École Polytechnique fédérale de Lausanne
Section de Mathématiques

Semester project, Master I

The correspondence between binary quadratic forms and quadratic fields

Author: Corentin Perret-Gentil

Supervised by Paul D. Nelson

Chair of Analytic Number Theory
Prof. Philippe Michel

Automn 2012

Abstract

This document is the final report for a master semester project, whose goal was to study in detail the beautiful connection between integral binary quadratic forms and quadratic fields, along with its uses in these two settings.

To do so, we begin by studying integral binary quadratic forms and the number-theoretic questions associated: which integers are represented by a given form/set of forms, how many representation does an integer admit by a given form/set of forms and so on. Doing so, we study in depth the equivalence of forms and the theories of reduction of definite and indefinite forms developed by Gauss. Class numbers of quadratic forms and their links with representation questions are introduced.

Then, we recall some results about orders in the rings of integers of quadratic fields and we show how (classes) of forms can be associated to (classes) of ideals in such orders and vice-versa. Combining these results, we give the precise correspondence between classes of forms and narrow Picard groups of orders in quadratic fields.

In the third chapter, we work on the correspondence obtained to transpose and answer questions from one setting to the other. The composition law on binary quadratic forms discovered by Gauss is derived from the group structure of Picard groups using the correspondence. We introduce how Manjul Bhargava recovered Gauss composition law in an elementary manner and how he generalized it to higher order spaces of forms.

We show how to determine Picard groups of orders in quadratic fields (in particular ideal class groups and class numbers) very easily from the perspective of forms. These ideas are used to give tables summing up the correspondence for the first form discriminants. Working in the context of forms, we also present a proof of the class number one problem for even negative discriminants.

Then, we study units in orders of rings of integers of quadratic fields, automorphisms of forms and show how they are closely related. We count the number of representations of an integer by the set of classes of forms of a given discriminant in two ways: working in quadratic fields thanks to the correspondence and without the latter, working in the point of view of forms. Doing so, we illustrate how insightful the correspondence is.

After obtaining a closed formula for the number of representations of an integer by binary quadratic forms of given discriminant, we derive the Dirichlet class number formula from it, using an estimation by a L-series and a lattice point counting argument, again using the two settings of binary quadratic forms and quadratic fields.

CONTENTS

References

A complete bibliography is given at the end of the document. A detailed list of references chapter by chapter is given by the following:

- Introduction: Based on [Sti10, Ch. 3&5, §4]), [Cox89] and [Kle07, Ch. III, §2 and Ch. IV, §2].
- I. Binary quadratic forms: The references are [Hec10, Ch. VII, §53], [Ste03, Ch. 9], [Gra07] and [Cox89, Ch. 1, §2] for representation problems. The foundational *Disquisitiones Arithmeticae* [Gau86] of Gauss has also been used to study reduction of indefinite forms, along with [Coh93].
- II. Quadratic fields and binary quadratic forms: The main references are [Hec10, Ch. VII, §53], [Cox89, Ch. 2, §7] and [Ste03, Ch. 9]. Hecke and Stein only treat fundamental discriminants (so only ideals in maximal orders) and Cox only treats negative discriminants (so only imaginary quadratic fields). Therefore, we work to generalize both methods by combining them to obtain a complete correspondence.
- III. Using the two points of view: This chapter is mostly made of exercises from [Gra07], [Cox89] or suggested by the supervisor or the author. Exceptions are: the determination of units in quadratic fields ([Fla89, Ch. 4, §3]) and the explicit formula for $|\{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}|$ ([Lan99, Th. 87 and Th. 97]). The considerations about M. Bhargava's higher composition laws have his first paper [Bha04a] as reference. The historical comments on ideal class groups are based on [Kle07, Ch. III, §2 and Ch. IV, §2].
- IV. Dirichlet Class Number Formula: the main references are [Dav00, Ch. 6] and [Gra07]. We complete the missing parts and detail the others, here or before, in Chapter I.

Computations

All the non-trivial numerical calculations in this project have been implemented using the *Sage* open-source mathematical software system, available at `sagemath.org`.

Acknowledgements

I am grateful to Paul Nelson for his very valuable help during this project.

INTRODUCTION

Quadratic forms, this is homogeneous polynomials of degree 2, are fundamental objects of number theory, whose binary specimens (i.e. with two variables) appeared since Antiquity with the family of diophantine equations

$$x^2 - ny^2 = 1 \ (n \geq 1)$$

called Pell's equations, studied notably by Pythagoreans and the Indian mathematician Brahmagupta (598-668 B.C.)[1]

The most fundamental questions arising about a quadratic form f in k variables are:

- (representability) Given an integer n, does there exist a solution to the diophantine equation $f(x_1, \dots, x_k) = n$? Do there exist conditions characterizing such n with a solution to this equation?
- (number of representations) Given an integer n, how many solutions to the diophantine equation $f(x_1, \dots, x_k) = n$ do there exist?

Around 1640, Fermat studied these questions for certain forms of the type $x^2 + ny^2$ and discovered notably his famous two-squares theorem, giving an explicit characterization of integers which can be written as the sum of two squares (this is, represented by the form $x^2 + y^2$)[2]

A general theory of quadratic form began to be developed by Lagrange (1736-1813), and Legendre (1752-1833) dealt more precisely with the case of binary quadratic forms (with integral coefficients), followed by Gauss (1777-1855) in his famous *Disquisitiones Arithmeticae.*

One of Gauss's result is that for a certain equivalence relation on binary quadratic forms, some sets of classes of forms can be endowed the a natural structure of **abelian group**! Gauss generalized therefore the ideas of composition going back to the Antiquity (see the footnote).

As a matter of fact, it happens that binary quadratic forms have a very strong link with another fundamental object of number theory: **quadratic fields**.

[1] The Pythagoreans studied the case $n = 2$, generating recursively integral solutions larger and larger, letting them approximate $\sqrt{2}$ (see [Sti10, Ch. 3, §4]). Brahmagupta discovered a method to find integral solutions to some Pell's equations from a *composition identity*, generalizing a well-known identity from Diophantus on the product of sums of two squares (see [Sti10, Ch. 5, §4]).

[2] The two-squares theorem was first proven by Euler in 1747, using a particular case of the same composition identity as above.

Historically, it is actually the work of Gauss on binary quadratic forms that motivated the general definition of number fields and ideal class groups by Kummer and Kronecker, who inspired themselves from the idea of composing classes.

De facto, there exists a **bijection** between some sets of classes of binary quadratic forms (to be defined) and Picard groups of orders in the ring of integers of quadratic fields (generalizing ideal class groups). Consequently, these classes are forms are endowed with an induced group law, and we recover Gauss's composition law[3].

Questions on quadratic fields such as

– What is the asymptotic behavior of the class number $h(d)$? How many quadratic fields with a given class number does there exist?

– What are the integers represented by the ideals of the ring of integers of a quadratic fields?

– How can the ideal class group of a given quadratic field be determined?

can also be asked. Using the correspondence between binary quadratic forms and quadratic fields, we will see that questions in these two settings transpose from one to the other. We will see that for many problems, considering them in the two points of view can simplify them or open new perspectives.

Using the point of view of quadratic fields, it will be for example relatively easy to answer some question about the **number of representations** of integers by (sets of) quadratic forms. Reciprocally, the famous **Dirichlet class number formula** will be proved passing through the points of view of forms.

More recently, Manjul Bhargava (Princeton University) was able in the 2000s to give an elementary interpretation of Gauss's composition law and managed to generalize the ideas of the latter to give composition laws to set of forms of **higher degrees** (e.g. ternary cubic forms) with correspondence to number fields of higher degrees (e.g. cubic fields).

In this document, we begin by presenting the foundations of the theory of binary quadratic forms of Gauss, Lagrange and Legendre. Then, we explicit the correspondence between these and quadratic fields. Finally, we study how some problems transpose in the two point of views, obtaining in this way answers to some of the questions asked above, and a proof of the Dirichlet class number formula. Notably, we meanwhile will study the relationships between class numbers of quadratic fields/class numbers of forms, norms of ideals/representations of integers by forms, and units in orders of quadratic fields/automorphisms of forms.

[3] Up to the fact that Gauss considered only forms whose coefficient of xy is even.

