $F(x, y)$ of discriminant D is the *composition* of f and g if

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)),$$

where

$$B_i(x,y;z,w) = a_ixz + b_ixw + c_iyz + d_iyw, \qquad i = 1,2,$$

are integral bilinear forms.

Suppose that $F(x,y) = Ax^2 + Bxy + Cy^2$ is the composition of the primitive positive definite forms $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$, so

$$f(x,y)g(z,w) = F(a_1xz + b_1xw + c_1yz + d_1yw, a_2xz + b_2xw + c_2yz + d_2yw). \tag{9}$$

We can make the following claim of which the proof is discussed in [7, Exercise 3.1].

Claim.

$$a_1b_2 - a_2b_1 = \pm f(1,0), \qquad a_1c_2 - a_2c_1 = \pm g(1,0). \tag{10}$$

Proof. Take $x = z = 1$ and $y = w = 0$. Then (9) becomes

$$aa' = Aa_1^2 + Ba_1a_2 + Ca_2^2. \tag{11}$$

Similarly, taking $x = w = 1$ and $y = z = 0$ in (9) gives

$$ac' = Ab_1^2 + Bb_1b_2 + Cb_2^2. \tag{12}$$

Set $x = z = w = 1$ and $y = 0$ in (9). Then we obtain

$$a(a' + b' + c') = A(a_1 + b_1)^2 + B(a_1 + b_1)(a_2 + b_2) + C(a_2 + b_2)^2. \tag{13}$$

If we substitute (11) and (12) in (13) and rewrite the resulting equation, we get

$$ab' = 2Aa_1b_1 + B(a_1b_2 + b_1a_2) + 2Ca_2b_2. \tag{14}$$

Equations (11), (12) and (14) give expressions for a', b' and c'. Using this expressions, we can show that

$$a^2(b'^2 - 4a'c') = (a_1b_2 - a_2b_1)^2(B^2 - 4AC)$$

from which it follows that $a = f(1,0) = \pm(a_1b_2 - a_2b_1)$. In the same way, we can find expressions for $a'a, a'b$ and $a'c$, which we can use to show that $a'^2(b^2 - 4ac) = (a_1c_2 - a_2c_1)^2(B^2 - 4AC)$. It follows that $a' = g(1,0) = \pm(a_1c_2 - a_2c_1)$. □

Definition 2.20. The composition in Definition 2.19 is called a *direct composition* if both signs in Equation (10) are +.

The following lemma is taken from [7, Lemma 3.5], but the proof is based on [3, Lemma 2.9].

Lemma 2.21. Let $p_1, q_1, \ldots, p_r, q_r, m$ be integers with $\gcd(p_1, \ldots, p_r, m) = 1$. Then there exists a unique integer $B \mod m$ such that

$$p_i B \equiv q_i \mod m, \qquad i = 1, \ldots, r$$

if and only if

$$p_i q_j \equiv p_j q_i \mod m,$$

for all $i, j = 1, \ldots, r$.

Proof. Assume that there exists a unique integer $B \mod m$ such that

$$p_i B \equiv q_i \mod m, \qquad i = 1, \ldots, r.$$

Let $i, j \in \{1, \ldots, r\}$ be arbitrary. There exists integers k and l such that

$$\begin{aligned} p_i B &= q_i + mk, \\ p_j B &= q_j + ml \implies q_j = p_j B - ml. \end{aligned}$$

Using these equalities, we get

$$\begin{aligned} p_i q_j &= p_i(p_j B - ml) \\ &= p_j p_i B - p_i ml \\ &= p_j(q_i + mk) - p_i ml \\ &= p_j q_i + m(p_j k - p_i l) \\ &\equiv p_j q_i \mod m \end{aligned}$$

Next assume that $p_i q_j \equiv p_j q_i \mod m$ for all $i, j = 1, \ldots, r$. Since $\gcd(p_1, \ldots, p_r, m) = 1$, a repeated application of Bézout's identity implies that there exist integers $a, a_1, \ldots, a_r$ such that $am + \sum_{i=1}^r a_i p_i = 1$. It follows that $\sum_{i=1}^r a_i p_i \equiv 1 \mod m$. Let B be the unique integer between 0 and m such that

$$B \equiv \sum_{i=1}^r a_i q_i \mod m.$$

Let $j \in \{1, \ldots, r\}$ be arbitrary. Then we find

$$\begin{aligned} p_j B &\equiv \sum_{i=1}^r a_i p_j q_i \mod m \\ &= \sum_{i=1}^r a_i p_i q_j \mod m \\ &= q_j \sum_{i=1}^r a_i p_i \mod m \\ &= q_j \mod m. \end{aligned}$$

This proves that there exists an integer $B \mod m$ that satisfies $p_i B \equiv q_i \mod m$ for $i = 1, \ldots, r$.

Next, we will show that the integer B is unique modulo m. Suppose that both B and B' satisfy $p_i B \equiv q_i \mod m$ for $i = 1, \ldots, r$. Then for all $i = 1, \ldots, r$, we have $p_i(B - B') \equiv 0 \mod m$ and hence $m | p_i(B - B')$. Let k be the least integer such that $m | k(B - B')$. If $k = \pm 1$, then $m | (B - B')$ and it follows that $B \equiv B' \mod m$. We will therefore assume that $k \neq \pm 1$. Suppose there exists another integer l such that $m | l(B - B')$. Then $|l| \geq |k|$, so we can write $l(B - B') = r \cdot k(B - B') + s(B - B')$, where $|s| < |k|$. Note that $m | l(B - B')$ and $m | k(B - B')$, so also $m | s(B - B')$. This is however a contradiction with the minimality of k, unless $s = 0$. Therefore $s = 0$ and it follows that l is a multiple of k. If $m | p_i(B - B')$ and $m \nmid (B - B')$, then this argument shows that p_i, for $i = 1, \ldots, r$, is a multiple of k. Since $\gcd(p_1, \ldots, p_r, m) = 1$, it holds that $\gcd(k, m) = 1$. By Bézout's identity, there exist integers x and y such that $kx + my = 1$. Multiplying by $B - B'$ gives $k(B - B')x + m(B - B')y = B - B'$. Note that $m | k(B - B')$ and $m | m(B - B')y$, so $m | k(B - B')x + m(B - B')y = B - B'$. Hence, $B \equiv B' \mod m$, which shows that B is unique modulo m. □

Lemma 2.22 ([7, Lemma 3.2])**.** Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ have discriminant D such that $\gcd(a, a', \frac{b+b'}{2}) = 1$. Then there exists a unique integer B modulo $2aa'$ such that

$$B \equiv b \mod 2a, \tag{15}$$

$$B \equiv b' \mod 2a', \tag{16}$$

$$B^2 \equiv D \mod 4aa'. \tag{17}$$

Proof. First note that b and b' have the same parity as both have the same parity as D. Therefore, $b + b'$ is even and $\frac{b+b'}{2}$ is indeed an integer.

Congruence (15) and (16) imply that there exist integers k and l such that $B = b + 2ak$ and $B = b' + 2a'l$. It follows that $(B - b)(B - b') = 4aa'kl$, so we have

$$B^2 - (b + b')B + bb' = (B - b)(B - b') \equiv 0 \mod 4aa'.$$

Using (17), we can rewrite the above equation in the following way:

$$(b + b')B \equiv B^2 + bb' \mod 4aa' \equiv D + bb' \mod 4aa'.$$

Dividing by 2 gives

$$\frac{b + b'}{2} B \equiv \frac{D + bb'}{2} \mod 2aa'.$$

If we multiply (15) and (16) by a' and a respectively, we obtain that the congruences in

Lemma 2.22 are equivalent to

$$a'B \equiv a'b \mod 2aa', \tag{18}$$
$$aB \equiv ab' \mod 2aa', \tag{19}$$
$$\frac{b+b'}{2}B \equiv \frac{D+bb'}{2} \mod 2aa'. \tag{20}$$

Since $\gcd(a, a', \frac{b+b'}{2}) = 1$ and it holds that

$$\begin{aligned} a'ab' &\equiv aa'b \mod 2aa', \\ a'\frac{D+bb'}{2} &\equiv \frac{b+b'}{2}a'B \mod 2aa' = \frac{b+b'}{2}a'b \mod 2aa', \\ a\frac{D+bb'}{2} &\equiv \frac{b+b'}{2}aB \mod 2aa' = \frac{b+b'}{2}ab' \mod 2aa', \end{aligned}$$

we can apply Lemma 2.21 to find the unique integer $B \mod 2aa'$ that satisfies (18), (19) and (20). □

Definition 2.23. Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant D such that $\gcd(a, a', \frac{b+b'}{2}) = 1$. Then

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

is the *Dirichlet composition* of f and g, where B is the unique integer modulo $2aa'$ of Lemma 2.22. We denote the Dirichlet composition of f and g by $f \circ g$.

Lemma 2.24 ([8, Theorem 7.1])**.** Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive form and M an integer. Then $f(x,y)$ properly represents at least one integer coprime to M.

Proof. We write M as its factorization into primes, so $M = \prod_{i=1}^{n} p_i^{r_i}$. We will show by contradiction that each p_i is relatively prime to at least one of the integers $f(1,0)$, $f(0,1)$ and $f(1,1)$. Let $i \in \{1, \ldots, n\}$ be arbitrary and suppose that p_i is not coprime to $f(1,0)$, $f(0,1)$ and $f(1,1)$. Then $p_i | f(1,0) = a$, $p_i | f(0,1) = c$ and $p_i | f(1,1) = a + b + c$, so also $p_i | b$. Therefore p_i divides all coefficients of f, which is a contradiction with the fact that f is primitive. Hence p_i is coprime to at least one of the integers $f(1,0)$, $f(0,1)$ and $f(1,1)$.

Let (x_i, y_i) be the pair of integers such that $f(x_i, y_i)$ is coprime to p_i. Then $f(x_i, y_i)$ is coprime to $p_i^{r_i}$. By the Chinese Remainder Theorem, there exist integers u and v that satisfy the equations

$$u \equiv x_i \mod p_i^{r_i} \qquad \text{and} \qquad v \equiv y_i \mod p_i^{r_i}, \qquad i = 1, \ldots, n.$$

Note that $f(u,v) \equiv f(x_i, y_i) \mod p_i^{r_i}$ for all $i = 1, \ldots, n$. This implies that $f(u,v)$ is coprime to $p_i^{r_i}$ for all $i = 1, \ldots, n$. Hence, it follows that $f(u,v)$ is coprime to M. □

Theorem 2.25 ([7, Proposition 3.8])**.** Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant D such that $\gcd(a, a', \frac{b+b'}{2}) = 1$. Then the Dirichlet composition $F(x,y)$ of f and g is a primitive positive definite form of discriminant D. Moreover, $F(x,y)$ is the direct composition of f and g.

Proof. We have

$$B^2 - 4aa'\frac{B^2-D}{4aa'} = B^2 - B^2 + D = D,$$

which shows that F has discriminant D. Moreover, the fact that f and g are positive definite implies that $aa' > 0$ and therefore F is positive definite.

Let $C = \frac{B^2-D}{4aa'}$, so that $F(x,y) = aa'x^2 + Bxy + Cy^2$. Since $B \equiv b \mod 2a$, there exists an integer k such that $B = b + 2ak$. Then $(x,y) \mapsto (x + ky, y)$ shows that f is properly equivalent to

$$\begin{aligned} f(x+ky,y) &= a(x+ky)^2 + b(x+ky)y + cy^2 \\ &= ax^2 + (b+2ak)xy + (c+bk+ak^2)y^2 \\ &= ax^2 + Bxy + a'Cy^2, \end{aligned}$$

where the last line follows from

$$\begin{aligned} a'C &= a'\frac{B^2-D}{4aa'} \\ &= \frac{(b+2ak)^2 - b^2 + 4ac}{4a} \\ &= \frac{b^2 + 4abk + 4a^2k^2 - b^2 + 4ac}{4a} \\ &= c + bk + ak^2. \end{aligned}$$

In the same way, we can show that g is properly equivalent to the form $a'x^2+Bxy+aCy^2$. Namely, $B \equiv b' \mod 2a'$ implies that there exists an integer l such that $B = b' + 2a'l$. Then $(x,y) \mapsto (x + ly, y)$ shows that g is properly equivalent to

$$\begin{aligned} g(x+ly,y) &= a'x^2 + (b'+2a'l)xy + (c'+b'l+a'l^2)y^2 \\ &= a'x^2 + Bxy + aCy^2, \end{aligned}$$

where the last line follows from

$$\begin{aligned} aC &= a\frac{B^2-D}{4aa'} \\ &= \frac{(b'+2a'l)^2 - b'^2 + 4a'c'}{4a'} \\ &= c' + b'l + a'l^2. \end{aligned}$$

Define $X \coloneqq xz - Cyw$ and $Y \coloneqq axw + a'yz + Byw$. Then an elaborate computation shows that

$$f(x + ky, y)g(z + lw, w) = aa'X^2 + BXY + CY^2.$$

Set $x' = x + ky$ and $z' = z + lw$. If we substitute x and z by x' and z' respectively in the equations for X and Y, we get that $X' = xz + lxw + kyz + klyw$ and $Y' = axw + a'yz + (ak + a'l + B)yw$. For this X' and Y' it holds that

$$f(x', y)g(z', w) = aa'(X')^2 + BX'Y' + C(Y')^2 = F(X', Y'),$$

which shows that F is the composition of f and g. Using the notation from Definition 2.19, we can read off from the equations for X' and Y' that

$$\begin{aligned} a_1 &= 1, & a_2 &= 0, \\ b_1 &= l, & b_2 &= a, \\ c_1 &= k, & c_2 &= a', \end{aligned}$$

so it follows that

$$a_1b_2 - a_2b_1 = a = +f(1, 0), \qquad a_1c_2 - a_2c_1 = a' = +g(1, 0).$$

Hence, F is the direct composition of f and g.