CHAPTER 1

BINARY QUADRATIC FORMS

In this first chapter, we introduce binary integral quadratic forms, representations problems, the notion of form equivalences and Gauss' theory of reduction.

Definition 1.1. A n**-ary integral quadratic form** is a homogeneous polynomial of degree 2 in $\mathbb{Z}[X_1, \ldots, X_n]$.

Definition 1.2. An integer m is said to be **represented** by a n-ary integral quadratic form f if there exists $x_1, \ldots, x_n \in \mathbb{Z}$ such that

$$f(x_1, \ldots, x_n) = m.$$

The point $(x_1, \ldots, x_n)$ is then called a **representation** of m by f. Moreover, we say that m is **properly represented** if there exists such integers which are relatively prime.

Remark 1.3. We note that each representation of a prime number is automatically a proper representation.

As we noted in the introduction, the following questions arise naturally:

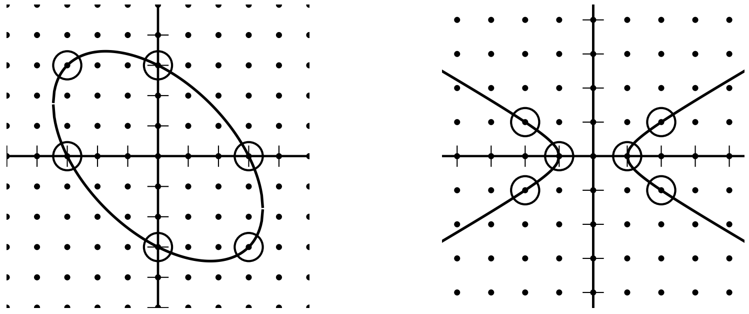
- Which integers can be represented by a given quadratic form?
- In how many ways can a given integer be represented by a given quadratic form?

Example 1.4. Famous examples of binary quadratic form are the forms $x^2 + ny^2$ for $n \in \mathbb{Z}$. When $n \geq 1$, Fermat conjectured congruence relations characterizing primes represented by some of these forms, later proven by Euler and Lagrange, which we will treat later on in this chapter. When n is negative, the representation problem $x^2 + ny^2 = 1$ defines the famous 'Pell's equation'.

Of course, since quadratic forms are *homogeneous* polynomials, it suffices to study forms whose coefficients are relatively prime, any quadratic form being equal to a square times such a form; whence the following definition:

Definition 1.5. A n-ary quadratic form is **primitive** if its coefficients are relatively prime integers.

In this document, we will mainly direct our attention to *binary* integral



(a) Representations of 9 by $x^2 + xy + y^2$.

(b) Representations of 1 by $x^2 - 3y^2$.

Figure 1.1: Representations of given integers by given forms.

quadratic forms, i.e. to polynomials of the form

$$ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y].$$

For the sake of simplicity, we will write only *form* or *quadratic form* instead of *integral binary quadratic form* in the rest of this document. Moreover, we will write $[a, b, c]$ with $a, b, c \in \mathbb{Z}$ for the form $ax^2 + bxy + cy^2$.

It will be useful to note that any binary form can be written matricially (being inspired by the general theory) in a unique way:

Definition 1.6. For a form f, the **matrix** of f is the unique 2×2 symmetric matrix M_f such that $f(x, y) = (x\,y)M_f\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$.

Explicitly, if $f = [a, b, c]$, we find at once that

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

1. Discriminants, definite and indefinite forms

Definition 1.7. The **discriminant** of a form $f = [a, b, c]$ is $\Delta(f) = b^2 - 4ac$.

Remark 1.8. The discriminant of f is related to the determinant of its matrix by $\Delta(f) = -4 \det M_f$. This will be useful in calculations.

Proposition 1.9. *The set of discriminants of forms is the set of integers d such that $d \equiv 0, 1 \pmod 4$.*

Proof. If d is the discriminant of a form $[a, b, c]$, then $d = b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod 4$, since the quadratic residues modulo 4 are 0 and 1. Conversely, if

$d \equiv 0, 1 \pmod 4$, consider the form

$$\begin{cases} [1, 0, -d/4] & \text{if } d \equiv 0 \pmod 4 \\ [1, 1, (1-d)/4] & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{1.1}$$

This form is called the **principal form** of discriminant d. □

Proposition 1.10. *Let f be a form of discriminant Δ. Then*

1. *if $\Delta > 0$, f represents both positive and negative integers;*
2. *if $\Delta < 0$, f represents either only positive, either only negative integers.*

Proof. Let $f = [a, b, c]$. If $a = c = 0$, then $\Delta(f) = b^2$ and the result is obvious. So we can suppose, by symmetry, that $a \neq 0$. Let us note that, by completing the square,

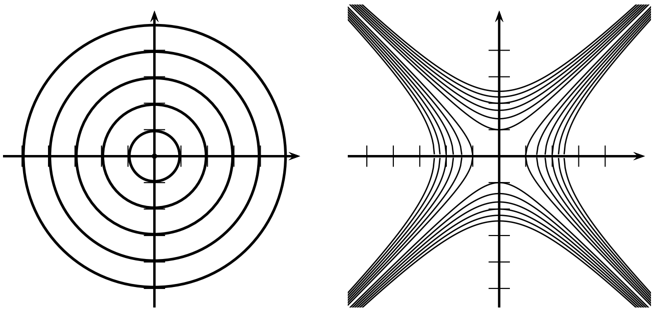
$$4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - \Delta y^2.$$

This expression is always positive if $\Delta < 0$, so f takes only positive or negative values according to the sign of a. On the other hand, if $\Delta > 0$, the right hand side expression represents positive (e.g. take $(x, y) = (1, 0)$) and negative integers (e.g. take $(x, y) = (-b, -2a)$), thus the same holds for f. □

This proposition leads to the following definition:

Definition 1.11. A form of positive discriminant is called **indefinite** and a form of negative discriminant is called **positive/negative definite**, according to whether it represents positive or negative integers.

Examples 1.12. The form $x^2 + y^2$ has discriminant -4 and represents $1 > 0$. It is therefore positive-definite. The form $x^2 - y^2$ has discriminant 4 and is indefinite.



(a) $x^2 + y^2$. (b) $x^2 - y^2$.

Figure 1.2: Level sets of a positive-definite form and an indefinite form.

Definition 1.13. Let $d \equiv 0, 1 \pmod 4$ be an integer. We will denote by $\mathrm{Form}_p(d)$ the set of all primitive binary quadratic forms of discriminant d.

2. Equivalence of forms

Given a quadratic form, we can naturally apply a linear change of variables to obtain a second one. More specifically, this yields to an action of the group $\mathrm{GL}_2(\mathbb{Z})$ of unimodular matrices on the set of forms:

Definition 1.14. Given a form $f = [a, b, c]$ and $\sigma \in \mathrm{GL}_2(\mathbb{Z})$, let σf be the form defined by

$$\sigma f(x, y) = f((x, y)\,\sigma).$$

In other words, we do the linear change of variable induced by σ.

This clearly defines an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of integral binary quadratic forms, since if f is a form and $\sigma, \tau \in \mathrm{GL}_2(\mathbb{Z})$, we have that

$$\sigma(\tau f)(x, y) = \tau f((x, y)\,\sigma) = f((x, y)\,\sigma\tau) = (\sigma\tau)f(x, y).$$

Therefore, we get an equivalence relation on the set of forms (namely two forms are equivalent if and only if they belong to the same orbit).

Remark 1.15. In the matrix form (see Definition 1.6), this means that $M_{\sigma f} = \sigma(M_f)\sigma^T$. Indeed, $\sigma f(x, y) = f((x, y)\,\sigma) = (x, y)\sigma(M_f)\,\sigma^T \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ and since $\sigma M_f \sigma^T$ is also symmetric, it is equal to $M_{\sigma f}$.

We note that this action preserves discriminants thanks to the fact that unimodular matrices have determinant ±1:

Proposition 1.16. *Two equivalent forms have the same discriminant.*

Proof. Let f and $\sigma \in \mathrm{GL}_2(\mathbb{Z})$. By Remarks 1.8 and 1.15, we find that

$$\Delta(\sigma f) = \det(M_{\sigma f}) = \det(\sigma(M_f)\sigma^T) = \det(\sigma)^2 \det(M_f) = \Delta(f).$$

Note that using matrices and determinants, we avoid all the calculations done in some books. □

2.1. First algebraic properties

The following property, relating the problem of integer representations with equivalence of forms, is fundamental and is one of the main reasons to consider this equivalence relation.

Proposition 1.17. *Two equivalent forms under the action of* $\mathrm{GL}_2(\mathbb{Z})$ *represent the same sets of integers.*

Proof. Let f be a form and $\sigma \in \mathrm{GL}_2(\mathbb{Z})$. If an integer n is represented by f, there exists $x, y \in \mathbb{Z}$ such that $f(x,y) = n$ and we see that $(x,y)\sigma^{-1} \in \mathbb{Z}^2$ represents n in σf. Conversely, if an integer n is represented by σf with $(x,y) \in \mathbb{Z}^2$, then $(x,y)\sigma \in \mathbb{Z}^2$ represents n in f. □

Example 1.18. The seemingly-complicated form $50x^2 + 214xy + 229y^2$ is actually equivalent to $x^2 + y^2$, under the action of $\left(\begin{smallmatrix} 2 & -1 \\ 15 & -7 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, since

$$\sigma \begin{pmatrix} 50 & 107 \\ 107 & 229 \end{pmatrix} \sigma^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore, studying the integers represented by the first one amounts to studying the integers that are sums of two squares, a problem solved by Fermat, which we will also shortly present and solve.

We already saw that the action of $\mathrm{GL}_2(\mathbb{Z})$ on forms behaved well with respect to discriminants. By Proposition 1.17, we have two other examples preserved sets of forms:

Corollary 1.19. *The action of* $\mathrm{GL}_2(\mathbb{Z})$ *on forms restricts to an action on positive-definite (resp. negative-definite) forms.*

Corollary 1.20. *The action of* $\mathrm{GL}_2(\mathbb{Z})$ *on forms restricts to an action on primitive forms.*

Proof. Let $f = [a, b, c]$ be a primitive form. If σf is not primitive, there exists $d > 1$ such that all integers represented by σf are in $d\mathbb{Z}$. By Proposition 1.17, the same holds for f. Thus $a = f(1,0), c = f(0,1)$ both lie in $d\mathbb{Z}$ and then also $b = f(1,1) - a - b \in d\mathbb{Z}$. This contradicts the primitivity of f. □

2.2. Proper and improper equivalence

Since the modular group $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$, the action above restricts to an action of $\mathrm{SL}_2(\mathbb{Z})$ on binary quadratic forms, which also yields to an equivalence relation.

Definition 1.21. Two binary quadratic forms equivalent under the action of $\mathrm{GL}_2(\mathbb{Z})$ are said **properly equivalent** (or simply **equivalent**) if they are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$. Otherwise, they are said to be **improperly equivalent**.

Remark 1.22. Note that proper equivalence is an equivalence relation, but improper equivalence is *not*: if f is improperly equivalent to g and g is improperly to h, then $f = \sigma h$ with $\sigma \in \mathrm{GL}_2(\mathbb{Z})$ such that $\det \sigma = (-1)^2 = 1$, i.e. f is properly equivalent to h.

Remark 1.23. Given a binary form $f = [a, b, c]$ with $ac \neq 0$, let us consider the roots of $f(\,\cdot\,, 1)$, namely $z_\pm = (-b \pm \sqrt{d})/(2a)$.

If $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, then a root z_σ of $\sigma f(\,\cdot\,, 1)$ verifies $f(az_\sigma + c, bz_\sigma + d) = 0$. If $ac \neq 0$, we have that that $bz_\sigma + d$, so

$$f\left(\frac{az_\sigma + c}{bz_\sigma + d}, 1\right) = 0.$$

It implies that $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of the roots of $f(\,\cdot\,, 1)$ by the restriction of its action on the projective line $\mathrm{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ through

$$z \mapsto \sigma^{-T} z.$$

In particular, if $\Delta(f) < 0$, we can consider the root z of $f(\,\cdot\,, 1)$ with positive imaginary part, i.e. $z \in \mathbb{H}$. Therefore, the classical action $\mathrm{SL}_2(\mathbb{Z})$ on the Poincare half-plane $\mathbb{H}$ gives a left-action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ given by

$$\sigma \star z = \sigma^{-T} z,$$

which compatible with the action on forms, in the sense that $z \star \sigma$ is the root of σf belonging to $\mathbb{H}$.

By Proposition 1.16 and Corollaries 1.20, 1.19, we can do the following definition:

Definition 1.24. Let $d \equiv 0, 1 \pmod 4$ be an integer. We denote by

- $C(d)$ the set of classes of integral binary quadratic forms of discriminant d;
- $C_p(d)$ the intersection of $C(d)$ with the set of classes of primitive binary quadratic forms;
- $C_p^+(d)$ the intersection of $C_p(d)$ with the set of classes of binary quadratic forms which are positive-definite if $d < 0$.

Lemma 1.25. *A form properly represents an integer n if and only if it is properly equivalent to a form $[n, b', c']$, with $b', c' \in \mathbb{Z}$.*

Proof. If $f = [a, b, c]$ properly represents n, say $ax^2 + bxy + cy^2 = n$ with $x, y \in \mathbb{Z}$ coprime, we consider a Bezout identity $\alpha x + \beta y = 1$ with $\alpha, \beta \in \mathbb{Z}$. Let

$$\sigma = \begin{pmatrix} x & y \\ -\beta & \alpha \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Using Remark 1.15, we compute that the coefficient of X^2 in σf is $ax^2+bxy+cy^2=n$. The converse is obvious. □

The interest of proper equivalence (and the origin of the terminology) is that proper representation of an integer is conserved under proper equivalence:

Corollary 1.26. *Properly equivalent forms represent properly exactly the same sets of integers.*

Proof. This is a consequence of Lemma 1.25 and Proposition 1.17. Let f_1 and f_2 be two properly equivalent forms. If f_1 properly represents an integer n, then f_1 is properly equivalent to a form $[n,b',c']$ ($b',c' \in \mathbb{Z}$), which is then properly equivalent to f_2. Using the converse of the Lemma gives that n is properly represented by f_2. □

Remark 1.27. The converse is not true. For example, we will see later that the positive-definite forms $[2,1,3]$ and $[2,-1,3]$ are not equivalent. However, they clearly represent the same integers.

2.3. Integers represented by some form of given discriminant

The problem of determining which integers are represented by a given form is in general not easy, but the following Proposition gives an easy criterion to determine when an integer is represented by *some* form of given discriminant.

Proposition 1.28. *Let d be an integer such that $d \equiv 0,1 \pmod 4$. Then an integer n coprime to d is properly represented by a primitive form of discriminant d if and only if d is a square modulo $4n$.*

Proof. Suppose that an integer n coprime to d is properly represented by a primitive form f of discriminant d, say $ax^2+bxy+cy^2=n$ for $x,y \in \mathbb{Z}$ coprime. By Lemma 1.25, f is equivalent to a form $\hat{f}=[n,b,c]$ with $b,c \in \mathbb{Z}$. By Proposition 1.16,

$$D = \Delta(\hat{f}) = b^2-4nc \equiv b^2 \pmod{4n}.$$

Conversely, let n an integer coprime to d such that there exists $b \in \mathbb{Z}$ with $d \equiv b^2 \pmod{4n}$. In other words, there exists $c \in \mathbb{Z}$ such that $d=b^2-4nc$. The form $[n,b,c]$ has discriminant d and properly represents n. Moreover, it is primitive, since if e divides n,b,c, it also divides d, which implies that $e=\pm 1$ because n and d are coprime. □

Remark 1.29. We will strongly refine this proof later to explicitly obtain the number of representations modulo some equivalence relation of an integer by classes of forms.

Remark 1.30. Note that if n is odd, then such a d is a square modulo $4n$ if and only if it is a square of modulo n. Indeed, if $d = b^2 + nc$ with $b, c \in \mathbb{Z}$, we can suppose that d and b have the same parity, because n is odd. Since $d \equiv 0, 1 \pmod 4$, we get that $nc \in 4\mathbb{Z}$, so $d \equiv b^2 \pmod{4n}$.