It remains to show that F is primitive. Suppose that there exists a prime p that divides all the coefficients of F. Then p divides all integers that are represented by F. Note that all integers of the form $f(x, y)g(z, w)$ for $x, y, z, w \in \mathbb{Z}$ are represented by F, because F is the composition of f and g. Since f and g are primitive positive definite forms, we know by Lemma 2.24 that there exist integers q and r both coprime to p that are represented by f and g respectively. Then the integer qr is also coprime to p and represented by F. This is a contradiction with our assumption that p divides all the coefficients of F. Hence, no prime p divides all the coeffients of F and it follows that F is primitive. □

Let $f = (a, b, c)$ and $g = (a', b', c')$ be two primitive positive definite forms of discriminant D for which the Dirichlet composition $f \circ g$ is defined. Then

$$f \circ g = (aa', B, C),$$

where $C = \frac{B^2 - D}{4aa'}$ and B the unique integer modulo $2aa'$ of Lemma 2.22. The proof of Theorem 2.25 shows that f is properly equivalent to the form $f' = (a, B, a'C)$ and g is properly equivalent to the form $g' = (a', B, aC)$. Equations (15) and (16) state that $B \equiv b \mod 2a$ and $B \equiv b' \mod 2a'$, so there exist integers k and k' such that

$$B = b + 2ak = b' + 2a'k'. \tag{21}$$

The Dirichlet composition of f and g is defined, so $\gcd(a, a', \frac{b+b'}{2}) = 1$. By Bézout's identity, there exist integers n_1, n_2 and n_3 such that

$$an_1 + a'n_2 + \frac{b + b'}{2}n_3 = 1.$$

Using Equation (21), we can write this as

$$an_1 + a'n_2 + \frac{B - 2ak + B - 2a'k'}{2}n_3 = a(n_1 - kn_3) + a'(n_2 - k'n_3) + Bn_3 = 1,$$

which shows that $\gcd(a, a', B) = 1$. Hence, the Dirichlet composition of f' and g' is defined. It is easy to check that B satisfies the congruences in Lemma 2.22, so

$$f' \circ g' = (aa', B, \frac{B^2 - D}{4aa'}) = (aa', B, C) = f \circ g.$$

Remark 2.26. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ be two arbitrary primitive positive definite forms of discriminant D. By Lemma 2.24, g properly represents an integer a' coprime to a. Then it follows from Lemma 2.7 that there exist integers b' and c' such that g is properly equivalent to the form $g'(x, y) = a'x^2 + b'xy + c'y^2$. The Dirichlet composition of f and g' is defined, because $\gcd(a, a') = 1$. Since g' is in the same equivalence class as g, this implies that the Dirichlet composition is defined for any pair of equivalence classes in the set $C(D)$.

The next lemma proves that the Dirichlet composition of any pair of equivalence classes in the set $C(D)$ is well-defined. This means that for any two equivalence classes $[f], [g] \in C(D)$, there exists an equivalence class $[h] \in C(D)$ such that for every $f' \in [f]$ and $g' \in [g]$ for which the Dirichlet composition $f' \circ g'$ is defined, $f' \circ g' \in [h]$. The proof of the lemma uses the symbol $\sim$ to denote "is properly equivalent to". Furthermore, a form $ax^2 + bxy + cy^2$ is again denoted by (a, b, c). The proof of this lemma is based on [8, Section 7.3].

Lemma 2.27. The Dirichlet composition on any pair of equivalence classes in the set $C(D)$ is well-defined.

Proof. Let

$$\begin{aligned} f_1 = (a, b, c), \quad g_1 = (a', b', c'), \\ f_2 = (u, v, w), \quad g_2 = (u', v', w'), \end{aligned} \tag{22}$$

be primitive positive definite forms of discriminant D. Assume that $f_1 \sim f_2$, $g_1 \sim g_2$ and the Dirichlet compositions $f_1 \circ g_1$ and $f_2 \circ g_2$ are defined. We showed in the proof of Theorem 2.25 that we can replace the functions in (22) by

$$\begin{aligned} f_1 = (a, B, a'C), \quad g_1 = (a', B, aC), \\ f_2 = (u, V, u'W), \quad g_2 = (u', V, uW), \end{aligned} \tag{23}$$

which have exactly the same properties. We will continue the proof using the functions in (23). We have

$$F_1 = f_1 \circ g_1 = (aa', B, \frac{B^2 - D}{4aa'}) = (aa', B, C),$$

where B is the unique integer modulo $2aa'$ of Lemma 2.22, and

$$F_2 = f_2 \circ g_2 = (uu', V, \frac{V^2 - D}{4uu'}) = (uu', V, W),$$

where V is the unique integer modulo $2uu'$ of Lemma 2.22. In the next four steps we will show that $F_1 \sim F_2$.

Step 1. Suppose that $f_1 = f_2$, $\gcd(a, u') = 1$ and $B = V$. Then $(a, B, a'C) = (u, B, u'W)$, which implies that $a = u$. We want to show that $f_1 \circ g_1 \sim f_1 \circ g_2$, so $(aa', B, C) \sim (au', B, W)$. The matrices

$$\begin{pmatrix} a' & \frac{B}{2} \\ \frac{B}{2} & aC \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} u' & \frac{B}{2} \\ \frac{B}{2} & aW \end{pmatrix}$$

represent the forms g_1 and g_2 respectively. Since $g_1 \sim g_2$, there exist integers p, q, r, s such that

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a' & \frac{B}{2} \\ \frac{B}{2} & aC \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix}^T = \begin{pmatrix} u' & \frac{B}{2} \\ \frac{B}{2} & aW \end{pmatrix}, \qquad ps - qr = 1. \tag{24}$$

Then it holds that

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a' & \frac{B}{2} \\ \frac{B}{2} & aC \end{pmatrix} = \begin{pmatrix} u' & \frac{B}{2} \\ \frac{B}{2} & aW \end{pmatrix} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}.$$

We can perform the matrix multiplication on both sides of the equation and compare the upright coefficients of the resulting matrices. This gives $p\frac{B}{2} + arC = -qu' + p\frac{B}{2}$, which simplifies to $arC = -qu'$. It follows that $a|qu'$. We assumed that $\gcd(a, u') = 1$, so by Bézout's identity there exist integers s and t such that $as + u't = 1$. If we multiply both sides of this equation by q, we get that $qas + qu't = q$. It is clear that $a|qas$ and moreover $a|qu'$, which implies that $a|qas + qu't = q$ and $\frac{q}{a}$ is an integer. Hence the matrix

$$\begin{pmatrix} p & ra \\ \frac{q}{a} & s \end{pmatrix}$$

has integer coefficients.

If we explicitly compute the matrix on the left-hand side of Equation (24), we get

$$\begin{pmatrix} a'p^2 + prB + ar^2C & a'pq + qr\frac{B}{2} + ps\frac{B}{2} + arsC \\ a'pq + ps\frac{B}{2} + qr\frac{B}{2} + arsC & a'q^2 + qsB + as^2C \end{pmatrix} = \begin{pmatrix} u' & \frac{B}{2} \\ \frac{B}{2} & aW \end{pmatrix}.$$

Using the equalities obtained by comparing the coefficients of the matrices in the equation above, we can show that

$$\begin{aligned} \begin{pmatrix} p & ra \\ \frac{q}{a} & s \end{pmatrix} \begin{pmatrix} aa' & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} \begin{pmatrix} p & ra \\ \frac{q}{a} & s \end{pmatrix}^T &= \begin{pmatrix} a(a'p^2 + prB + ar^2C) & a'pq + qr\frac{B}{2} + ps\frac{B}{2} + arsC \\ a'pq + ps\frac{B}{2} + qr\frac{B}{2} + arsC & \frac{1}{a}(a'q^2 + Bqs + as^2C) \end{pmatrix} \\ &= \begin{pmatrix} au' & \frac{B}{2} \\ \frac{B}{2} & W \end{pmatrix}. \end{aligned}$$

Note that $\det \begin{pmatrix} p & ra \\ q & s \\ a & \end{pmatrix} = ps - qr = 1$. Hence, the above computation shows that $(aa', B, C) \sim (au', B, W)$, so $f_1 \circ g_1 \sim f_1 \circ g_2$.

Step 2. Suppose that $g_1 = g_2$, $\gcd(a, u') = 1$ and $B = V$. Then applying the same argument used in Step 1, we can show that $g_2 \circ f_1 \sim g_2 \circ f_2$. Hence, combining the results of Step 1 and Step 2 gives

$$f_1 \circ g_1 \sim f_1 \circ g_2 \sim g_2 \circ f_1 \sim g_2 \circ f_2 \sim f_2 \circ g_2.$$

Step 3. In Step 1 and Step 2, we have shown that $f_1 \circ g_1 \sim f_2 \circ g_2$ under the assumption that $B = V$. We now drop this assumption. Assume that $\gcd(aa', uu') = 1$. Then either aa' and uu' are both odd or one of aa' and uu' is even. If aa' and uu' are both odd, then $\gcd(2aa', uu') = 1$. If one of aa' and uu' is even, then without loss of generality we can assume that aa' is even (otherwise switch the roles of aa' and uu' in this step). It follows that $\gcd(2aa', uu') = 1$. By the Chinese Remainder Theorem, there is an integer B^* that satisfies the equations

$$x \equiv B \mod 2aa' \qquad \text{and} \qquad x \equiv V \mod uu'.$$

Then there exist integers n_1 and m such that

$$B^* = B + 2aa'n_1 = V + uu'm.$$

Since F_1 and F_2 have the same discriminant, the parity of B and V is the same. This implies that the integer m must be even, so we write $m = 2n_2$. Thus,

$$B^* = B + 2aa'n_1 = V + 2uu'n_2.$$

The transformation $(x, y) \mapsto (x + a'n_1y, y)$ takes $f_1 = (a, B, a'C)$ to $\tilde{f}_1 = (a, B^*, C_1)$, where $C_1 = aa'^2n_1^2 + Ba'n_1 + a'C$ and the transformation $(x, y) \mapsto (x + an_1y)$ takes $g_1 = (a', B, aC)$ to $\tilde{g}_1 = (a', B^*, C_1')$, where $C_1' = a^2a'n_1^2 + Ban_1 + aC$. Clearly, we have that $f_1 \sim \tilde{f}_1$ and $g_1 \sim \tilde{g}_1$.

We want to find an expression for $\tilde{f}_1 \circ \tilde{g}_1$. First we note that the integer B^* satisfies (15), (16) and (17) in Lemma 2.22. Therefore, $\tilde{f}_1 \circ \tilde{g}_1 = (aa', B^*, C_1^*)$, where

$$\begin{aligned} C_1^* &= \frac{B^{*2} - D}{4aa'} \\ &= \frac{(B + 2aa'n_1)^2 - (B^2 - 4aa'C)}{4aa'} \\ &= aa'n_1^2 + Bn_1 + C. \end{aligned}$$

The transformation $(x, y) \mapsto (x + n_1y, y)$ takes $F_1 = (aa', B, C)$ to

$$(aa', B + 2aa'n_1, aa'n_1^2 + Bn_1 + C) = (aa', B^*, C_1^*).$$

This shows that $F_1 \sim \tilde{f}_1 \circ \tilde{g}_1$.

The transformation $(x, y) \mapsto (x + u'n_2y, y)$ takes $f_2 = (u, V, u'W)$ to $\tilde{f}_2 = (u, B^*, C_2)$, where $C_2 = uu'^2n_2 + Vu'n_2 + u'W$, and the transformation $(x, y) \mapsto (x + un_2y, y)$ takes $g_2 = (u', V, uW)$ to $\tilde{g}_2 = (u', B^*, C_2')$, where $C_2' = u^2u'n_2^2 + Vun_2 + uW$. Clearly, we have $f_2 \sim \tilde{f}_2$ and $g_2 \sim \tilde{g}_2$.

We want to find an expression for $\tilde{f}_2 \circ \tilde{g}_2$. First we note that the integer B^* satisfies (15), (16) and (17) in Lemma 2.22. Therefore, $\tilde{f}_2 \circ \tilde{g}_2 = (aa', B^*, C_2^*)$, where

$$\begin{aligned} C_2^* &= \frac{B^{*2} - D}{4uu'} \\ &= \frac{(V + 2uu'n_2)^2 - (V^2 - 4uu'W)}{4uu'} \\ &= uu'n_2 + Vn_2 + W. \end{aligned}$$

The transformation $(x, y) \mapsto (x + n_2y, y)$ takes $F_2 = (uu', V, W)$ to

$$(uu', V + 2uu'n_2, uu'n_2^2 + Vn_2 + W) = (uu', B^*, C_2^*).$$

This shows that $F_2 \sim \tilde{f}_2 \circ \tilde{g}_2$. Note that the middle coefficient of $\tilde{f}_1$, $\tilde{g}_1$, $\tilde{f}_2$ and $\tilde{g}_2$ is B^*. If we assume that $\gcd(a, u') = 1$, then the argument used in Step 1 shows that $\tilde{f}_1 \circ \tilde{g}_1 \sim \tilde{f}_1 \circ \tilde{g}_2$ and $\tilde{g}_2 \circ \tilde{f}_1 \sim \tilde{g}_2 \circ \tilde{f}_2$. It follows that

$$F_1 \sim \tilde{f}_1 \circ \tilde{g}_1 \sim \tilde{f}_1 \circ \tilde{g}_2 \sim \tilde{g}_2 \circ \tilde{f}_1 \sim \tilde{g}_2 \circ \tilde{f}_2 \sim \tilde{f}_2 \circ \tilde{g}_2 \sim F_2.$$

Step 4. In this last step, we will show that for any f_1, g_1, f_2, and g_2 as given at the beginning of this proof, we can always put ourselves in the situation of Step 3. Following the argument given in Step 3, then shows that $f_1 \circ g_1 \sim f_2 \circ g_2$. By Lemma 2.24, we know that f_1 properly represents an integer s coprime to $aa'uu'$. It follows from Lemma 2.7 that there exist integer B' and C' such that the form $f = (s, B', C')$ is properly equivalent to f_1. In the same way, g_1 properly represents an integer s' coprime to $aa'uu's$ and there exist integers B" and C" such that the form $g = (s', B", C")$ is properly equivalent to g_1. From the statements $\gcd(s, aa'uu') = 1$ and $\gcd(s', aa'uu's) = 1$, it can be easily proven that $\gcd(ss', aa') = \gcd(ss', uu') = \gcd(s, a') = \gcd(s, u') = 1$ using Bézout's identity. In Step 3, we have shown that $f_1 \circ g_1 \sim f_2 \circ g_2$ assuming that $gcd(aa', uu') = 1$ and $\gcd(a, u') = 1$. Therefore, we can apply the argument in Step 3 to prove that $f \circ g \sim f_1 \circ g_1$ and $f \circ g \sim f_2 \circ g_2$. Hence,

$$f_1 \circ g_1 \sim f \circ g \sim f_2 \circ g_2. \qquad \square$$

We have proven that Dirichlet composition is a well-defined operation on the set $C(D)$. We are now ready to prove that the set $C(D)$ with the operation induced by Dirichlet composition makes this set into a finite Abelian group. The proof of this theorem follows both [7, Theorem 3.9] and [8, Section 7.2].

Theorem 2.28. Let $D \equiv 0, 1 \mod 4$ be negative. Then Dirichlet composition induces a well-defined binary operation on $C(D)$ which makes $C(D)$ into a finite Abelian group. The identity element is the class containing the form

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

which is called the principal form. The inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing the form $ax^2 - bxy + cy^2$.

Proof. Theorem 2.25 states that the Dirichlet composition of two primitive positive definite forms of discriminant D is itself a primitive positive definite form of discriminant D. Furthermore, Lemma 2.27 states that Dirichlet composition is well-defined on the set $C(D)$. It follows that the set $C(D)$ is closed under Dirichlet composition.