Corollary 1.31. *Let n be an integer and p be a prime not dividing $4n$. Then p is represented by a primitive form of discriminant $-4n$ if and only if*

$$\left(\frac{-n}{p}\right) = 1.$$

Proof. By Proposition 1.28, the prime p is represented by a primitive form of discriminant $-4n$ if and only if $-4n$ is a square mod $4p$, namely if and only if $\left(\frac{-n}{p}\right) = 1$. □

Example 1.32. Let p be an odd prime. Because $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$, p is represented by a form of discriminant -4 if and only if $p \equiv 1 \pmod 4$. We will soon see that we can actually give explicitly the forms representing p under this condition.

2.4. Automorphisms

Definition 1.33. An **automorphism** of a form f is an element of the isotropy group $\mathrm{Aut}(f)$ of f under the action of $\mathrm{SL}_2(\mathbb{Z})$. In other words, $\sigma \in \mathrm{Aut}(f)$ if and only if $\sigma f = f$.

We will shortly see that automorphisms play an important role in the questions concerning representation of integers by forms. In the following chapter, we will furthermore answer the following questions: does a given form have infinitely many automorphisms? Otherwise how many? Can they be parametrized?

Example 1.34. Any form has the two trivial automorphisms

$$\text{id and } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Proposition 1.35. *If f and g are two equivalent forms, i.e. $f = \sigma g$ with $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, then $Aut(f) = \sigma Aut(g) \sigma^{-1}$.*

Proof. An element $\tau \in \mathrm{SL}_2(\mathbb{Z})$ belongs to $\mathrm{Aut}(f)$ if and only if $\tau f = f$, i.e. if and only if $\tau\sigma g = \sigma g$, which is finally equivalent to $\sigma^{-1}\tau\sigma \in \mathrm{Aut}(g)$. The result follows by symmetry. □

3. Reduction of definite forms

Since equivalent forms represent the same integers, it would be very useful to be able to determine a complete reduced system of representatives of equivalence classes. In the following two sections, we will show that it is possible and easy, as Gauss discovered. More precisely, we will show that there is only a finite number of equivalence classes of forms of given discriminants and we will give a method to list them.

In this section, we begin with definite forms. Without loss of generality for our considerations, we can focus only on *positive*-definite forms, since any negative-definite form is equal to -1 times a positive-definite one. Note that a positive-definite form $[a, b, c]$ verifies $a, c > 0$, because a and c are trivially represented. We can also restrict ourselves to primitive forms as we remarked before.

Definition 1.36. A primitive positive-definite form $[a, b, c]$ is **reduced** if

$$|b| \leq a \leq c$$

and if $b \geq 0$ as soon as one of the inequalities is an equality.

Example 1.37. The principal forms (1.1) are always reduced forms. The form $[2, 1, 6]$ is reduced, but $[16, 23, 9]$ is not.

Remark 1.38. Following Remark 1.23, let us consider a primitive positive-definite form $f = [a, b, c]$ of discriminant d with $z = (-b + \sqrt{d})/(2a) \in \mathbb{H}$ the root of $f(\cdot, 1)$ in the Poincare half-plane. We note that f if reduced if and only if z belongs to the fundamental region

$$E_{\mathrm{SL}_2(\mathbb{Z})} = \{z = x + iy \in \mathbb{H} : |x| < 1/2 \text{ and } (|z| > 1 \text{ or } (|z| = 1, x \leq 0))\},$$

of $\mathrm{SL}_2(\mathbb{Z})$. Indeed, we have $|z| = \sqrt{c/a}$ and $|\mathrm{Re}(z)| = |b/(2a)|$. If f is reduced, then $|z| \geq 1$, $|\mathrm{Re}(z)| \leq 1/2$ and if one of these inequalities is not strict, then $\mathrm{Re}(z) \leq 0$. The converse holds by the same argument.

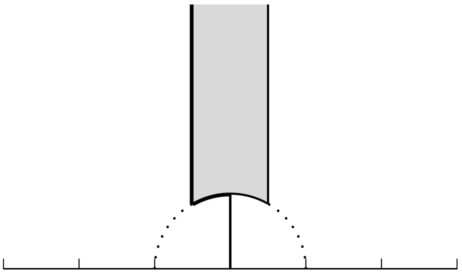


Figure 1.3: The fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ in $\mathbb{H}$.

We shortly remark the following property of reduced forms and the integers they represent.

Proposition 1.39. *The smallest non-zero integer represented by a reduced form $[a, b, c]$ is a.*

Proof. Denote the form by $f = [a, b, c]$. The value a is clearly represented, since $a = f(1, 0)$. Moreover, if $x, y \neq 0$, then

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

Since $f(x, 0) = ax^2 \geq a$ and $f(0, y) = cy^2 \geq ay^2 \geq a$ for all $x, y \in \mathbb{Z}$, the proof is done. □

The following Theorem shows that reduced forms constitute a complete reduced system of representatives of classes of $\mathrm{Form}_p(d)$ for a given discriminant d, which is hence very nice.

Theorem 1.40. *Every primitive positive-definite form is properly equivalent to a unique reduced form.*

Proof. First, we show that any positive-definite primitive form f is equivalent to a reduced form. In the equivalence class of f, let $g = [a, b, c]$ with $|b|$ minimal. If $|b| > a$, let $m \in \mathbb{Z}$ and

$$\sigma = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Using Remark 1.15, we see that the coefficient of xy in σg is $2am + b$. Since $a \geq 0$ and $|b|/a > 1$, we can find $m \in \mathbb{Z}$ such that $|2a/bm + 1| < 1$. In other words, we can find a form equivalent to f whose coefficient of xy is $2am + b$ with $|2am + b| < |b|$, which would contradict the minimality of $|b|$. Therefore, $|b| \leq a$. By symmetry, we also find that $|b| \leq c$. If $a > c$, we apply

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

to g to get the form $[a', b', c'] = [c, -b, a]$ equivalent to g (and therefore to f), which satisfies $|b'| \leq a' \leq c'$. For the sake of clarity, let us denote a', b', c' by a, b, c again. This new form is reduced if the two inequalities are strict or if $b \geq 0$.

Otherwise, when $b < 0$ and $a = -b, c$, we prove that the reduced form $[a, -b, c]$ is properly equivalent to $[a, b, c]$. Indeed, consider $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ defined by

$$\sigma = \begin{cases} \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) & \text{if } a = -b \\ \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) & \text{if } a = c \end{cases}$$

Then $\sigma[a, -b, c] = [a, b, c]$. This concludes the proof that any positive-definite form is equivalent to a reduced form.

Now, we prove that in each equivalence class lies only one reduced form. Let $f = [a, b, c]$ be a reduced form. We first prove that if $[a', b', c']$ is equivalent to f, then $a \leq a'$. Indeed, let $\sigma = \left(\begin{smallmatrix} \alpha & \gamma \\ \beta & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ such that $\sigma[a, b, c] = [a', b', c']$. Suppose that $\alpha, \gamma \neq 0$. As before, we determine using the matrix of f that

$$a' = \alpha^2 a + \alpha\gamma b + \gamma^2 c = \alpha^2 a \left(1 + \frac{b\gamma}{a\alpha}\right) + \gamma^2 c = \alpha^2 a + \gamma^2 c \left(1 + \frac{b\alpha}{c\gamma}\right). \quad (1.2)$$

If $\gamma/\alpha \leq 1$, then, using the first equality,

$$a' \geq a \left(\alpha^2 \left(1 + \frac{b\gamma}{a\alpha}\right) + \gamma^2\right) \geq a \left(\alpha^2 \left(1 - \frac{\gamma}{\alpha}\right) + \gamma^2\right) \geq a,$$

If $\gamma/\alpha > 1$, we use the second equality to conclude the same thing.

Finally, if $\gamma = 0$, then $\sigma = \begin{pmatrix} \pm 1 & 0 \\ \beta & \pm 1 \end{pmatrix}$ and $a' = a$. If $\alpha = 0$, then $\sigma = \left(\begin{smallmatrix} 0 & \mp 1 \\ \pm 1 & \delta \end{smallmatrix}\right)$ and $a' = -c \leq -a < a$.