Let $[f]$ be the class containing the form $f = (a, b, c)$. Since the first coefficient of the principal form is 1, the Dirichlet composition of f with the principal form is defined. Taking $B = b$ satisfies Equations (15), (16) and (17) in Lemma 2.22. Namely, if $D \equiv 0 \mod 4$, then D is even and hence b is even, so $b \equiv 0 \mod 2$. If $D \equiv 1 \mod 4$, then D is odd and hence b is odd, so $b \equiv 1 \mod 2$. This shows that Equation (16) is satisfied. It is clear that Equation (15) is satisfied and $D = b^2 - 4ac \equiv b^2 \mod 4a$ shows that also Equation (17) is satisfied. Then the Dirichlet composition of f and the principal form is

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

which shows that the principal form is indeed the identity element.

Let $[f]$ be the class containing the form $f = (a, b, c)$ and $[g]$ be the class containing the form $g = (a, -b, c)$. We want to show that $[g]$ is the inverse of $[f]$. Since $\gcd(a, a, \frac{b-b}{2}) = a$, which might be larger than 1, the Dirichlet composition of f and g might not be defined. The transformation $(x, y) \mapsto (-y, x)$ takes g to $g' = (c, b, a)$. Note that $g' \sim g$ and $\gcd(a, c, \frac{b+b}{2}) = \gcd(a, b, c) = 1$, because f is primitive. Hence, the Dirichlet composition of f and g' is defined. It is easy to check that taking $B = b$ satisfies Equations (15), (16) and (17) in Lemma 2.22. Then

$$f \circ g' = \left(ac, b, \frac{b^2 - D}{4ac}\right) = (ac, b, 1).$$

The transformation $(x, y) \mapsto (-y, x)$ takes $f \circ g'$ to $(1, -b, ac)$, so $f \circ g'$ and $(1, -b, ac)$ are properly equivalent. It remains to show that $f \circ g'$ is equivalent to the principal form. If $D \equiv 0 \mod 4$, then D and hence b is even, so $\frac{b}{2}$ is an integer. Then the transformation

$(x, y) \mapsto (x + \frac{b}{2}y, y)$ takes $(1, -b, ac)$ to

$$\begin{aligned}\left(x + \frac{b}{2}y\right)^2 - b\left(x + \frac{b}{2}\right)y + acy^2 &= x^2 + (b-b)xy + \left(\frac{b^2}{4} - \frac{b^2}{2} + ac\right)y^2 \\ &= x^2 + \left(\frac{-b^2 + 4ac}{4}\right)y^2 \\ &= x^2 - \frac{D}{4}y^2.\end{aligned}$$

Hence, $f \circ g'$ is properly equivalent to the principal form.

If $D \equiv 0 \mod 4$, then D and hence b is odd, so $\frac{b+1}{2}$ is an integer. Then the transformation $(x, y) \mapsto (x + \frac{b+1}{2}y, y)$ takes $(1, -b, ac)$ to

$$\begin{aligned}\left(x + \frac{b+1}{2}y\right)^2 - b\left(x + \frac{b+1}{2}y\right)y + acy^2 &= x^2 + (b+1-b)xy \\ &\quad + \left(\frac{(b+1)^2}{4} - \frac{b(b+1)}{2} + ac\right)y^2 \\ &= x^2 + xy + \left(\frac{-b^2 + 1 + 4ac}{4}\right)y^2 \\ &= x^2 + xy + \frac{-D+1}{4}y^2.\end{aligned}$$

Hence, $f \circ g'$ is properly equivalent to the principal form.

Let $[f]$, $[g]$ and $[h]$ be equivalence classes in $C(D)$. Let $f = (a, b, c)$. Then g properly represents an integer a' coprime to $2a$ by Lemma 2.24. It follows from Lemma 2.7 that there exist integers b' and c' such that g is properly equivalent to $g' = (a', b', c')$. Similarly, h is properly equivalent to a form $h' = (a'', b'', c'')$ with $\gcd(a'', 2aa') = 1$. It follows that $\gcd(a'', 2a) = \gcd(a'', a') = 1$. The Chinese Remainder Theorem implies that there exists an integer B satisfying

$$\begin{aligned}B &\equiv b \mod 2a, \\ B &\equiv b' \mod a', \\ B &\equiv b'' \mod a''.\end{aligned}$$

There exist integers k, l and m such that

$$B = b + 2ak = b' + a'l = b'' + a''m.$$

The forms f, g' and h' have the same discriminant, so b, b' and b'' all have the same parity. Therefore, $a'l$ and $a''m$ have to be even. The integers a' and a'' are odd, because $\gcd(a', 2a) = 1$ and $\gcd(a'', 2a) = 1$. Hence, l and m are even. We can thus write

$$B = b + 2ak = b' + 2a'l' = b'' + 2a''m',$$

for some $l', m' \in \mathbb{Z}$. We have the following transformations:

$$\begin{aligned}(x,y) \mapsto (x+ky,y) : f \mapsto \tilde{f} = (a,B,c_1), \text{ where } c_1 = ak^2 + bk + c,\\ (x,y) \mapsto (x+l'y,y) : g' \mapsto \tilde{g} = (a',B,c_2), \text{ where } c_2 = a'l'^2 + b'l' + c',\\ (x,y) \mapsto (x+m'y,y) : h' \mapsto \tilde{h} = (a'',B,c_3), \text{ where } c_3 = a''m'^2 + b''m' + c''.\end{aligned}$$

It is clear that $f \sim \tilde{f}$, $g' \sim \tilde{g}$ and $h' \sim \tilde{h}$. We have

$$\begin{aligned}\tilde{f} \circ \tilde{g} = (aa', B, C), \text{ where } C = \frac{B^2 - D}{4aa'},\\ \tilde{g} \circ \tilde{h} = (a'a'', B, C'), \text{ where } C' = \frac{B^2 - D}{4a'a''}.\end{aligned}$$

Moreover,

$$\begin{aligned}(\tilde{f} \circ \tilde{g}) \circ \tilde{h} = (aa'a'', B, C_1), \text{ where } C_1 = \frac{B^2 - D}{4aa'a''},\\ \tilde{f} \circ (\tilde{g} \circ \tilde{h}) = (aa'a'', B, C_2), \text{ where } C_2 = \frac{B^2 - D}{4aa'a''}.\end{aligned}$$

This shows that $([f] \circ [g]) \circ [h] = [f] \circ ([g] \circ [h])$ and hence Dirichlet composition is associative. This concludes the proof that the set $C(D)$ provided with Dirichlet composition is a finite Abelian group. □

3 Quadratic fields

A *quadratic field* is a subfield of the complex numbers which has dimension two as a vector space over the rational numbers. Quadratic fields have the form

$$\mathbb{Q}(\sqrt{N}) = \mathbb{Q}[\sqrt{N}] = \{a + b\sqrt{N} : a, b \in \mathbb{Q}\},$$

where $N \neq 0, 1$ is a squarefree integer. A field $\mathbb{Q}(\sqrt{N})$ is called a *real quadratic field* if $N > 0$ and an *imaginary quadratic field* if $N < 0$.

Definition 3.1. The *discriminant* d_K of a quadratic field $K = \mathbb{Q}(\sqrt{N})$ is

$$d_K = \begin{cases} N & \text{if } N \equiv 1 \mod 4, \\ 4N & \text{otherwise.} \end{cases}$$

Note that a quadratic field K can be written in terms of its discriminant as $\mathbb{Q}(\sqrt{d_K})$.

3.1 Algebraic integers

Definition 3.2. A complex number is called an *algebraic integer* if it is the root of a monic polynomial with integer coefficients.

Theorem 3.3 ([9, Theorem 2])**.** The following are equivalent for $\alpha \in \mathbb{C}$:

1. α is an algebraic integer in a quadratic field;
2. The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated;
3. There exists a subring of $\mathbb{C}$ with a finitely generated additive group having α as a member;
4. $\alpha A \subset A$ for some finitely generated additive subgroup $A \subset \mathbb{C}$.

Proof.
(**1**) $\implies$ (**2**) Assume that α is an algebraic integer. Then there exists a monic polynomial with integer coefficients having α as a root. Let n be the degree of this polynomial. Note that $n \leq 2$ as α is an element in a quadratic field. Then the additive group of the ring $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$.

(**2**) $\implies$ (**3**) The subring of $\mathbb{C}$ with a finitely generated additive group having α as a member is the ring $\mathbb{Z}[\alpha]$.

(**3**) $\implies$ (**4**) Let A be the subring of C with a finitely generated additive group having α as a member. Then clearly $\alpha A \subset A$ and A is a finitely generated additive group.

(**4**) $\implies$ (**1**) Let $a_1, a_2, \ldots, a_n$ generate A. Then we can express each αa_i, for $i = 1, \ldots, n$, as a linear combination

$$\alpha a_i = m_{i1}a_1 + m_{i2}a_2 + \cdots + m_{in}a_n,$$

where $m_{i1}, \ldots, m_{in} \in \mathbb{Z}$. We can write this as

$$\begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ \vdots \\ \alpha a_n \end{pmatrix} = \underbrace{\begin{pmatrix} m_{11} & m_{12} & \ldots & m_{1n} \\ m_{21} & m_{22} & \ldots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \ldots & m_{nn} \end{pmatrix}}_{M} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

It follows that

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the a_i, $i = 1, \ldots, n$ are not all zero, this equation implies that α is an eigenvalue of M and hence the determinant of $\alpha I - M$ is zero. If we compute the determinant in terms of the coefficients of $\alpha I - M$, we get an expression of the form

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$

where $c_{n-1}, \ldots, c_1, c_0 \in \mathbb{Z}$. Hence, α is the root of a monic polynomial with integer coefficients. This shows that α is an algebraic integer. □

Definition 3.4. The set of algebraic integers in a quadratic field K is called the *ring of integers* and is denoted by $\mathcal{O}_K$.

Lemma 3.5 ([9, Chapter 2, Lemma])**.** Let $f \in \mathbb{Z}[X]$ be monic and suppose that $f = gh$ for monic polynomials $g, h \in \mathbb{Q}[X]$. Then actually $g, h \in \mathbb{Z}[X]$.

Proof. Let $m > 0$ be the smallest positive integer such that $mg \in \mathbb{Z}[X]$. Suppose that there exists an integer $a > 0$ dividing all the coefficients of mg. Since g is monic, the first coefficient of mg is m and it follows that a divides m. Hence, we have $\frac{m}{a}g \in \mathbb{Z}[X]$. The minimality of m implies that $a = 1$. Thus, the greatest common divisor of the coefficients of mg is one. Let $n > 0$ be the smallest positive integer such that $nh \in \mathbb{Z}[X]$. Then in the same way we can show that the greatest common divisor of the coefficients of nh is one.

Suppose that $mn > 1$ and let p be any prime dividing mn. We have $mnf = mg \cdot nh$. Reducing the coefficients modulo p of the polynomials on both side of the equation gives

$$\bar{0} = \bar{mg} \cdot \bar{nh},$$

where $\bar{mg}, \bar{nh} \in \mathbb{Z}/p\mathbb{Z}[X]$. Note that $\mathbb{Z}/p\mathbb{Z}[X]$ has no zero divisors as it is an integral domain. Therefore, $\bar{mg} = \bar{0}$ or $\bar{nh} = \bar{0}$ and hence p divides all coefficients of mg or all coefficiens of nh. However, we have shown that the greatest common divisor of the coefficients of mg and the coefficients of nh is one, which is a contradiction. Hence, we have $mn = 1$ and $g, h \in \mathbb{Z}[X]$. □

Theorem 3.6 ([9, Corollary 1 of Theorem 1])**.** The set of algebraic integers in $\mathbb{Q}$ is precisely $\mathbb{Z}$.

Proof. Let $\alpha \in \mathbb{Z}$. Then α is a root of the monic polynomial $x - \alpha \in \mathbb{Z}$ which shows that α is an algebraic integer.

Let $\alpha \in \mathbb{Q}$ be an algebraic integer. Then α is the root of the monic irreducible polynomial $g(x) = x - \alpha \in \mathbb{Q}[X]$. As α is an algebraic integer, we know that α satisfies a monic polynomial with integer coefficients. Let $f \in \mathbb{Z}[X]$ be the monic polynomial of least

degree having α as a root. Note that the degree of f is either 1 or 2, because K is a quadratic field. Suppose f has degree 2. Dividing f by g gives

$$f(x) = g(x)q(x) + r(x), \text{ where } q(x), r(x) \in \mathbb{Q}[X] \text{ and } \deg r < \deg g.$$

The degree of g is 1. It follows that the degree of r is 0 and hence r is constant. If we fill in α in the above equation, we get $r(\alpha) = 0$, which implies that $r(x) = 0$. Hence $f(x) = g(x)q(x)$, where g and q are monic. Lemma 3.5 implies that $g, q \in \mathbb{Z}[X]$. However, α must be a root of either g or q and both have degree less than f. This is a contradiction. Hence f must have degree 1 and is therefore irreducible. Since the monic irreducible polynomial having α as a root is unique, we get $f(x) = x - \alpha$, which is only possible if $\alpha \in \mathbb{Z}$. Hence, the algebraic integers in $\mathbb{Q}$ are precisely the integers and the statement holds. □

The goal is to prove the following theorem, which describes exactly what the ring of integers in a quadratic field looks like.

Theorem 3.7 ([9, Corollary 2 of Theorem 1])**.** The set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{N})$, with N squarefree, is

$$\begin{cases} \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \mod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{N}}{2}\right] & \text{if } N \equiv 1 \mod 4. \end{cases}$$

The proof will be given in section 3.3, but first we will explain the norm and the trace.

3.2 The norm and the trace

Let $K = \mathbb{Q}(\sqrt{N})$ be a quadratic field and let $\alpha \in K \backslash \mathbb{Q}$. Then there exist $r, s \in \mathbb{Q}$ with $s \neq 0$, such that $\alpha = r + s\sqrt{N}$. Note that α is a root of the monic polynomial

$$x^2 - 2rx + r^2 - Ns^2 \in \mathbb{Q}[X]. \tag{25}$$

Definition 3.8. The *norm* of $\alpha = r + s\sqrt{N} \in K$ is $\alpha\bar{\alpha}$, where we call $\bar{\alpha} = r - s\sqrt{N}$ the *conjugate* of α. We denote the norm of α by $N(\alpha)$. Note that in case $N < 0$, the conjugate of α coincides with the complex conjugate.

Computing the norm of α gives $N(\alpha) = r^2 - s^2N$.

Definition 3.9. The *trace* of α is $\alpha + \bar{\alpha}$, which we denote by $T(\alpha)$.

Computing the trace of α gives $T(\alpha) = 2r$. Thus, the polynomial in (25) becomes

$$x^2 - T(\alpha)x + N(\alpha) \in \mathbb{Q}[X].$$

If $N(\alpha)$ and $T(\alpha)$ are integers, then α is the root of a monic polynomial with integer coefficients and hence an algebraic integer. We will show that the converse holds as well.