Thus if $[a', b', c']$ is a reduced form equivalent to $[a, b, c]$, then $a' = a$ by symmetry. Since a and c are coprime, Equation (1.2) gives that $\alpha = \pm 1$ and $\gamma = 0$, whence $\sigma = \begin{pmatrix} \pm 1 & 0 \\ \beta & \pm 1 \end{pmatrix}$. In other words, $b' = b \pm 2\beta a$. Since $|b|, |b'| \leq a = a'$, we have $\beta = 0$ and $\sigma = \mathrm{id}$, which finally gives $[a', b', c'] = \sigma[a, b, c] = [a, b, c]$. □

Proposition 1.41. *The number of classes of positive-definite forms of given discriminant is finite.*

Proof. Let $[a, b, c]$ be a reduced form of discriminant $d < 0$, namely $d = b^2 - 4ac$. Since the form is reduced, we have that $b^2 \leq a^2 \leq ac$, thus

$$d = b^2 - 4ac \leq -3ac,$$

or equivalently $ac \leq -d/3$. This implies that there is only a finite number of choices for a and c. Since b is bounded in absolute value by a and c, we deduce that there is only a finite number of reduced forms. By Theorem 1.40, this implies the result. □

Definition 1.42. For $d < 0$ an integer such that $d \equiv 0, 1 \pmod 4$, we let $h_f(d)$ be the number of equivalence classes of primitive positive-definite forms, called the **form class number** of discriminant d.

3.1. Determination of the class number and reduced classes

The proofs above of the existence of a unique reduced form in each class and of the finiteness of class number give simple algorithms to compute reduced forms and class numbers. We formalize them below and apply them to several examples.

Algorithm 1.43 (determination of a reduced representative)**.** Let $f = [a, b, c]$ be a primitive positive-definite form. While f is not reduced, do the following:

- If $a > c$ or ($c = a$ and $b < 0$), then replace f by the equivalent form $[c, -b, a]$.
- If $|b| > a$ or $b = -a$, then replace f by the equivalent form $[a, b', c']$ where $b' \equiv b \pmod{2a}$, $-a < b' \leq a$ and $c' = ((b')^2 - D)/(4a)$.

Then this procedure ends in a finite number of steps and gives the reduced form equivalent to f.

Proof. The transformations correspond respectively to the actions of

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

on $[a, b, c]$, with k such that $b' = b + 2ak$, $-a < b' \leq a$ as we saw during the proof of Theorem 1.40. At each step, we have that $a' + |b'| < a + |b|$, except when

- $c = a$ in the first condition. Here, $[a, b, a]$ will be transformed to $[a, -b, a]$ and the algorithm ends.
- $b = -a$ in the second condition. There, $[a, -a, c]$ will be transformed to $[a, a, c]$ and the algorithm ends.

Therefore, the algorithm always ends in a finite number of steps. □

Remark 1.44. Following Remarks 1.38 and 1.23, we see that given $f = [a, b, c]$ a primitive positive-definite form, the algorithm acts on the root z of f belonging to the Poincare half-plane $\mathbb{H}$ by

$$z \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-T} z = \frac{-1}{z} \text{ and } z \mapsto \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}^{-T} z = z - k$$

until it belongs the the fundamental region $E_{\mathrm{SL}_2(\mathbb{Z})}$.

Example 1.45. We apply the above algorithm to find the reduced form equivalent to $f = [16, 23, 9]$:

$$[16, 23, 9] \to [9, -23, 16] \to [9, -5, 2] \to [2, 5, 9] \to [2, 1, 6].$$

The successive transformations of the roots in the half-plane are illustrated in Figure 1.4. Similarly, we find that $g = [64, 73, 21]$ is also equivalent to $[2, 1, 6]$. Therefore, f and g are equivalent, since $[2, 1, 6]$ is reduced.

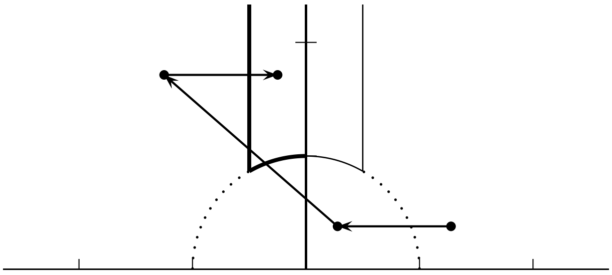


Figure 1.4: Reduction of the form $[16, 23, 9]$: action on the roots in $\mathbb{H}$.

Algorithm 1.46 (determination of all reduced forms of given discriminant)**.** Let $d < 0$ be a negative integer such that $d \equiv 0, 1 \pmod 4$. All reduced forms lie in the set

$$\{[c, b, n/c] : -d/4 \leq n \leq -d/3,\ c|n,\ c^2 \leq n,\ c^2 + 4n = b^2\},$$

so it suffices to test a finite number of triples (in $O(d^2)$).

Proof. We saw in the proof of Proposition 1.41 that if $[a, b, c]$ is a reduced form of discriminant d, then $ac \leq -d/3$. Moreover, since $d + 4ac = b^2 \geq 0$, we have that $ac \geq -d/4$ and $d + 4ac$ is a perfect square. □

Example 1.47. If $d = -28$, a reduced form $[a, b, c]$ of discriminant d verifies especially $7 \leq ac \leq 9$. Since $-28 + 4 \cdot 9 = 8$ is not a perfect square, the case $ac = 9$ is excluded. For $ac = 8$, the possibilities are $[1, \pm 4, 8]$ and $[2, \pm 4, 8]$, which are not reduced. For $ac = 7$, the only possibility is the form $[1, 0, 7]$, which is therefore the only reduced form of discriminant -28. In other words, $h_f(-28) = 1$.

Example 1.48. Similarly, we easily compute that there are 5 reduced classes of discriminant -47, given by

$$[1, 1, 12], [2, 1, 6], [2, -1, 6], [3, 1, 4], [3, -1, 4].$$

By Theorem 1.40, this is a complete system of representatives of equivalence classes of forms of discriminant -47 and $h_f(-47) = 5$.

Example 1.49. In Table 1.1, we give more generally the values of $h_f(d)$ for discriminants $-180 \leq d < 0$, computed using the above algorithm implemented on a computer

d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$
-3	①	-39	4	-75	2	-111	8	-147	2
-4	①	-40	2	-76	3	-112	2	-148	2
-7	①	-43	①	-79	5	-115	2	-151	7
-8	①	-44	3	-80	4	-116	6	-152	6
-11	①	-47	5	-83	3	-119	10	-155	4
-12	①	-48	2	-84	4	-120	4	-156	4
-15	2	-51	2	-87	6	-123	2	-159	10
-16	①	-52	2	-88	2	-124	3	-160	4
-19	①	-55	4	-91	2	-127	5	-163	①
-20	2	-56	4	-92	3	-128	4	-164	8
-23	3	-59	3	-95	8	-131	5	-167	11
-24	2	-60	2	-96	4	-132	4	-168	4
-27	①	-63	4	-99	2	-135	6	-171	4
-28	①	-64	2	-100	2	-136	4	-172	3
-31	3	-67	①	-103	5	-139	3	-175	6
-32	2	-68	4	-104	6	-140	6	-176	6
-35	2	-71	7	-107	3	-143	10	-179	5
-36	2	-72	2	-108	3	-144	4	-180	4

Table 1.1: Values of $h_f(d)$ for discriminants $-180 \leq d \leq 1$.

4. Reduction of indefinite forms

For indefinite binary quadratic forms, a similar theory of reduction still exists, also developed by Gauss, but things are a little harder as we will shortly see.

In the following section, all discriminants will be supposed nonsquare. The case of square discriminants is easier, but asks for some work which is less interesting and too lengthy for this document. All the details for this case are available in articles 206-212 of the *Disquisitiones Arithmeticae* [Gau86].

Definition 1.50. A primitive indefinite form $[a, b, c]$ of a nonsquare discriminant $d > 0$ is **reduced** if $|2|a| - \sqrt{d}| < b < \sqrt{d}$.