The next theorem is stated in the proof of [9, Corollary 2 of Theorem 1]. We need this theorem to prove Theorem 3.7.

Theorem 3.10. The element $\alpha \in K$ is an algebraic integer if and only if $N(\alpha)$ and $T(\alpha)$ are integers.

Proof. We still have to show the "only if" part. First note that if $\alpha \in \mathbb{Q}$, then Theorem 3.6 shows that $\alpha \in \mathbb{Z}$. In this case $N(\alpha)$ and $T(\alpha)$ are integers.

Assume $\alpha = r + s\sqrt{N}$, where $s \neq 0$, is an algebraic integer. Then α satisfies a monic polynomial with integer coefficients. Let $f \in \mathbb{Z}[X]$ be the monic polynomial of least degree having α as a root. Then f is irreducible in $\mathbb{Z}[X]$. Since f is monic, f is also irreducible in $\mathbb{Q}[X]$.

Note that the degree of f is two. We have already seen that the minimal polynomial of α is $x^2 - T(\alpha)x + N(\alpha)$ and hence this polynomial is irreducible. Since the monic irreducible polynomial having α as a root is unique, we get $f(x) = x^2 - T(\alpha)x + N(\alpha)$, which is only possible if $T(\alpha)$ and $N(\alpha)$ are integers. This proves the theorem. □

3.3 The ring of integers

Lemma 3.11 ([9, Chapter 2, Exercise 25])**.** Let $\mathbb{Q}(\sqrt{N})$ be a quadratic field. For every $x \in \mathbb{Q}(\sqrt{N})$, there exists a nonzero $m \in \mathbb{Z}$ such that $mx \in \mathcal{O}_K$.

Proof. Let $x \in \mathbb{Q}(\sqrt{N})$. We can find $p, q, r, s \in \mathbb{Z}$ such that $x = \frac{p}{q} + \frac{r}{s}\sqrt{N}$. Note that p and s are nonzero. Then the polynomial

$$x^2 - 2\frac{p}{q}x + \frac{p^2}{q^2} - \frac{r^2}{s^2}N$$

has $\frac{p}{q} + \frac{r}{s}\sqrt{N}$ as a root. If we multiply this polynomial by q^2s^2, we get the polynomial

$$q^2s^2x^2 - 2pqs^2x + p^2s^2 - r^2q^2N,$$

with integer coefficients and still having $\frac{p}{q} + \frac{r}{s}\sqrt{N}$ as a root. Note that $qs(\frac{p}{q} + \frac{r}{s}\sqrt{N})$ satisfies a monic polynomial with integer coefficients, since

$$(qs(\frac{p}{q} + \frac{r}{s}\sqrt{N}))^2 - 2ps(qs(\frac{p}{q} + \frac{r}{s}\sqrt{N})) + p^2s^2 - r^2q^2N = 0.$$

Hence $qs(\frac{p}{q} + \frac{r}{s}\sqrt{N})$, with qs nonzero, is an algebraic integer. □

The first paragraph of the proof of the following theorem follows [9, Corollary 1 of Theorem 2].

Theorem 3.12. Let K be a quadratic field. The ring of integers $\mathcal{O}_K$ is a subring of K whose field of fractions is K.

Proof. Suppose α and β are elements in $\mathcal{O}_K$. By part 2 of Theorem 3.3, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated additive groups. Let $\{a_1, \dots a_n\}$ be the set of generators for $\mathbb{Z}[\alpha]$ and $\{b_1, \dots b_m\}$ be the set of generators for $\mathbb{Z}[\beta]$. Then the products $a_i b_j$ for $i = 1, \dots, n$ and $j = 1, \dots, m$ generate the additive group $\mathbb{Z}[\alpha, \beta]$. Note that $\alpha + \beta$ and $\alpha\beta$ are elements of the ring $\mathbb{Z}[\alpha, \beta]$. It follows from part 3 of Theorem 3.3 that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers and hence also elements of $\mathcal{O}_K$. This shows that $\mathcal{O}_K$ is a subring of K.

Let $x \in K$. It follows from Lemma 3.11 that there exists an integer $m \in \mathbb{Z}$ such that $mx \in \mathcal{O}_K$. Hence, $x = \frac{mx}{m}$, which shows that x is in the field of fractions of $\mathcal{O}_K$. Thus, we have shown that K is contained in the field of fractions of $\mathcal{O}_K$. Since the field of fractions of $\mathcal{O}_K$ is the smallest field containing $\mathcal{O}_K$, it follows that K is the field of fractions of $\mathcal{O}_K$. □

We are now ready to prove Theorem 3.7.

Proof. Let $\alpha \in \mathbb{Q}(\sqrt{N})$. Then there exist $r, s \in \mathbb{Q}$ such that $\alpha = r + s\sqrt{N}$. Theorem 3.10 shows that α is an algebraic integer if and only if $N(\alpha) = r^2 - s^2 N$ and $T(\alpha) = 2r$ are integers.

Assume that $r^2 - s^2 N$ and $2r$ are integers and let $r^2 - s^2 N = k$. Then

$$4Ns^2 = 4r^2 - 4k = (2r)^2 - 4k \in \mathbb{Z}.$$

Suppose that $2s = \frac{p}{q}$, with $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Then

$$(2s)^2 N = \frac{p^2}{q^2} N \in \mathbb{Z},$$

which implies that $q = 1$ or $\frac{N}{q^2} \in \mathbb{Z}$. Remember that N is a squarefree integer so that $\frac{N}{q^2} \notin \mathbb{Z}$. Hence, we have $q = 1$ and $2s \in \mathbb{Z}$.

Define $m \coloneqq 2r$ and $n \coloneqq 2s$. We have shown above that $m, n \in \mathbb{Z}$ if α is an algebraic integer. Then $m^2 - Nn^2 = 4r^2 - 4Ns^2$, so we have

$$r^2 - Ns^2 \in \mathbb{Z} \iff 4 | m^2 - Nn^2.$$

This implies that α is an algebraic integer if and only if $m, n \in \mathbb{Z}$ and $4|m^2 - Nn^2$. First assume that $N \equiv 2, 3 \mod 4$. It follows that $4|m^2 + Nn^2$ if and only if m and n are even. Moreover, m and n are even precisely when r and s are integers. Hence, α is an algebraic integer if and only if $r, s \in \mathbb{Z}$, so the set of algebraic integers in $\mathbb{Q}(\sqrt{N})$ is $\mathbb{Z}[\sqrt{N}]$.

Next assume that $N \equiv 1 \mod 4$. Note that N is squarefree, which implies that $N \not\equiv 0 \mod 4$. Then $m^2 - Nn^2 \equiv m^2 - n^2 \mod 4$. It holds that $4|m^2 - n^2$ if and only if m and n have the same parity. Note that

$$\alpha = r + s\sqrt{N} = \frac{m + n\sqrt{N}}{2} = \frac{m+n}{2} + n\left(\frac{-1+\sqrt{N}}{2}\right).$$

Since m and n have the same parity, $\frac{m+n}{2}$ is an integer. It follows that the set of algebraic integers is contained in the set $\mathbb{Z}[\frac{-1+\sqrt{N}}{2}]$. To show that the ring of integers is equal to $\mathbb{Z}[\frac{-1+\sqrt{N}}{2}]$, note that we can write $N = 4k + 1$ for some $k \in \mathbb{Z}$, as $N \equiv 1 \mod 4$. Then $\frac{-1+\sqrt{N}}{2}$ is a root of the monic polynomial $x^2 + x - k \in \mathbb{Z}[X]$ and hence $\frac{-1+\sqrt{N}}{2}$ is an algebraic integer. It follows from Theorem 3.12 that $\mathbb{Z}[\frac{-1+\sqrt{N}}{2}]$ is contained in the set of algebraic integers of $\mathbb{Q}(\sqrt{N})$, which proves the theorem. □

Remark 3.13. The ring of integers $\mathcal{O}_K$ of a quadratic field K can be written in terms of the discriminant d_K of K as

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right].$$

Corollary 3.14. Let K be a quadratic field. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank two.

3.4 Dedekind domains

Lemma 3.15 ([9, Chapter 2, Exercise 24])**.** A subgroup H of a free Abelian group G of rank n is a free Abelian group of rank $\leq n$.

Proof. The proof uses induction. First assume that $n = 1$. Then $G \cong \mathbb{Z}$, so the subgroups of G are isomorphic to the subgroups of $\mathbb{Z}$, which are $\{0\}$ and $n\mathbb{Z}$, where $n \in \mathbb{Z}$. Note that $\{0\}$ is a free Abelian group of rank 0 and $n\mathbb{Z}$ is a free Abelian group of rank 1. Hence, the result holds for $n = 1$.

Assume that the result holds for $n - 1$. Let $\{x_1, \ldots, x_n\}$ be the set of generators for G. Then every element $x \in G$ can be written as $x = a_1x_1 + \cdots + a_nx_n$, for some $a_1, \ldots, a_n \in \mathbb{Z}$. Consider the projection on the first component $\pi : G \to \mathbb{Z}$ given by

$$a_1x_1 + \cdots + a_nx_n \mapsto a_1.$$

Let K be the kernel of π. Then $x_2, \ldots, x_n$ generate K and hence K is a free Abelian group of rank $n-1$. Note that $H \cap K$ is a subgroup of K and by the induction hypothesis $H \cap K$ is a free Abelian group of rank $\leq n-1$.

The set $\pi(H)$ is a subgroup of $\mathbb{Z}$, so $\pi(H)$ is either $\{0\}$ or of the form $k\mathbb{Z}$ for some $k \in \mathbb{Z}$. If $\pi(H) = \{0\}$, then $H = H \cap K$, which is a free Abelian group of rank $\leq n-1$. If $\pi(H) = k\mathbb{Z}$, then this means that every element $x \in H$ has its first component $a_1 \in k\mathbb{Z}$. Pick $h \in H$ such that $\pi(h) = k$. Then every integer multiple of h has its first component in $k\mathbb{Z}$ and the set $h\mathbb{Z}$ is a subgroup of H. Note that $h\mathbb{Z}$ and $H \cap K$ have only the zero element in common. Moreover, we can write every element $y \in H$ as $y = rh + s$, where $r \in \mathbb{Z}$ and $s \in H \cap K$, which shows that $H = h\mathbb{Z} \oplus H \cap K$. The set $H \cap K$ is a free Abelian group of rank $\leq n-1$ and $h\mathbb{Z} \cong \mathbb{Z}$. Hence, H is a free Abelian group of rank $\leq n$. □

Lemma 3.16. Let A be a free $\mathbb{Z}$-module of rank n and B a free $\mathbb{Z}$-module such that $B \subset A$. Then the quotient A/B is finite if and only if A and B have the same rank.

Proof. Assume A/B is finite. Let $\{x_1, \ldots, x_n\}$ be a basis of A. Since A/B is finite, the elements $x_i + B \in A/B$, where $i = 1, \ldots, n$, have finite order. Thus, for $i = 1, \ldots, n$, there exist integers m_i such that $m_i x_i + B = 0$. This implies that $m_1 x_1, \ldots, m_n x_n \in B$. If the elements $m_1 x_1, \ldots, m_n x_n$ are linearly dependent over $\mathbb{Z}$, then $a_1 m_1 x_1 + \cdots + a_n m_n x_n = 0$ for some $a_1, \ldots, a_n \in \mathbb{Z}$ not all zero. This contradicts the fact that the elements $x_1, \ldots, x_n$ are linearly independent. Hence, B contains the linearly independent elements $m_1 x_1, \ldots, m_n x_n$, which implies that the rank of B is at least n. Moreover, the rank of B is at most n since $B \subset A$.

Assume A and B have the same rank. Let $\{x_1, \ldots, x_n\}$ be a basis of A. Since $B \subset A$, we can express any basis for B in terms of the basis for A. Hence, there exist $m_1, \ldots, m_n \in \mathbb{Z}$ such that $\{m_1 x_1, \ldots, m_n x_n\}$ is a basis for B. Let $x + B \in A/B$. Then $m_1 \cdot \cdots \cdot m_n (x + B) = B$, which shows that every element in A/B has finite order. Hence, A/B is finite. □

Corollary 3.17 ([7, Exercise 5.1])**.** Let K be a quadratic field and I a nonzero ideal of $\mathcal{O}_K$. Then the quotient ring $\mathcal{O}_K/I$ is finite. Hence, I is a free $\mathbb{Z}$-module of rank 2.

Proof. Since I is a nonzero ideal, we can find a nonzero element $\alpha \in I$. Let $x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ be the minimal polynomial of α. Note that $a_n \neq 0$, otherwise the polynomial would not be minimal. It follows that

$$a_n = -\alpha^n - a_1 \alpha^{n-1} - \cdots - a_{n-1}\alpha \in I.$$

We can form the ideal $a_n \mathcal{O}_K \subset I$. Then the map

$$\mathcal{O}_K/a_n\mathcal{O}_K \to \mathcal{O}_K/I,$$
$$\alpha + a_n\mathcal{O}_K \mapsto \alpha + I.$$

is clearly surjective. By Corollary 3.14, we have $\mathcal{O}_K \cong \mathbb{Z}^2$. Therefore, $\mathcal{O}_K/a_n\mathcal{O}_K \cong (\mathbb{Z}/a_n\mathbb{Z})^2$ and hence $\mathcal{O}_K/a_n\mathcal{O}_K$ is finite. The surjective map given above, implies that the order of $\mathcal{O}_K/I$ is less than or equal to the order of $\mathcal{O}_K/a_n\mathcal{O}_K$. Thus, the quotient ring $\mathcal{O}_K/I$ is finite. The ideal I is a subgroup of the additive group of $\mathcal{O}_K$. By Lemma 3.14, $\mathcal{O}_K$ is a free Abelian group of rank 2. Then Lemma 3.16 implies that I is a free $\mathbb{Z}$-module of rank 2. □

Theorem 3.18 ([9, Theorem 14])**.** The ring of integers $\mathcal{O}_K$ in a quadratic field K is a *Dedekind domain*, which means that

1. $\mathcal{O}_K$ is integrally closed in K, i.e., if $\alpha \in K$ is the root of a monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$;
2. $\mathcal{O}_K$ is Noetherian, i.e., every ideal of $\mathcal{O}_K$ is finitely generated;
3. Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

Proof.