Remark 1.51. Following Remark 1.23, let us consider an indefinite form $f = [a, b, c]$ of discriminant $d > 0$ with $\rho_\pm = (-b \pm \sqrt{d})/(2a) \in \mathbb{R}$ the roots of $f(\,\cdot\,, 1)$. We note that f if reduced if and only if

$$|\rho_+| < 1 < |\rho_-| \text{ and } \rho_+\rho_- < 0.$$

Indeed, note that $\rho_+\rho_- = 2ac = 2(b^2 - d)$. Therefore, if f satisfies $|\rho_+| < 1 < |\rho_-|$ and $\rho_+\rho_- < 0$, we get that $|b| < \sqrt{d}$, so the first two inequalities give

$$-b + \sqrt{d} < 2|a| < b + \sqrt{d}$$

thus $b > 0$ and $|2|a| - \sqrt{d}| < b$. The converse is similar.

As for the positive-definite case, there are only finitely many reduced indefinite forms of given discriminant:

Proposition 1.52. *For any nonsquare discriminant $d > 0$, there are only finitely many reduced indefinite forms of discriminant d.*

Proof. If $[a, b, c]$ is an indefinite reduced form of discriminant d, this is,

$$|2|a| - \sqrt{d}| < b < \sqrt{d},$$

we get that $0 < b < \sqrt{d}$ by the second inequality. The first ones gives

$$4a^2 + (b^2 - 4ac) - 4|a|\sqrt{d} < b^2, \text{ so}$$

$$a^2 - ac < |a|\sqrt{d},$$

whence $|a| - \operatorname{sgn}(a)c < \sqrt{d}$. But $4ac = b^2 - d < 0$, so a and c have opposed signs, which implies then by the preceding inequality that $|a|+|c| < \sqrt{d}$. Since a, b, c are integers, the claim follows. □

Using the proof of Proposition 1.52, the set of reduced form with given discriminant $d > 0$ can easily be determined by trying all forms $[a, b, c]$ with $0 < b < \sqrt{d}$, $|a| + |c| < \sqrt{d}$ and $b^2 - 4ac = d$.

Example 1.53. For $d = 12 \equiv 0 \pmod 4$, there are exactly 4 reduced forms, given by

$$[-2, 2, 1], [-1, 2, 2], [1, 2, -2], [2, 2, -1].$$

Similarly, for $d = 17 \equiv 1 \pmod 4$, we find exactly 6 reduced forms

$$[-2, 1, 2], [2, 1, -2], [-2, 3, 1], [-1, 3, 2], [1, 3, -2], [2, 3, -1].$$

For positive-definite forms, we saw that there is exactly one reduced form in each $\mathrm{SL}_2(\mathbb{Z})$-equivalence class, which allowed to easily compute a complete system of representatives of $C_p^+(d)$ by finding all reduced forms of discriminant d. In the indefinite case, we will now show that there is still at least one reduced form in each equivalence class, but there might be more than one.

Recall that to reduce positive-definite forms, we used the two transformations

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

changing $[a, b, c]$ to $[a, -b, c]$ and $[c, b', c']$ respectively, where b' can be chosen modulo $2a$.

Combining the two transformations, we see that a form $[a, b, c]$ is equivalent to the forms $[c, b', c']$ for all $b \equiv -b \pmod{2c}$, with c' uniquely determined by the invariance of discriminants (i.e. $c = ((b')^2 - \Delta([a, b, c]))/(4a))$. Two such forms are called **neighbors** (note that it is clearly a symmetric relation).

Gauss gave an algorithm to obtain a reduced form by passing from neighbor to neighbor[1]:

Algorithm 1.54 (Reduction of indefinite forms)**.** Let $[a, b, c]$ be an indefinite primitive form of nonsquare discriminant $d > 0$.

1. If $[a, b, c]$ is reduced, end the algorithm
2. Let $b' \in \mathbb{Z}$ be such that $b' \equiv -b \pmod{2c}$ and
   a) $-|c| < b' \leq |c|$ if $|c| > \sqrt{d}$;
   b) $\sqrt{d} - 2|c| < b' < \sqrt{d}$ if $|c| < \sqrt{d}$.
3. Continue the algorithm with the neighbour $\rho([a, b, c]) := [c, b', c']$, where $c' = ((b')^2 - d)/(4c)$.

Note that c is never equal to $\sqrt{d}$ since d is supposed nonsquare.

Lemma 1.55. *The indefinite form reduction algorithm (Algorithm 1.54) terminates.*

Proof. Let $[a_0, b_0, c_0]$ be a form of discriminant $d > 0$. We prove that at each step $i \geq 1$, either the neighbor $[a_i, b_i, c_i]$ is reduced, or it satisfies $|c_i| < |c_{i-1|}$. Since the c_i are integers, the algorithm must terminate (in at most c_i iterations).

Indeed, in case 2.a), the form $[a_i, b_i, c_i]$ obtained from $[a_{i-1}, b_{i-1}, c_{i-1}]$ verifies $|b_i| \leq |c_{i-1}|$, thus

$$|c_i| = \frac{|d - b_i^2|}{4|c_{i-1}|} \leq \frac{|d| + |b_i|^2}{4|c_{i-1}|} \leq \frac{2|c_{i-1}|^2}{4|c_{i-1}|}$$

and $|c_i| < |c_{i-1}|$. In case 2.b), note that if $2|c_{i-1}| \leq \sqrt{d}$, then the form $[a_i, b_i, c_i]$ obtained from $[a_{i-1}, b_{i-1}, c_{i-1}]$ is reduced. Indeed, by the choice of b',

$$|\sqrt{d} - 2|a_i|| = \sqrt{d} - 2|c_{i-1}| < b_i < \sqrt{d}.$$

Otherwise, if $2|c_{i-1}| > \sqrt{d}$, we have that

$$|c_i| = \frac{d - b_i^2}{4|c_{i-1}|} \leq \frac{d}{4|c_{i-1}|} < |c_{i-1}|.$$

□

[1] Article 171 of the *Disquisitiones Arithmeticae* [Gau86]. However, note that the algorithm that we give is not *exactly* Gauss's, since he only worked with forms $[a, b, c]$ having b even.

Remark 1.56. Let f be an indefinite form. Following Remarks 1.23 and 1.51, we remark that Algorithm 1.54 acts on the roots $\rho_\pm$ of $f(\,\cdot\,,1)$ with the transformations

$$x \mapsto \frac{-1}{x} + k \ (k \in \mathbb{Z})$$

(see Remark 1.44) until they verify $|\rho_+| < 1 < |\rho_-|$ and $\rho_+\rho_- < 0$, i.e. when f is reduced.

Example 1.57. The reduction algorithm on the form $[333, 278, 58]$ passes through the forms

$$[333, 278, 58] \to [58, -46, 9] \to [9, -8, 1] \to [1, 4, -3]$$

and $[1, 4, -3]$ is reduced. Figure 1.5 illustrates the transformations of the roots noted in Remark 1.56.

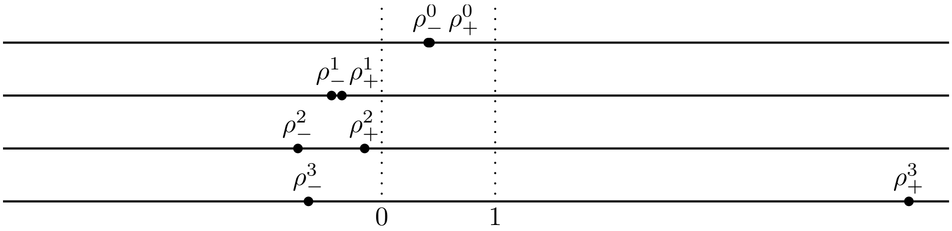


Figure 1.5: Transformation of the roots during the reduction of $[333, 278, 58]$ with discriminant 28. The solid lines represent segments of the real line, the intersection with the dotted line being the zeroes associated to the forms.

As an immediate consequence of Lemma 1.55 and Proposition 1.52, we have the following results:

Proposition 1.58. *Every primitive indefinite form is equivalent to some reduced form.*

Corollary 1.59. *There are only finitely many equivalence classes of primitive indefinite forms of given discriminant.*

As for the positive-definite case, we denote by $h_f(d)$, the **form class number**, the number of equivalence classes of primitive binary quadratic forms of discriminant $d > 0$.

Practically, there is one problem left: for a discriminant $d > 0$, we can determine a set of representatives of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes by reduced classes, but this set could contain two equivalent forms. Hence, we need a way to determine the reduced forms equivalent to such a form given.

The next Proposition explains the relationship between two equivalent reduced forms and gives such a method.