1. Suppose $a_0, \ldots, a_{n-1} \in \mathcal{O}_K$ and $\alpha \in \mathbb{C}$ satisfies
$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$
By part 2 of Theorem 3.3, the additive groups of the rings $\mathbb{Z}[a_0], \mathbb{Z}[a_1], \ldots, \mathbb{Z}[a_{n-1}]$ are finitely generated. Using induction, it follows that the additive group of the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}]$ is finitely generated. Let $\{g_1, \ldots, g_k\}$ be the generating set of the additive group of $\mathbb{Z}[a_0, \ldots, a_{n-1}]$. Then the products $g_i\alpha^j$ for $i = 1, \ldots, k$ and $j = 0, \ldots, n-1$ generate the additive group $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$. Clearly $\alpha \in \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$, so it follows from part 3 of Theorem 3.3 that α is an algebraic integer. Hence, $\mathcal{O}_K$ is integrally closed.
2. By Theorem 3.14, the ring $\mathcal{O}_K$ is a free Abelian group of rank two. Let I be an ideal of $\mathcal{O}_K$. Then I is a subgroup of $\mathcal{O}_K$. Hence, I is a free Abelian group of rank ≤ 2 by Lemma 3.15. It follows that I is finitely generated as an ideal.
3. Let P be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/P$ is an integral domain and moreover finite by Corollary 3.17. Let $\alpha \in \mathcal{O}_K/P$ be nonzero. Consider the sequence $\alpha, \alpha^2, \alpha^3, \ldots$. As $\mathcal{O}_K/P$ is finite, we must have $\alpha^n = \alpha^m$ for some $m, n \in \mathbb{N}$ such that $n < m$. Then
$$0 = \alpha^n - \alpha^m = \alpha^n(1 - \alpha^{m-n}).$$
The ring $\mathcal{O}_K/P$ is an integral domain and hence contains no zero divisors, so either $\alpha^n = 0$ or $1 - \alpha^{m-n} = 0$. For the same reason α^n is nonzero, because α is nonzero. Hence, $1 - \alpha^{m-n} = 0$, so $\alpha^{m-n} = \alpha \cdot \alpha^{m-n-1} = 1$, which shows that α is invertible. This shows that $\mathcal{O}_K/P$ is a field. It follows that P is maximal. □

3.5 Orders

Definition 3.19. An *order* $\mathcal{O}$ in a quadratic field K is a subset of K such that

1. $\mathcal{O}$ is a subring of K containing 1,
2. $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2.

Example 3.20. The ring of integers $\mathcal{O}_K$ of a quadratic field K is an order in K. The remark after Theorem 3.7 shows that $O_K = \mathbb{Z}[\frac{d_K+\sqrt{d_K}}{2}]$, which satisfies the conditions in Definition 3.19.

Theorem 3.21 ([7, §7A])**.** The ring of integers in a quadratic field K is the maximal order in K.

Proof. Let $\mathcal{O}$ be an order in K with basis $\{\alpha, \beta\}$. We can find $n, m \in \mathbb{Z}$ such that $n\alpha, m\beta \in \mathcal{O}_K$ by Lemma 3.11. Suppose that the elements $n\alpha$ and $m\beta$ are linearly dependent. Then there exist nonzero $u, v \in \mathbb{Z}$ such that $u \cdot n\alpha + v \cdot m\beta = 0$. This is not possible, since $\{\alpha, \beta\}$ forms a basis for $\mathcal{O}$ and hence α and β are linearly independent. Thus, $n\alpha$ and $m\beta$ are two linearly independent elements in $\mathcal{O}$, so $\{n\alpha, m\beta\}$ is also a basis for $\mathcal{O}$. This shows that $\mathcal{O} \subset \mathcal{O}_K$ and hence $\mathcal{O}_K$ is the maximal order in K. □

Definition 3.22. Let $\mathcal{O}$ be an order in a quadratic field K. Then $|\mathcal{O}_K/\mathcal{O}|$ is called the *conductor* of the order and is denoted by f.

Lemma 3.23 ([7, Lemma 7.2])**.** Let K be a quadratic field of discriminant d_K and $\mathcal{O}$ an order in K. Then the conductor f of $\mathcal{O}$ is finite and

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \left[1, f \cdot \frac{d_K + \sqrt{d_K}}{2}\right].$$

Proof. We have seen that $\mathcal{O}_K$ and $\mathcal{O}$ are free Abelian groups of rank 2, so it follows from Lemma 3.16 that f is finite. The quotient $\mathcal{O}_K/\mathcal{O}$ is an Abelian group with f elements. For every element $\alpha + \mathcal{O} \in \mathcal{O}_K/\mathcal{O}$, we have $f\alpha + \mathcal{O} = \mathcal{O}$, which shows that $f\mathcal{O}_K \subset \mathcal{O}$. By Definition 3.19, $1 \in \mathcal{O}$ and therefore $\mathbb{Z} \subset \mathcal{O}$. It follows that $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$. The remark after Theorem 3.7 shows that $\mathcal{O}_K = [1, \frac{d_K+\sqrt{d_K}}{2}]$, so $\mathbb{Z} + f\mathcal{O}_K = [1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$. It is clear that $[1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$ has index f in $\mathcal{O}_K$. We have

$$f = |\mathcal{O}_K/(\mathbb{Z} + f\mathcal{O}_K)| = |\mathcal{O}_K/\mathcal{O}||\mathcal{O}/(\mathbb{Z} + f\mathcal{O}_K)|$$

and $|\mathcal{O}_K/\mathcal{O}| = f$, which implies that $|\mathcal{O}/\mathbb{Z} + f\mathcal{O}_K| = 1$. Hence, $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$. □

Definition 3.24. Let $\mathcal{O} = [\alpha, \beta]$. Then the discriminant of $\mathcal{O}$ is the number

$$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}\right)^2,$$

where $\bar{\alpha}$ and $\bar{\beta}$ denote the conjugates of α and β respectively.

Remark 3.25. We have to prove that the discriminant of an order is well-defined. In other words, we have to show that the discriminant is independent of the integral basis used, see [7, Exercise 7.3(a)]. Let $\mathcal{O} = [\alpha, \beta] = [\eta, \mu]$. Then

$$\begin{aligned} \alpha &= n_1\eta + n_2\mu, & \bar{\alpha} &= \bar{\eta} + \bar{\mu}, \\ \beta &= m_1\eta + m_2\mu, & \bar{\beta} &= m_1\bar{\eta} + m_2\bar{\mu}, \end{aligned}$$

for some $n_1, n_2, m_1, m_2 \in \mathbb{Z}$. It follows that

$$\begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} = \begin{pmatrix} \eta & \mu \\ \bar{\eta} & \bar{\mu} \end{pmatrix} \underbrace{\begin{pmatrix} n_1 & m_1 \\ n_2 & m_2 \end{pmatrix}}_{M}.$$

Note that M is a nonsingular matrix since α and β are linearly independent. In exactly the same way, we have

$$\begin{pmatrix} \eta & \mu \\ \bar{\eta} & \bar{\mu} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} N,$$

where N is a nonsingular matrix with integer entries. Then

$$\begin{aligned} \left(\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}\right)^2 &= \left(\det \begin{pmatrix} \eta & \mu \\ \bar{\eta} & \bar{\mu} \end{pmatrix}\right)^2 (\det M)^2 \\ &= \left(\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}\right)^2 (\det N)^2 (\det M)^2, \end{aligned}$$

which shows that $(\det N)^2(\det M)^2 = 1$. Since M and N have integer coefficients, $\det N, \det M \in \mathbb{Z}$ and thus $\det M = \pm 1$ and $\det N = \pm 1$. This argument shows that matrices representing a change of basis always have determinant ± 1. Hence,

$$\left(\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}\right)^2 = \left(\det \begin{pmatrix} \eta & \mu \\ \bar{\eta} & \bar{\mu} \end{pmatrix}\right)^2,$$

which shows that the discriminant of an order is independent of the integral basis used.

In contrast to the ring of integers, orders that are not maximal are not Dedekind domains. It follows from the following corollary that orders are Noetherian and every prime ideal of an order is maximal.

Corollary 3.26. Let K be a quadratic field and I a nonzero ideal of $\mathcal{O}$. Then the quotient ring $\mathcal{O}/I$ is finite. Hence, I is a free $\mathbb{Z}$-module of rank 2.

Proof. The proof is exactly the same as the proof of Corollary 3.17. □

Using this corollary, it can be shown that orders are Noetherian in the same way as it was shown for the ring of integers. The same holds for the proof of the fact that every prime ideal of an order is maximal.

Orders are however not integrally closed, except for the maximal order. Suppose $\mathcal{O}$ is an order in a quadratic field K with conductor $f > 1$. Note that an order is the maximal order if and only if the conductor is one. Since $f > 1$, it holds that $\mathcal{O}_K \backslash \mathcal{O} \neq \emptyset$. Pick $\alpha \in \mathcal{O}_K \backslash \mathcal{O}$. Then α is an algebraic integer and hence satisfies a monic polynomial with integer coefficients. The integers are contained in $\mathcal{O}$, so α is the root of a monic polynomial with coefficients in $\mathcal{O}$. However, $\alpha \notin \mathcal{O}$ and therefore $\mathcal{O}$ is not integrally closed.

3.6 Ideal class group

Definition 3.27. Let $\mathcal{O}$ be an order in a quadratic field K. A subset of K which is a nonzero finitely generated $\mathcal{O}$-module is called a *fractional ideal* of $\mathcal{O}$.

Remark 3.28. If I is a fractional ideal of the order $\mathcal{O}$ in a quadratic field K and $\alpha \in K$, then αI is also a fractional ideal of the order $\mathcal{O}$. Namely, αI is a finitely generated $\mathcal{O}$-module, because I is a finitely generated $\mathcal{O}$-module.

Theorem 3.29 ([6, Theorem 2.3])**.** Let $\mathcal{O}$ be an order in a quadratic field K. Then I is a fractional ideal of $\mathcal{O}$ if and only if I is of the form αJ, where $\alpha \in K^\times$ and J is a nonzero ideal of $\mathcal{O}$.

Proof. Let I be a fractional ideal of $\mathcal{O}$. Then I is a finitely generated $\mathcal{O}$-module, so there exists a set $\{x_1, \ldots, x_n\} \in K$ such that $I = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$. By Lemma 3.11, we can find $d_i \in \mathbb{Z}$ such that $d_i x_i \in \mathcal{O}_K$ for $i = 1, \ldots, n$. Define $d \coloneqq d_1 \cdots d_n$. Using that $\mathcal{O} \in \mathcal{O}_K$, we get $dI \subset \mathcal{O}_K$. It follows that $fdI \in \mathcal{O}$, where f is the conductor of $\mathcal{O}$. Note that fdI is an $\mathcal{O}$-module contained in $\mathcal{O}$, so fdI is an ideal of $\mathcal{O}$. Hence, $I = \frac{1}{fd} \cdot fdI$, where $\frac{1}{fd} \in K^\times$.

Take $\alpha \in K^\times$ and J a nonzero ideal of $\mathcal{O}$. Corollary 3.26 implies that J is finitely generated as a $\mathbb{Z}$-module. It follows that J is finitely generated as an $\mathcal{O}$-module. Hence, αJ is a nonzero finitely generated $\mathcal{O}$-module. This proves the theorem. □

Definition 3.30. Let $\mathcal{O}$ be an order in a quadratic field K. Then a fractional ideal I of $\mathcal{O}$ is called *proper* if

$$\mathcal{O} = \{\beta \in K : \beta I \subset I\}.$$

Definition 3.31. A fractional ideal I of an order $\mathcal{O}$ is called *invertible* if there exists another fractional ideal J of $\mathcal{O}$ such that $IJ = \mathcal{O}$.

Lemma 3.32 ([7, Lemma 7.5])**.** Let $K = \mathbb{Q}(\tau)$ be a quadratic field and let $ax^2+bx+c \in \mathbb{Z}[X]$ be the polynomial of least degree having τ as a root such that a, b and c are relatively prime. Then $[1, \tau]$ is a proper fractional ideal of the order $[1, a\tau]$ in K.

Proof. It is clear that $[1, a\tau]$ satisfies the conditions in Definition 3.19 and hence $[1, a\tau]$ is an order. Moreover, it can easily be checked that multiplying an element in $[1, a\tau]$ by an element in $[1, \tau]$ gives another element in $[1, \tau]$, which implies that $[1, \tau]$ is a fractional ideal of $[1, a\tau]$. We will show that $[1, \tau]$ is proper.

Let $\beta \in K$. In order to satisfy $\beta[1, \tau] \subset [1, \tau]$, it must hold that

$$\begin{aligned} \beta \cdot 1 &\in [1, \tau], \\ \beta \cdot \tau &\in [1, \tau]. \end{aligned}$$

The first line implies that $\beta = n + m\tau$ for some $n, m \in \mathbb{Z}$. It follows that

$$\begin{aligned} \beta\tau = (n + m\tau)\tau = n\tau + m\tau^2 = n\tau - \frac{m}{a}(b\tau + c) \\ = -\frac{cm}{a} + \left(n - \frac{bm}{a}\right)\tau, \end{aligned}$$

where we used that τ is a root of the polynomial $ax^2 + bx + c$. Thus, $\beta\tau \in [1, \tau]$ if and only if $\frac{cm}{a}$ and $n - \frac{bm}{a}$ are integers. We will show that $\frac{cm}{a}$ and $n - \frac{bm}{a}$ are integers if and only if $a|m$. The "if" part is clear, so we will continue with the "only if" part.

Let k be the least integer such that $a|km$. If $k = \pm 1$, we are done. We will therefore assume that $k \neq \pm 1$. Suppose there exists another integer l such that $a|lm$. Then $|l| \geq |k|$, so we can write $lm = r \cdot km + sm$, where $|s| < |k|$. Note that $a|lm$ and $a|km$, so also $a|sm$. This is however a contradiction with the minimality of k, unless $s = 0$. Therefore $s = 0$ and it follows that l is a multiple of k. This argument shows that if $\frac{cm}{a}$ and $\frac{bm}{a}$ are integers and $a \nmid m$, then c and b are multiples of k. Since $\gcd(a, b, c) = 1$, it holds that $\gcd(a, k) = 1$. By Bézout's identity there exist integers x and y such that $ax + ky = 1$. Multiplying by m gives $max + mky = m$. Note that $a|max$ and $a|km$, so $a|max + mky = m$.

This shows that $\beta[1, \tau] \subset [1, \tau]$ if and only if $\beta = n + m\tau$ for $n, m \in \mathbb{Z}$, with $a|m$. Hence

$$\{\beta \in K : \beta[1, \tau] \subset [1, \tau]\} = [1, a\tau],$$

which proves that $[1, \tau]$ is proper. □

Lemma 3.33. Let $\mathcal{O}$ be an order in a quadratic field. A nonzero fractional ideal of $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2.

Proof. Let I be a nonzero fractional ideal of $\mathcal{O}$. Theorem 3.29 implies that there is an ideal J of $\mathcal{O}$ and an element $\alpha \in K^\times$ such that $I = \alpha J$. By Lemma 3.26, J is a free $\mathbb{Z}$-module of rank 2. It follows that $I = \alpha J$ is a free $\mathbb{Z}$-module of rank 2 as well. $\square$

Theorem 3.34 ([7, Proposition 7.4])**.** Let $\mathcal{O}$ be an order in a quadratic field $K = \mathbb{Q}(\sqrt{N})$ and let I be a fractional ideal of $\mathcal{O}$. Then I is proper if and only if I is invertible.

Proof. Assume I is invertible. By definition, I is an $\mathcal{O}$-module, which implies that $\mathcal{O} \subset \{\beta \in K : \beta I \subset I\}$. Let $\beta \in \{\beta \in K : \beta I \subset I\}$. There exists another fractional ideal J of $\mathcal{O}$ such that $IJ = \mathcal{O}$. Then we have

$$\beta\mathcal{O} = \beta(IJ) = (\beta I)J \subset IJ = \mathcal{O},$$

which shows that $\beta \in \mathcal{O}$. Hence, $\{\beta \in K : \beta I \subset I\} \subset \mathcal{O}$ and equality follows.

Assume that I is proper. By Lemma 3.33, I is a free $\mathbb{Z}$-module of rank 2, so $I = [\alpha, \beta]$ for some $\alpha, \beta \in K$. We can write $I = \alpha[1, \tau]$, where $\tau = \frac{\beta}{\alpha}$. Note that α and β are not both rational numbers, otherwise I is not a free $\mathbb{Z}$-module of rank 2. Thus, $\sqrt{N}$ appears in the expression for α or β. It follows that $K = \mathbb{Q}(\tau)$.

Let $ax^2 + bx + c \in \mathbb{Z}[X]$ with $\gcd(a, b, c) = 1$, be the polynomial of least degree having τ as a root. Then Lemma 3.32 implies that $[1, \tau]$ is a proper fractional ideal of the order $[1, a\tau]$ of K. It follows that also $I = \alpha[1, \tau]$ is a proper fractional ideal of the order $[1, a\tau]$. The polynomial $ax^2 + bx + c$ has one other root which is $\bar{\tau}$ (the conjugate of τ). Lemma 3.32 implies that $[1, \bar{\tau}]$ is a proper fractional ideal of the order $[1, a\bar{\tau}]$. Note that $a\bar{\tau} \in \mathcal{O}$ is an algebraic integer, so $a\bar{\tau} = \frac{p}{q} + \frac{r}{q}\sqrt{N}$, where q is either 1 or 2 by Theorem 3.7. It follows that $[1, a\bar{\tau}] = [1, a\tau]$. Therefore, $I' = \bar{\alpha}[1, \bar{\tau}]$ is a proper fractional ideal of the order $[1, a\tau]$.

We have

$$\begin{aligned} aII' &= a\alpha\bar{\alpha}[1, \tau][1, \bar{\tau}] \\ &= N(\alpha)[a, a\tau, a\bar{\tau}, a\tau\bar{\tau}] \\ &= N(\alpha)[a, a\tau, a\tau + a\bar{\tau}, a\tau\bar{\tau}] \\ &= N(\alpha)[a, a\tau, aT(\tau), aN(\tau)]. \end{aligned} \tag{26}$$

Remember that the minimal polynomial of τ is $x^2 - T(\tau)x + N(\tau) \in \mathbb{Q}[X]$. We defined $ax^2 + bx + c \in \mathbb{Z}[X]$ to be the polynomial of least degree having τ as a root. Hence, $x^2 + \frac{b}{a}x + \frac{c}{a}$ is also the minimal polynomial of τ. Since the minimal polynomial is unique, it follows that

$$x^2 - T(\tau)x + N(\tau) = x^2 + \frac{b}{a}x + \frac{c}{a}.$$

Hence

$$\begin{aligned} T(\tau) &= \tau + \bar{\tau} = -\frac{b}{a}, \\ N(\tau) &= \tau\bar{\tau} = \frac{c}{a}. \end{aligned}$$

Equation (26) then becomes

$$aII' = N(\alpha)[a, a\tau, -b, c] = N(\alpha)[1, a\tau] = N(\alpha)\mathcal{O},$$

where the second equality follows from the fact that $\gcd(a, b, c) = 1$. Thus

$$I\left(\frac{a}{N(\alpha)}I'\right) = \mathcal{O},$$

where $\frac{a}{N(\alpha)}I'$ is a fractional ideal of $\mathcal{O}$. Hence, I is invertible. □

Definition 3.35. The product of ideals I and J in a ring R is defined by

$$IJ = \left\{\sum_{i=1}^{n} x_i y_i : n \in \mathbb{Z}_{\geq 0}, x_i \in I, y_i \in J\right\}.$$

Definition 3.36. Let $\alpha I, \beta J \in I(\mathcal{O})$, where $\alpha, \beta \in K^\times$ and I, J are ideals in $\mathcal{O}$. Define the product of αI and βJ to be $\alpha\beta(IJ)$, where IJ is as in Definition 3.35.

Theorem 3.37. Let $\mathcal{O}$ be an order and let $I(\mathcal{O})$ denote the set of proper fractional ideals of $\mathcal{O}$. The set $I(\mathcal{O})$ together with the operation defined in Definition 3.36 is a group with unit element $\mathcal{O}$.

Proof. It is clear that $\mathcal{O}$ is a nonzero finitely generated $\mathcal{O}$-module, so $\mathcal{O}$ is a fractional ideal. Moreover, the set $\mathcal{O}$ contains 1, which shows that for $\beta \in K\backslash\mathcal{O}$, $\beta\mathcal{O} \not\subset \mathcal{O}$. Hence, $\mathcal{O}$ is proper. Let I be a proper fractional ideal of $\mathcal{O}$. Then $I = \alpha J$ for some $\alpha \in K^\times$ and ideal J of $\mathcal{O}$. As I is an $\mathcal{O}$-module, we have $I \cdot \mathcal{O} = I$. This shows that $\mathcal{O}$ is the unit element of $I(\mathcal{O})$.

Proper fractional ideals are invertible by Theorem 3.34. Let I be a proper fractional ideal of $\mathcal{O}$. Then there exists another fractional ideal I^{-1} of $\mathcal{O}$ such that $II^{-1} = \mathcal{O}$. Thus, I^{-1} is an invertible fractional ideal of $\mathcal{O}$. Then Theorem 3.34 implies that $I^{-1} \in I(\mathcal{O})$. Hence, $I(\mathcal{O})$ is closed under inverses.

Let I and J be proper fractional ideals of $\mathcal{O}$. We can find elements $\alpha, \beta \in K^\times$ and ideals I' and J' of $\mathcal{O}$ such that $I = \alpha I'$ and $J = \beta J'$. Then

$$IJ = (\alpha I')(\beta J') = (\alpha\beta)(I'J'),$$

where $\alpha\beta \in K^\times$ and $I'J'$ is an ideal of $\mathcal{O}$. Theorem 3.29 implies that IJ is a fractional ideal of $\mathcal{O}$. Moreover, Theorem 3.34 implies that there exist fractional ideals I^{-1} and J^{-1} of $\mathcal{O}$ such that $II^{-1} = \mathcal{O}$ and $JJ^{-1} = \mathcal{O}$. The product $J^{-1}I^{-1}$ is a fractional ideal of $\mathcal{O}$ and $IJ \cdot J^{-1}I^{-1} = \mathcal{O}$. This shows that IJ is invertible and hence proper by Theorem 3.34. Hence, $I(\mathcal{O})$ is closed under multiplication.

Let I, J and K be proper fractional ideals of $\mathcal{O}$. Then there exist elements $\alpha, \beta, \gamma \in K^\times$ and ideals I', J' and K' of $\mathcal{O}$ such that $I = \alpha I'$, $J = \beta J'$ and $K = \gamma K'$. Then

$$(IJ)K = (\alpha I' \beta J')\gamma K' = \alpha\beta\gamma(I'J')K'$$

and

$$I(JK) = \alpha I'(\beta J' \gamma K') = \alpha\beta\gamma I'(J'K').$$

It follows from the associativity of ideal multiplication that $(IJ)K = I(JK)$. This proves the theorem. □

Theorem 3.38. Let $\mathcal{O}$ be an order. The set of principal fractional ideals of $\mathcal{O}$, which are of the form $\alpha\mathcal{O}, \alpha \in K^\times$, forms a subgroup $P(\mathcal{O}) \subset I(\mathcal{O})$.

Proof. Lemma 3.26 states that ideals of $\mathcal{O}$ are finitely generated $\mathbb{Z}$-modules and hence finitely generated $\mathcal{O}$-modules. Therefore, the principal ideals of $\mathcal{O}$ are fractional ideals. Let $\alpha^{-1} \in K$ be the inverse of α. Then $\alpha\mathcal{O}\alpha^{-1}\mathcal{O} = \mathcal{O}$, which shows that $\alpha\mathcal{O}$ is invertible and hence proper by Theorem 3.34. Therefore the set of principal ideals of $\mathcal{O}$ is a subset of $I(\mathcal{O})$.

Note that $\mathcal{O}$ is a principal ideal of $\mathcal{O}$, so $P(\mathcal{O})$ contains the unit element of the group $I(\mathcal{O})$. The product of two principal ideals of $\mathcal{O}$ is again a principal ideal of $\mathcal{O}$, so $P(\mathcal{O})$ is closed under multiplication. Moreover, $P(\mathcal{O})$ is closed under inverses. This proves the theorem. □

It follows from Definition 3.36 that the group $I(\mathcal{O})$ is Abelian. Therefore, the following definition makes sense.

Definition 3.39. Let $\mathcal{O}$ be an order. The quotient

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

is the ideal class group of the order $\mathcal{O}$. The number of elements in the ideal class group is called the *class number*.

Remember that in Section 2.2, we defined the class number to be the number of elements in the form class group. It is not a coincidence that the same terminology is used. In the next section, we will prove that every form class group $C(D)$ is isomorphic to a unique ideal class group $C(\mathcal{O})$. This implies that the class number of $C(D)$ and the class number of $C(\mathcal{O})$ are equal.

4 The relation between the form class group and the ideal class group

In the previous two sections, we constructed the form class group and the ideal class group. These two groups are related to each other. Namely, for every form class group, there is a unique ideal class group isomorphic to this form class group. Remember that the form class group is characterized by its discriminant. This discriminant plays an important role in the construction of the isomorphism.

4.1 The isomorphism

Let $\mathcal{O}$ be an order in a quadratic field K. By Lemma 3.23, a basis of $\mathcal{O}$ is $\{1, f \cdot \frac{d_K+\sqrt{d_K}}{2}\}$. Computing the discriminant of $\mathcal{O}$ using this basis gives

$$\begin{aligned} D &= \left(\det \begin{pmatrix} 1 & f \cdot \frac{d_K+\sqrt{d_K}}{2} \\ 1 & f \cdot \frac{d_K-\sqrt{d_K}}{2} \end{pmatrix}\right)^2 \\ &= \left(f \cdot \frac{d_K - \sqrt{d_K}}{2} - f \cdot \frac{d_K + \sqrt{d_K}}{2}\right)^2 \\ &= \left(-f\sqrt{d_K}\right)^2 \\ &= f^2 d_K. \end{aligned} \tag{27}$$

Note that $f^2 \equiv 0, 1 \mod 4$ and $d_K \equiv 0, 1 \mod 4$ such that $D \equiv 0, 1 \mod 4$. This relation between D and d_K implies that D and d_K have the same sign. Hence, if an order in a quadratic field K has a negative discriminant, then $K = \mathbb{Q}(\sqrt{d_K})$ is an imaginary quadratic field.

Theorem 4.1 ([7, Exercise 7.3(b),(c),(d)])**.** Let D be a negative integer such that $D \equiv 0, 1 \mod 4$. Then there is a unique order in a unique imaginary quadratic field whose discriminant is D.

Proof. Let D be a negative integer and assume that $D \equiv 0 \mod 4$. Then $D = 4D'$ for some $D' \in \mathbb{Z}$. Let $p_1^{r_1} \cdots p_n^{r_n}$ be the prime factorization of D'. Write $r_i = 2k_i + l_i$ such that $l_i = 0, 1$, for $i = 1, \ldots, n$. Then

$$D' = p_1^{r_1} \cdots p_n^{r_n} = (p_1^{2k_1} \cdots p_n^{2k_n}) \cdot p_1^{l_1} \cdots p_n^{l_n} = (p_1^{k_1} \cdots p_n^{k_n})^2 \cdot (p_1^{l_1} \cdots p_n^{l_n}).$$

Let $N = p_1^{l_1} \cdots p_n^{l_n}$. By construction N is squarefree. Moreover, $N \neq 0$, because $D \neq 0$, and $N \neq 1$, otherwise D would be positive. Hence, $K = \mathbb{Q}(\sqrt{N})$ is an imaginary quadratic field. If $N \equiv 1 \mod 4$, then $d_K = N$. Define $f = 2 \cdot p_1^{k_1} \cdots p_n^{k_n}$. Then the

order $\mathcal{O} = [1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$ in K has discriminant D. If $N \equiv 2, 3 \mod 4$, then $d_K = 4N$. Define $f = p_1^{k_1} \cdots p_n^{k_n}$. Then the order $\mathcal{O} = [1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$ in K has discriminant D.

Let D be a negative integer and assume that $D \equiv 1 \mod 4$. Let $p_1^{r_1} \cdots p_n^{r_n}$ be the prime factorization of D. Write $r_i = 2k_i + l_i$ such that $l_i = 0, 1$, for $i = 1, \ldots, n$. Then

$$D = p_1^{r_1} \cdots p_n^{r_n} = (p_1^{2k_1} \cdots p_n^{2k_n}) \cdot p_1^{l_1} \cdots p_n^{l_n} = (p_1^{k_1} \cdots p_n^{k_n})^2 \cdot (p_1^{l_1} \cdots p_n^{l_n}) \equiv 1 \mod 4. \quad (28)$$

Define $f = p_1^{k_1} \cdots p_n^{k_n}$ and $N = p_1^{l_1} \cdots p_n^{l_n}$. Note that $(p_1^{k_1} \cdots p_n^{k_n})^2 \equiv 0, 1 \mod 4$, so (28) is satisfied if and only if $f^2 \equiv 1 \mod 4$ and $N \equiv 1 \mod 4$. By construction N is squarefree. Moreover, $N \neq 0$, because $D \neq 0$, and $N \neq 1$, otherwise D would be positive. Hence, $K = \mathbb{Q}(\sqrt{N})$ is an imaginary quadratic field with $N \equiv 1 \mod 4$, so $d_K = N$. Then D is the discriminant of the order $[1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$.