Proposition 1.60. *If f is a reduced indefinite form, there exists $n \geq 1$ such that the reduced forms equivalent to f are precisely*

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

where $\rho : \mathit{Form}_p(d) \to \mathit{Form}_p(d)$ is the application defined in Algorithm 1.54.

Proof. Let $d > 0$ be a discriminant and $f \in \mathrm{Form}_p(d)$. We note that ρ restricts to an application

$$\rho' : \mathrm{orb}_{\mathrm{SL}_2(\mathbb{Z})}(f) \cap R \to \mathrm{orb}_{\mathrm{SL}_2(\mathbb{Z})}(f) \cap R,$$

where R denotes the set of reduced indefinite forms. Indeed, suppose that $[a, b, c]$ is reduced. Remark that $|c| < \sqrt{d}$ since $|a| + |c| < \sqrt{d}$ by the proof of Proposition 1.52. We saw in the proof of Lemma 1.55 that $\rho([a, b, c]) = [c, b', c']$ is reduced if $2|c| \leq \sqrt{d}$. If $2|c| > \sqrt{d}$, then

$$|2|c| - \sqrt{d}| = 2|c| - \sqrt{d} < b' < \sqrt{d}$$

by definition of b', since $|c| < \sqrt{d}$.

Moreover, note that ρ' is injective since if $\rho([a_1, b_1, c_1]) = \rho([a_2, b_2, c_2])$, then $c_1 = c_2$. By definition of ρ, we must have $b_1 = b_2$ and finally $a_1 = a_2$ by invariance of the discriminant.

By the finiteness of the number of reduced classes (Proposition 1.52), the map ρ' is bijective and

$$\mathrm{orb}_{\mathrm{SL}_2(\mathbb{Z})}(f) \cap R = \{\rho(f), \rho^2(f), \ldots, \rho^n(f)\}$$

for some $n \geq 1$, since $\rho(g) \neq g$ for all $g \in R$ (otherwise, we get that $c|b$, contradicting the primitivity). □

Algorithm 1.61 (Determination of a complete system of representatives of $\mathrm{SL}_2(\mathbb{Z})$ equivalence classes of indefinite forms with given discriminant.)**.** Let $d > 0$ be a positive discriminant.

1. Determine the set R of all reduced forms of discriminant d using Proposition 1.52;
2. For each reduced form f, compute $\rho^n(f)$ ($n \geq 1$) until obtaining a cycle $f, \rho(f), \ldots, \rho^N(f), \rho^{N+1}(f) = f$. Remove $\rho^i(f)$ from R for $1 \leq i \leq N$.
3. R is a complete reduced system of representatives of $\mathrm{SL}_2(\mathbb{Z})$ equivalence classes of indefinite forms with discriminant d.

d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$
5	①	52	2	92	①	132	2	172	①
8	①	53	①	93	①	133	①	173	①
12	①	56	①	96	3	136	2	176	2
13	①	57	①	97	①	137	①	177	①
17	①	60	2	101	①	140	2	180	4
20	2	61	①	104	2	141	①	181	①
21	①	65	2	105	2	145	4	184	①
24	①	68	2	108	2	148	4	185	2
28	①	69	①	109	①	149	①	188	①
29	①	72	2	112	2	152	①	189	2
32	2	73	①	113	①	153	2	192	4
33	①	76	①	116	2	156	2	193	①
37	①	77	①	117	2	157	①	197	①
40	2	80	3	120	2	160	4	200	3
41	①	84	2	124	①	161	①	201	①
44	①	85	2	125	2	164	2	204	2
45	2	88	①	128	3	165	2	205	2
48	2	89	①	129	①	168	2	208	3

Table 1.2: Values of $h_f(d)$ for nonsquare discriminants $1 \leq d \leq 208$.

Example 1.62. We saw that for $d = 12 \equiv 0 \pmod 4$, there are exactly 4 reduced forms:

$$[-2,2,1],[-1,2,2],[1,2,-2],[2,2,-1].$$

The cycle associated to $[-2,2,1]$ is $[-2,2,1],[1,2,-2],[-2,2,1],\dots$ and the cycle associated to $[-1,2,2]$ is $[-1,2,2],[2,2,-1],[-1,2,2],\dots$ Therefore, a complete reduced set of reduced representatives of $C_p^+(12)$ is given by

$$[-2,2,1],[-1,2,2].$$

Example 1.63. For $d = 41 \equiv 1 \pmod 4$, we find that there are 10 reduced forms, but since the cycle associated to $[-4,3,2]$ is

$$\begin{aligned}&[-4,3,2],[2,5,-2],[-2,3,4],[4,5,-1],[-1,5,4],\\&[4,3,-2],[-2,5,2],[2,3,-4],[-4,5,1],[1,5,-4],[-4,3,2],\dots\end{aligned}$$

of length 10, there is only one $\mathrm{SL}_2(\mathbb{Z})$ equivalence class.

Example 1.64. Implementing this algorithm on a computer, we find Table 1.2, similar to Table 1.1.

5. Primes represented by a positive-definite form of discriminant with class number one

After these considerations on the structure of equivalence classes of forms, we can come back to representation problems, more precisely to the question of determining which primes are represented by a given form. Although it is not easy to answer it in a general setting, the case of forms with discriminant with class number one is simple.

Indeed, the criterion of Proposition 1.28 lets us know when an integer is represented by *some* form of discriminant d. When $h_f(d) = 1$, all forms are mutually equivalent and since equivalent forms properly represent the same integers (Corollary 1.26), this criterion lets us know when an integer is represented by a *given* form. We record this fact in the following Proposition:

Proposition 1.65. *Let f be a positive-definite form of discriminant d. Suppose that $h_f(d) = 1$. Then an integer n coprime to d is properly represented by f if and only if d is a square modulo $4n$.*

Corollary 1.66. *Let f be a positive-definite form of discriminant $4n$ with $n \geq 1$. Suppose that $h(4n) = 1$. Then an odd prime p not dividing n is properly represented by f if and only if $\left(\frac{-n}{p}\right) = 1$.*

Proof. See Corollary 1.31. □

5.1. Examples

Using the preceding results, we can now characterize primes represented by some quadratic forms.

Proposition 1.67. *If $n = 1, 2, 3, 4, 7$ and $p \neq n$ is an odd prime,*

$$p \textit{ is represented by } x^2 + ny^2 \quad \Leftrightarrow \quad \left(\frac{-n}{p}\right) = 1.$$

Proof. We see in table 1.1 that $h_f(-4n) = 1$ for $n = 1, 2, 3, 4, 7$. Since the discriminant of the form $[1, 0, n]$ is $-4n$, we conclude by Corollary 1.66. □

The case $n = 1$ asserts that a prime p is the sum of two squares if and only if -1 is a square modulo p, i.e. $p \equiv 1 \pmod 4$ by the first complement to the quadratic reciprocity law. This is exactly Fermat's famous *two squares theorem* (1640), proven by Lagrange and Gauss. This proof using quadratic forms is actually Lagrange's.

Remark 1.68. A classical proof of the two squares theorem uses considerations about the ring of integers $\mathbb{Z}[i]$ of the quadratic field $\mathbb{Q}(i)$. However, at the time of the discovery of a proof, in the XVIII$^{\text{th}}$ century, ideals and number fields were not yet formalized and the proof given by Lagrange and Gauss is the above one, with quadratic forms. In the following chapters, we will show that these domains are actually perfectly connected (and this partly led to the formalization of ideals/ideals class groups, see [Kle07]).

The other cases are generalization of the two squares theorem, conjectured by Fermat for $n = 2, 3$. Using quadratic reciprocity, we can similarly give congruence conditions for a prime to be represented as $x^2 + ny^2$ for $n = 1, 2, 3, 4, 7$.

For example, let p an odd prime. By Proposition 1.67, p can be written as $x^2 + y^2$ with $x, y \in \mathbb{Z}$ if and only if $\left(\frac{-2}{p}\right) = 1$. By the complementary laws to the quadratic reciprocity,

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod 8 \\ -1 & \text{otherwise,} \end{cases} \tag{1.3}$$

whence $p = x^2 + 2xy^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 3 \pmod 8$.