Let D be a negative discriminant. The argument above shows that D can be uniquely written as $f^2 d_K$, where d_K is the discriminant of an imaginary quadratic field K. Remember that $K = \mathbb{Q}(\sqrt{d_K})$. The order $[1, f \cdot \frac{d_K+\sqrt{d_K}}{2}]$ in K has discriminant D. This shows that an order in an imaginary quadratic field is uniquely determined by its discriminant. □

Example 4.2. Let $D = -96 \equiv 0 \mod 4$. The proof of Theorem 4.1 describes how we can find the unique order whose discriminant is D. We have $D = 4 \cdot D'$, where $D' = -24$. The prime factorization of D' is

$$D' = -24 = -2^3 \cdot 3 = 2^2 \cdot -(2 \cdot 3).$$

Let $N = -6$ and $K = \mathbb{Q}(\sqrt{-6})$ a quadratic field. Then $-6 \equiv 2 \mod 4$, so the discriminant of K is $d_K = 4 \cdot -6 = -24$. Hence, the order $[1, 2 \cdot \frac{-24+\sqrt{-24}}{2}]$ in the field $\mathbb{Q}(\sqrt{-6})$ has discriminant $2^2 \cdot -24 = -96$.

Theorem 4.1 shows that for any form class group $C(D)$ of discriminant D, there is a unique order $\mathcal{O}$ in a unique quadratic field K whose discriminant is D. Let $\mathcal{O}$ be an order in an imaginary quadratic field with a negative discriminant D. Then the ideal class group $C(\mathcal{O})$ is isomorphic to the form class group $C(D)$. This is explained in the following theorem.

Theorem 4.3 ([7, Theorem 7.7(i),(ii)])**.** Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K. If $f(x, y) = ax^2 + bx + c$ is a primitive positive definite form of discriminant D, then $[a, \frac{-b+\sqrt{D}}{2}]$ is a proper ideal of $\mathcal{O}$. The form class group $C(D)$ and the ideal class group $C(\mathcal{O})$ are isomorphic. The isomorphism between $C(D)$ and $C(\mathcal{O})$ is induced by the map

$$ax^2 + bxy + cy^2 \mapsto \left[a, \frac{-b + \sqrt{D}}{2}\right].$$

Proof.
Step 1. Let $f(x,y) = ax^2+bxy+cy^2$ be a primitive positive definite form of discriminant D. We will first prove that $[a, \frac{-b+\sqrt{D}}{2}]$ is a proper ideal of $\mathcal{O}$. The zeros of $f(x,1)$ are $\frac{-b\pm\sqrt{D}}{2a}$. Note that the zeros of $f(x,1)$ are complex since $D<0$. One of these zeros lies in the upper half of the complex plane and one in the lower half of the complex plane. Call the zero in the upper half plane the *root*. The root of f is $\tau = \frac{-b+\sqrt{D}}{2a}$, because $a>0$. We form the set

$$\left[a, \frac{-b+\sqrt{D}}{2}\right] = a\left[1, \frac{-b+\sqrt{D}}{2a}\right] = a[1,\tau].$$

By Lemma 3.32, $[1,\tau]$ is a proper fractional ideal of the order $[1,a\tau]$. It follows from Remark 3.28 that $a[1,\tau]$ is a proper fractional ideal of $[1,a\tau]$. The set $a[1,\tau]$ is actually a proper ideal of $[1,a\tau]$, because $a[1,\tau] \subset [1,a\tau]$. We will show that $[1,a\tau] = \mathcal{O}$.

The order $\mathcal{O}$ has discriminant D in K. Therefore, $D = f^2 d_K$, where f is the conductor of $\mathcal{O}$. We have seen before that $D \equiv b^2 \mod 2 = b \mod 2$, so D has the same parity as b. It also holds that D has the same parity as fd_K. If D is odd, then f^2 and d_K are odd and hence fd_K is odd. If D is even, then either f^2 or d_K is even, so fd_K is even. We have

$$a\tau = \frac{-b+\sqrt{D}}{2} = \frac{-b+f\sqrt{d_K}}{2} = -\frac{b+fd_K}{2} + f\cdot\frac{d_K+\sqrt{d_K}}{2},$$

where $\frac{b+fd_K}{2} \in \mathbb{Z}$, because b and fd_K have the same parity. It follows that

$$[1,a\tau] = \left[1, f\cdot\frac{d_K+\sqrt{d_K}}{2}\right] = \mathcal{O}.$$

Hence, $a[1,\tau]$ is a proper ideal of $\mathcal{O}$.

Step 2. Before we can show that the given map induces an isomorphism, we first have to prove two equivalences. We will use these equivalences when we show that the induced map between $C(D)$ and $C(\mathcal{O})$ is well-defined and injective. Let $f(x,y)$ and $g(x,y)$ be primitive positive definite forms of discriminant D. Let τ be the root of f and τ' be the root of g. We will first prove the following equivalence:

$$\begin{aligned} &f(x,y) \text{ and } g(x,y) \text{ are properly equivalent} \\ &\iff \tau' = \frac{p\tau+q}{r\tau+s}, \text{ where } p,q,r,s\in\mathbb{Z} \text{ and } ps-qr=1. \end{aligned} \tag{29}$$

Assume that $f(x,y)$ and $g(x,y)$ are properly equivalent, so there exist integers p,q,r and s such that $f(x,y) = g(px+qy, rx+sy)$ with $ps-qr=1$. Then

$$0 = f(\tau,1) = g(p\tau+q, r\tau+s) = (r\tau+s)^2 g\left(\frac{p\tau+q}{r\tau+s}, 1\right) \tag{30}$$

and hence $g(\frac{p\tau+q}{r\tau+s}, 1) = 0$. Note that if $\mathrm{Im}(\frac{p\tau+q}{r\tau+s}) > 0$, then $\frac{p\tau+q}{r\tau+s}$ is the root of g and $\tau' = \frac{p\tau+q}{r\tau+s}$ by uniqueness of the root. We have

$$\frac{p\tau+q}{r\tau+s} = \frac{(p\tau+q)(r\bar{\tau}+s)}{(r\tau+s)(r\bar{\tau}+s)} = \frac{prN(\tau)+qs+ps\tau+qr\bar{\tau}}{|r\tau+s|^2},$$

so

$$\mathrm{Im}\left(\frac{p\tau+q}{r\tau+s}\right) = \frac{(ps-qr)\,\mathrm{Im}(\tau)}{|r\tau+s|^2} = \frac{\mathrm{Im}(\tau)}{|r\tau+s|^2} > 0. \tag{31}$$

Hence, $\tau' = \frac{p\tau+q}{r\tau+s}$.

Now assume that $\tau' = \frac{p\tau+q}{r\tau+s}$, where $p, q, r, s \in \mathbb{Z}$ and $ps - qr = 1$. Then (30) shows that τ is the root of both $f(x, y)$ and $g(px + qy, rx + sy)$. We will show that this implies that $f(x, y)$ and $g(px + qy, rx + sy)$ must be equal. Remember that $f(x, y)$ and $g(x, y)$ are primitive positive definite forms of discrminant D. Since $ps - qr = 1$, $g(x, y)$ and $g(px + qy, rx + sy)$ are properly equivalent and therefore $g(px + qy, rx + sy)$ is also a primitive positive definite form of discriminant D. Let $f(x, y) = ax^2 + bxy + cy^2$. Since $f(x, y)$ is primitive and the root τ of $f(x, 1) = ax^2 + bx + c$ is complex, $f(x, 1)$ is the polynomial of least degree such that a, b and c are relatively prime. Then Lemma 3.32 shows that $[1, a\tau]$ is an order in $K = \mathbb{Q}(\tau)$. We have

$$\begin{aligned}\left(\det\begin{pmatrix}1 & a\tau\\ 1 & a\bar{\tau}\end{pmatrix}\right)^2 &= (a\bar{\tau} - a\tau)^2 = a^2\bar{\tau}^2 - 2a^2\tau\bar{\tau} + a^2\tau^2\\ &= a^2(\bar{\tau}+\tau)^2 - 4a^2\tau\bar{\tau} = a^2T(\tau)^2 - 4a^2N(\tau).\end{aligned} \tag{32}$$

Remember that the minimal polynomial of τ is $x^2 - T(\tau)x + N(\tau) \in \mathbb{Q}[X]$. Moreover, $x^2 + \frac{b}{a}x + \frac{c}{a}$ is also the minimal polynomial of τ. Since the minimal polynomial is unique, it follows that

$$x^2 - T(\tau)x + N(\tau) = x^2 + \frac{b}{a}x + \frac{c}{a}.$$

Hence

$$\begin{aligned}T(\tau) &= \tau + \bar{\tau} = -\frac{b}{a},\\ N(\tau) &= \tau\bar{\tau} = \frac{c}{a}.\end{aligned}$$

Then Equation (32) becomes

$$\left(\det\begin{pmatrix}1 & a\tau\\ 1 & a\bar{\tau}\end{pmatrix}\right)^2 = a^2\frac{b^2}{a^2} - 4a^2\frac{c}{a} = b^2 - 4ac,$$

which shows that the discriminant D of $f(x, y)$ is equal to the discriminant of the order $[1, a\tau]$. Let $g(px + qy, rx + sy) = a'x^2 + b'xy + c'y^2$. In the same way, we can show that D is equal to the discriminant of the order $[1, a'\tau]$. Theorem 4.1 states that the order of

discriminant D is unique, so it follows that $[1, a\tau] = [1, a'\tau]$ and hence $a = a'$. Moreover, we have

$$T(\tau) = -\frac{b}{a} = -\frac{b'}{a'},$$
$$N(\tau) = \frac{c}{a} = \frac{c'}{a'},$$

so $b = b'$ and $c = c'$. This shows that $f(x, y)$ and $g(px + qy, rx + sy)$ are equal, which proves the equivalence in (29).

Step 3. Secondly, we will prove

$$\tau' = \frac{p\tau + q}{r\tau + s}, \text{ where } ps - qr = 1 \iff [1, \tau] = \lambda[1, \tau'] \text{ for some } \lambda \in K^\times. \tag{33}$$

Assume $\tau' = \frac{p\tau+q}{r\tau+s}$ with $ps - qr = 1$. Let $\lambda = r\tau + s \in K^\times$. We have

$$\lambda[1, \tau'] = (r\tau + s)\left[1, \frac{p\tau + q}{r\tau + s}\right] = [r\tau + s, p\tau + q] = [1, \tau],$$

since $ps - qr = 1$.

Next assume that $[1, \tau] = \lambda[1, \tau']$ for some $\lambda \in K^\times$. Then $[1, \tau] = [\lambda, \lambda\tau']$. It follows that

$$\lambda\tau' = p\tau + q,$$
$$\lambda = r\tau + s,$$

for some $p, q, r, s \in \mathbb{Z}$ and hence $\tau' = \frac{p\tau+q}{r\tau+s}$. Note that $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is nonsingular, because $\lambda\tau'$ and λ are linearly independent. Moreover, $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ represents a change of basis, so its determininant is ± 1, see Remark 3.25. Note that τ' is the root of g and therefore lies in the upper half of the complex plane. Equation (31) then implies that $ps - qr > 0$. Hence $ps - qr = 1$, which proves (33).

Step 4. In this step, we will prove that the map

$$ax^2 + bxy + cy^2 \mapsto \left[a, \frac{-b + \sqrt{D}}{2}\right]$$

induces a well-defined map between $C(D)$ and $C(\mathcal{O})$. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be properly equivalent primitive positive definite forms of discriminant D. Let τ and τ' be the roots of f and g respectively. Then $f(x, y)$ is mapped to $a[1, \tau]$ and $g(x, y)$ is mapped to $a'[1, \tau']$. We will show that $a[1, \tau]$ and $a'[1, \tau']$

belong to the same class in $C(\mathcal{O})$. Equivalences (29) and (33) show that $[1,\tau] = \lambda[1,\tau']$ for some $\lambda \in K^\times$. It follows that

$$a[1,\tau] = a\lambda[1,\tau'] = a[1,\tau'] \cdot \lambda\mathcal{O},$$

where the last equality follows from the fact that $a[1,\tau']$ is an ideal of $\mathcal{O}$. This shows that $a[1,\tau]$ and $a[1,\tau']$ belong to the same class in $C(\mathcal{O})$. Hence, the induced map between $C(D)$ and $C(\mathcal{O})$ is well-defined.

Step 5. Next, we will show that the induced map between $C(D)$ and $C(\mathcal{O})$ is a homomorphism. Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive positive definite form of discriminant D and consider the equivalence class $[f] \in C(D)$. Let $[g]$ be another equivalence class in $C(D)$. Remember that we can pick $f'(x,y) = a'x^2 + b'xy + c'y^2$ in $[g]$ such that $\gcd(a, a', \frac{b+b'}{2}) = 1$. Then the Dirichlet composition of f and f' is defined and is given by

$$f \circ f' = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

where B is the unique integer modulo $2aa'$ such that

$$B \equiv b \mod 2a, \tag{34}$$
$$B \equiv b' \mod 2a', \tag{35}$$
$$B^2 \equiv D \mod 4aa', \tag{36}$$

see Lemma 2.22. Define $\triangle := \frac{-B+\sqrt{D}}{2}$. Equations (34) and (35) imply that there exist $k, l \in \mathbb{Z}$ such that $b = B + 2ak$ and $b' = B + 2a'l$. It follows that

$$\begin{aligned} f &\mapsto \left[a, \frac{-b+\sqrt{D}}{2}\right] = \left[a, \frac{-B-2ak+\sqrt{D}}{2}\right] = [a, \triangle], \\ f' &\mapsto \left[a', \frac{-b'+\sqrt{D}}{2}\right] = \left[a', \frac{-B-2a'l+\sqrt{D}}{2}\right] = [a', \triangle], \\ f \circ f' &\mapsto \left[aa', \frac{-B+\sqrt{D}}{2}\right] = [aa', \triangle]. \end{aligned}$$

Note that

$$\gcd\left(a, a', \frac{b+b'}{2}\right) = \gcd\left(a, a', \frac{2B + 2(ak + a'l)}{2}\right) = \gcd(a, a', B) = 1. \tag{37}$$

Moreover,

$$\begin{aligned} \triangle^2 &= \frac{B^2 - 2B\sqrt{D} + D}{4} \equiv \frac{2B^2 - 2B\sqrt{D}}{4} \mod aa' \\ &= -B\frac{-B+\sqrt{D}}{2} \mod aa' = -B\triangle \mod aa', \end{aligned} \tag{38}$$

where the second equality follows from Equation (36). It follows that

$$[a, \triangle][a', \triangle] = [aa', a\triangle, a'\triangle, \triangle^2] = [aa', a\triangle, a'\triangle, -B\triangle] = [aa', \triangle],$$

where we have used (37) and (38). This shows that the induced map between $C(D)$ and $C(\mathcal{O})$ is a homomorphism.

Step 6. We will show that the induced homomorphism is injective. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant D and let τ and τ' be the roots of f and g respectively. Assume that $a[1, \tau]$ and $a'[1, \tau']$ are part of the same class in the group $C(\mathcal{O})$. Then for some principal fractional ideal $\alpha\mathcal{O}$ with $\alpha \in K^\times$, we have

$$a[1, \tau] = a'[1, \tau'] \cdot \alpha\mathcal{O} = \alpha \left(a'[1, \tau'] \cdot \mathcal{O}\right) = \alpha a'[1, \tau'],$$

where the last equality follows from the fact that $a'[1, \tau']$ is an ideal of $\mathcal{O}$. It follows from the equivalences in (29) and (33) that f and g are properly equivalent. Hence, the induced map between $C(D)$ and $C(\mathcal{O})$ is an injective homomorphism.

Step 7. The final step is to show that the induced injective homomorphism is surjective. Let I be a fractional ideal of the order $\mathcal{O}$ in the imaginary quadratic field K. Lemma 3.33 states that I is a free $\mathbb{Z}$-module of rank 2, so we can write $I = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Switching α and β if necessary, we can assume that $\tau = \frac{\beta}{\alpha}$ lies in the upper half of the complex plane. Let $ax^2 + bx + c \in \mathbb{Z}[X]$ be the polynomial of least degree with $\gcd(a, b, c) = 1$ and $a > 0$ having τ as a root. Note that the discriminant of $ax^2 + bx + c$ is negative, because $\tau \notin \mathbb{R}$. Hence, the quadratic form $f(x, y) = ax^2 + bxy + cy^2$ satisfies $D < 0$ and $a > 0$ and is therefore positive definite. The form $f(x, y)$ maps to $a[1, \tau]$. Note that

$$a[1, \tau] = \alpha\frac{a}{\alpha}[1, \tau] = \frac{a}{\alpha}[\alpha, \beta] = I \cdot \frac{a}{\alpha}\mathcal{O},$$

which shows that $a[1, \tau]$ is part of the same class in $C(\mathcal{O})$ as I. Hence, $C(D)$ and $C(\mathcal{O})$ are isomorphic. □

4.2 Computing class numbers

Let D be any negative discriminant and consider the form class group $C(D)$. Let $\mathcal{O}$ be the unique order of discriminant D in an imaginary quadratic field K. Theorem 4.3 states that $C(D)$ and $C(\mathcal{O})$ are isomorphic and therefore have the same class number. In section 2.3, we looked at two algorithms that compute the class number of $C(D)$. Using these algorithms, we can easily compute the class number of any order with a negative discriminant D satisfying $D \equiv 0, 1 \mod 4$.

D	h(D)	D	h(D)	D	h(D)	D	h(D)	D	h(D)
-3	1	-36	2	**-71**	7	**-104**	6	**-139**	3
-4	1	**-39**	4	-72	2	**-107**	3	-140	6
-7	1	**-40**	2	-75	2	-108	3	**-143**	10
-8	1	**-43**	1	-76	3	**-111**	8	-144	4
-11	1	-44	3	**-79**	5	-112	2	-147	2
-12	1	**-47**	5	-80	4	**-115**	2	**-148**	2
-15	2	-48	2	**-83**	3	**-116**	6	**-151**	7
-16	1	**-51**	2	**-84**	4	**-119**	10	**-152**	6
-19	1	**-52**	2	**-87**	6	**-120**	4	**-155**	4
-20	2	**-55**	4	**-88**	2	**-123**	2	-156	4
-23	3	**-56**	4	**-91**	2	-124	3	**-159**	10
-24	2	**-59**	3	-92	3	**-127**	5	-160	4
-27	1	-60	2	**-95**	8	-128	4	**-163**	1
-28	1	-63	4	-96	4	**-131**	5	**-164**	8
-31	3	-64	2	-99	2	**-132**	4	**-167**	11
-32	2	**--67**	1	-100	2	-135	6	**-168**	4
-35	2	**-68**	4	**-103**	5	**-136**	4	-171	4

Table 1: Class numbers for the orders with discriminant D with $-171 \leq D \leq -3$

Computing the class number of the ring of integers measures how far the ring of integers is from being a unique factorization domain. This will be the subject of the following theorem.

Theorem 4.4. The class number of the ring of integers in a quadratic field is one if and only if the ring of integers is a unique factorization domain.

The proof of this theorem requires the following results.

Theorem 4.5 ([9, Theorem 18])**.** A Dedekind domain is a unique factorization domain if and only if it is a principal ideal domain.

Lemma 4.6 ([7, Exercise 7.6(b)])**.** All nonzero ideals of the ring of integers in a quadratic field K are proper. This means that for every nonzero ideal I of $\mathcal{O}_K$, it holds that

$$\mathcal{O}_K = \{\beta \in K : \beta I \subset I\}.$$

Proof. Let I be a nonzero ideal in the ring of integers $\mathcal{O}_K$ in a quadratic field K. We have $\mathcal{O}_K \subset \{\beta \in K : \beta I \subset I\}$, since I is an ideal of $\mathcal{O}_K$. To prove that I is proper, we have to show the inclusion $\{\beta \in K : \beta I \subset I\} \subset \mathcal{O}_K$. Suppose there exists $\alpha \in K \backslash \mathcal{O}_K$ such that $\alpha I \subset I$. By Lemma 3.11, there exists an integer m such that $m\alpha \in \mathcal{O}_K$, so we can take m to be the smallest such integer. Let $\beta = m\alpha \in \mathcal{O}_K$ such that $\alpha = \frac{\beta}{m}$. By

assumption, $\frac{\beta}{m} I \subset I \subset \mathcal{O}_K$, so we have $I \subset m\mathcal{O}_K$. Thus, I is an ideal of $\mathcal{O}_K$ contained in the principal ideal $m\mathcal{O}_K$. This implies that I is a principal ideal of $\mathcal{O}_K$ of the form $m\gamma\mathcal{O}_K$ for some $\gamma \in \mathcal{O}_K$. We have

$$\alpha \cdot m\gamma = \frac{\beta}{m} \cdot m\gamma = \beta\gamma \in m\gamma\mathcal{O}_K,$$

so we can write β as $m\beta'$ for some $\beta' \in \mathcal{O}_K$. Then

$$\alpha = \frac{\beta}{m} = \frac{m\beta'}{m} = \beta' \in \mathcal{O}_K,$$

which is a contradiction. This proves the inclusion $\{\beta \in K : \beta I \subset I\} \subset \mathcal{O}_K$ and hence I is proper. □

We can now prove Theorem 4.4.

Proof. Let $\mathcal{O}_K$ be the ring of integers in a quadratic field K and assume that the class number of $\mathcal{O}_K$ is one. It follows from Theorem 3.29 that the nonzero ideals of $\mathcal{O}_K$ are fractional ideals of $\mathcal{O}_K$. Moreover, the nonzero ideals of $\mathcal{O}_K$ are proper by Lemma 4.6. Hence, the nonzero ideals of $\mathcal{O}_K$ form a subset of $I(\mathcal{O}_K)$. The class number of $\mathcal{O}_K$ is one, which means that $I(\mathcal{O}_K) = P(\mathcal{O}_K)$. Thus, all nonzero ideals of $\mathcal{O}_K$ are principal and therefore $\mathcal{O}_K$ is a principal ideal domain. Theorem 4.5 implies that $\mathcal{O}_K$ is a unique factorization domain.

Assume that $\mathcal{O}_K$ is a unique factorization domain. Then $\mathcal{O}_K$ is a principal ideal domain by Theorem 4.5, so all nonzero ideals of $\mathcal{O}_K$ are of the form $\alpha\mathcal{O}_K$, for some $\alpha \in \mathcal{O}_K$. It follows from Theorem 3.29 that all fractional ideals are of the form $\beta \cdot \alpha\mathcal{O}_K$, with $\beta \in K^\times$ and $\alpha\mathcal{O}_K$ a nonzero ideal of $\mathcal{O}_K$. Hence, all proper fractional ideals of $\mathcal{O}_K$ are principal and it holds that $I(\mathcal{O}_K) = P(\mathcal{O}_K)$. The class number of $\mathcal{O}_K$ is therefore equal to one. □

Remark 4.7. The proof of Theorem 4.4 makes use of the fact that the ring of integers in a quadratic field is a Dedekind domain. Since orders that are not maximal are not Dedekind domains, Theorem 4.4 only applies to the maximal order in a quadratic field.

The bold numbers in Table 4.2 are discriminants of imaginary quadratic fields. They are called *fundamental discriminants*. Since the conductor of the ring of integers is by definition equal to one, Equation (27) implies that the ring of integers has the same discriminant as the quadratic field it is contained in. Thus, when we compute the class number for a fundamental discriminant D, we compute the class number of the ring of integers in the unique imaginary quadratic field with discriminant D. We can read off from Table 4.2 that the class number is one for the fundamental discriminants

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

The imaginary quadratic fields with these discriminants are listed in the following table.

Discriminant	**Imaginary quadratic field**
-3	$\mathbb{Q}(\sqrt{-3})$
-4	$\mathbb{Q}(\sqrt{-1})$
-7	$\mathbb{Q}(\sqrt{-7})$
-8	$\mathbb{Q}(\sqrt{-2})$
-11	$\mathbb{Q}(\sqrt{-11})$
-19	$\mathbb{Q}(\sqrt{-19})$
-43	$\mathbb{Q}(\sqrt{-43})$
-67	$\mathbb{Q}(\sqrt{-67})$
-163	$\mathbb{Q}(\sqrt{-163})$

Table 2: Fundamental discriminants with their corresponding imaginary quadratic field

Hence, the ring of integers of the fields in Table 4.2 are unique factorization domains by Theorem 4.4. In 1966, Baker proved that the imaginary quadratic fields in Table 4.2 are the only imaginary quadratic fields of which the ring of integers is a unique factorization domain as a result of [1, Theorem]. In 1967, Stark gave another proof of this same result in [12].

Finally, we compared the computation times of Algorithm 2.16 and Algorithm 2.18 for large discriminants. We also added the time Sage takes to compute the class number, for which we used the following command.

```
1  K.<a> = NumberField(x^2 + D)
2  \%time K.class_number()
```

The results are in the table below.

D	**Algorithm 2.16**	**Algorithm 2.18**	**Sage**
$-3 \cdot 5 \cdot 7 \cdot 11$	1.89 ms	1.83 ms	23.1 μs
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	27.9 ms	8.02 ms	20 μs
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	212 ms	43.1 ms	27.9 μs
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	1 min 2 s	13.5 s	30 μs
$-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$	42 min 19 s	6 min 26 s	51 μs

Table 3: Comparison of the computation times

5 Conclusion

We studied the connection between binary quadratic forms and imaginary quadratic number fields with the aim of computing class numbers of orders in imaginary quadratic fields. We first studied the integral binary quadratic forms in order to construct the form class group. For a fixed negative discriminant D, we looked at the set of primitive positive definite integral binary quadratic forms of discriminant D and applied proper equivalence to this set. We proved in detail that the set of equivalence classes of primitive, positive definite forms of discriminant D with the operation induced by Dirichlet composition is an Abelian group. This is usually proven after the bijection between the form class group and the ideal class group is established. We looked at two algorithms that compute the class number of the form class group for a given negative discriminant.

Then we moved on to quadratic fields. Besides the construction of the ideal class group, which is the main goal of this section, we also showed what the ring of integers exactly looks like and that the ring of integers is a Dedekind domain. This property of the ring of integers is important when we explained in the last section that the class number of the ring of integers in a quadratic field measures how far the ring of integers is from being a unique factorization domain.

In the last section, we finally proved that for every form class group, there is a unique ideal class group that is isomorphic to this form class group, and vice versa. It is important to understand how the unique ideal class group isomorphic to the form class group is found. The key is the discriminant of both groups. We proved that for any negative discriminant D, there is a unique order in a unique imaginary quadratic field with discriminant D. The proof is constructive, so it shows how to find this unique order. The form class group $C(D)$ is then isomorphic to the ideal class group $C(\mathcal{O})$, where $\mathcal{O}$ is the unique order of discriminant D, and vice versa. We can therefore use Algorithm 2.16 and Algorithm 2.18 to compute the class number of orders in imaginary quadratic fields.

Many obtained results not only hold for quadratic fields, but for number fields in general. The definition of the ideal class group of orders in number fields is for example the same as for a quadratic field. It also holds that the ring of integers in a number field is a unique factorization domain if and only if the class number of the ring of integers is one. The computation of class numbers of orders in number fields of degree larger than two requires other methods than the one we discussed. One method is described in [4], where the analytic class number formula is used to develop an algorithm to compute the class number of the ring of integers in algebraic number fields. Integral binary forms cannot be used to compute class numbers of orders in algebraic number fields of degree larger than two. The result in [2, Theorem 1.1] does however establish a link between the integral binary cubic forms and cubic number fields.

A Implementation of algorithms

Algorithm 2.16 (Computing reduced forms)

```
def class_number(D):
  list = []
  for a in range(1, floor(sqrt(-D/3)+1)):
    for b in range(-a,a+1):
      c = (b^2-D)/(4*a)
      if c.is_integer() and c >= a and gcd(gcd(a,b),c)==1:
        if abs(b) == a or a == c:
          if b>= 0:
            elt = [a,b,c]
            list.append(elt)
        else:
          elt = [a,b,c]
          list.append(elt)

  return list, len(list)
```

Algorithm 2.18 (Counting reduced forms)

```
def h(d):
  b = d%2
  B = floor(sqrt(-d/3))
  h=0
  while (b <= B):
    q = (b^2 - d)/4
    a=b
    if (a<1):
      a=1
    while (a^2 <= q):
      if ((q%a == 0) and (gcd(gcd(a,b),q/a) == 1)):
        if (a == b) or (a^2 == q) or (b == 0):
          h = h+1
        else:
          h = h+2
      a = a+1
    b = b+2

  print h
```

References

[1] A. Baker. Linear forms in the logarithms of algebraic numbers. *Mathematika*, 13:204–216, December 1966.

[2] K. Belabas. A fast algorithm to compute cubic fields. *Mathematics of Computation*, 66:1213–1237, July 1997.

[3] F. Bouyer. *Composition and Bhargava's Cubes.* https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/gauss_composition.pdf.

[4] J. Buchman and H. Williams. On the computation of the class number of an algebraic number field. *Mathematics of Computation*, 53:679–688, October 1989.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 1 edition, 1993.

[6] K. Conrad. *Ideal Factorization.* https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[7] D. A. Cox. *Primes of the Form $x^2 + ny^2$.* Wiley, 2 edition, 2013.

[8] C. H. Huat. *MA3265 Introduction to Number Theory.* http://www.math.nus.edu.sg/∼chanhh/notes/MA3265.pdf.

[9] D. A. Marcus. *Number Fields.* Springer, 2 edition, 2018.

[10] R. A. Mollin. *Algebraic Number Theory.* CRC Press, 2 edition, 2011.

[11] C. Perret-Gentil. *The correspondence between binary quadratic forms and quadratic fields.* https://corentinperretgentil.gitlab.io/static/documents/correspondence-bqf-qf.pdf, 2012. Master project.

[12] H. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal*, 14:1–27, April 1967.