To study primes represented by $x^2 + 3y^2$, we remark that

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right),$$

so $x^2 + 3y^2$ represents primes p such that $p = 3$ or $p \equiv 3 \pmod 3$. The other cases are similar.

Remark 1.69. Congruence conditions on representations of integer by forms of discriminants whose class number is not 1 can also be discussed, using the *genus theory* developed by Legendre. However, this is not the subject of this project (see the Conclusion for some perspectives).

CHAPTER 2

QUADRATIC FIELDS AND BINARY QUADRATIC FORMS

In this chapter, we show the deep relationship between classes of binary quadratic forms and class groups/Picard groups in orders of quadratic fields.

We begin by recalling some definitions and results about quadratic fields and their orders. Then, we show how integral binary quadratic forms can be associated to ideals of such orders and vice-versa. At the end of this chapter, we will have given a complete correspondence between ideals of orders of quadratic fields and classes of integral binary quadratic forms.

1. Quadratic fields

In Appendix A, the most important definitions and results about number fields and their orders are recalled. In this section, we consider the particular case of quadratic fields:

Definition 2.1. A **quadratic field** is an algebraic number field of degree 2.

Let K be a quadratic field. Since all number fields are simple extensions of $\mathbb{Q}$, suppose that $K = \mathbb{Q}(\theta)$. Since θ satisfies a rational irreducible polynomial of degree 2, we can write $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ a squarefree integer and an obvious $\mathbb{Q}$-basis is $(1, \sqrt{d})$.

Therefore, we will let for the rest of this chapter $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with $d \in \mathbb{Z}$ a squarefree integer.

1.1. Ring of integers, discriminant, norms and traces

The two $\mathbb{Q}$-homomorphisms $\sigma_1, \sigma_2 : K \to K$ are given by, for $a, b \in \mathbb{Z}$,

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d} \text{ and } \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

For $x \in K$, we will denote $\sigma_2(x)$ by x', the *conjugate* of x.

We now give the ring of integers and discriminant of a quadratic field, along with the the norm, trace and characteristic polynomial of any element. The following results are very standard and their proof is omitted. The latter can be for example found in [Neu99] or [Sam71].

To begin with, the ring of integers of a quadratic field has the following simple expression.

Proposition 2.2. *The ring of integers of K is given by*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proposition 2.3. *The discriminant of K is given by*

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

Definition 2.4. An integer which is the discriminant of a quadratic field is called a **fundamental discriminant**.

In other words, by Proposition 2.3, an integer $d \in \mathbb{Z}$ is a fundamental discriminant if and only if $d \equiv 1 \pmod 4$ and d is squarefree, or if $d = 4k$ with $k \in \mathbb{Z}$ squarefree such that $k \equiv 2,3 \pmod 4$. Of course, there exists a unique quadratic number field for every fundamental discriminant. Note that fundamental discriminants are always congruent to 0 or 1 modulo 4, exactly like those of binary quadratic forms.

Finally, we give an integral basis for K along with explicit expressions for the norm, trace and discriminant of an element.

Proposition 2.5. *An integral basis of K is given by* $(1, \frac{d_K+\sqrt{d_K}}{2})$.

Proposition 2.6. *For $x = a + b\sqrt{d} \in K$ with $a, b \in \mathbb{Q}$, we have that*

$$\begin{aligned} N(x) &= a^2 - db^2, \\ \mathrm{Tr}(x) &= 2a, \\ \Delta(x) &= X^2 - 2aX + (a^2 - db^2) \in \mathbb{Q}[X]. \end{aligned}$$

1.2. Orders in quadratic fields

If we want to get a relationship between ideals of quadratic fields and binary quadratic forms, working only in the maximal order (i.e. the ring of integers) would not be sufficient. Actually, we would only get forms with fundamental discriminants, or equivalently, we would miss certain forms whose discriminant is not squarefree. These facts will clearly appear at the end of the chapter.

Hence we begin by studying orders in quadratic fields. First of all, they have very simple expressions:

Proposition 2.7. *Let $\mathcal{O}$ be an order in K. Then $F = [\mathcal{O}_K : \mathcal{O}]$ is finite and*

$$\mathcal{O} = \mathbb{Z} + F\mathcal{O}_K.$$

Moreover, any set $\mathcal{O} = \mathbb{Z} + F\mathcal{O}_K$ with $F \geq 1$ is an order in K such that $[\mathcal{O}_K : \mathcal{O}] = F$.

Before proving Proposition 2.7, we prove the following Lemma:

Lemma 2.8. *Let $A \subset B \subset C$ three free abelian groups of rank r. If $[C : A] = [C : B]$, then $A = B$.*

Proof. Let $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ and $c = (c_1, \ldots, c_n)$ be $\mathbb{Z}$-bases for A, B, C. Let M_1, M_2 be $n \times n$ matrices such that $a = M_1 b$ and $b = M_2 c$. Since $[C : A] = |\det M_1 M_2|$ and $[C : B] = |\det M_2|$, we get that M_1 is unimodular, so a is a basis for B, whence $A = B$. □

Proof of Proposition 2.7. By Propositions A.6 and A.29, $\mathcal{O}_K$ and $\mathcal{O}$ are free $\mathbb{Z}$-modules of rank 2, so the index $c = [\mathcal{O}_K : \mathcal{O}]$ is finite. Since $c\mathcal{O}_K \subset \mathcal{O}$, we have that $\mathbb{Z} + c\mathcal{O}_K \subset \mathcal{O}$. By the Lemma, it suffices to show that that $c = [\mathcal{O}_K : (\mathbb{Z} + c\mathcal{O}_K)]$. Using the integral bases given after Proposition 2.2, we get that $\mathcal{O}_K = [1, x]$ and $\mathbb{Z} + c\mathcal{O}_K = [1, cx]$ for some $x \in \mathcal{O}_K$, so the result is obvious.

If $c \geq 1$, then $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$ is an order, because it is a subring of K, finitely generated as a $\mathbb{Z}$-module, and since $\mathcal{O}_K$ contains a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K, this ring contains the $\mathbb{Q}$-basis $c\alpha_1, \ldots, c\alpha_n$. By the last paragraph, $[\mathcal{O}_K : \mathcal{O}] = c$. □

The index $[\mathcal{O}_K : \mathcal{O}]$ is called the **conductor** of the order $\mathcal{O}$. By the above proposition, for each integer $F \geq 1$, there exists a unique order of conductor F in K.

Proposition 2.9. *The discriminant of an order $\mathcal{O}$ of conductor F is $F^2 d_K$.*

Proof. In the proof of Proposition 2.7, we saw that there exists a basis $(1, x)$ of $\mathcal{O}_K$ such that $(1, Fx)$ is a basis of $\mathcal{O}$, for some $x \in \mathcal{O}_K$. Consequently, by Proposition A.13, the discriminant of $\mathcal{O}$ is $D(1, Fx) = F^2 D(1, x) = F^2 d_K$. □

Hence, we see that discriminants of orders in K are exactly fundamental discriminants (i.e. discriminants of the maximal order) multiplied by a square, this is, exactly discriminants of binary quadratic forms.

In other words, if $d \equiv 0, 1 \pmod 4$, we can write d in a unique way as $d = F^2 d_K$ with d_K the (fundamental) discriminant of a quadratic field K and $F \geq 1$ the conductor of an order in K. This gives a preview of what we will finally obtain in the correspondence.

Ideals and invertibility In a quadratic field, there is a simple condition for an ideal in an order to be invertible:

Definition 2.10. Let $\mathcal{O}$ be an order in K. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is **proper** if $\mathcal{O} = \{x \in K : x\mathfrak{a} \subset \mathfrak{a}\}$.

Example 2.11. All ideals in the maximal order of a number field are proper. Actually, this is part of the standard proof that all such ideals are invertible (e.g. see [Neu99, Prop. 3.5] or [Sam71, Theorem 2, p.50]). We will shortly see that this can be generalized to a condition about invertibility of ideals in arbitrary orders of quadratic fields.

Example 2.12. Let $K = \mathbb{Q}(\sqrt{-3})$, whose ring of integers is $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{-3}/2)]$, and consider its order $\mathcal{O}$ of conductor 2, this is

$$\mathcal{O} = \mathbb{Z} + 2\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\sqrt{-3}].$$

Then the $\mathcal{O}$-ideal $\mathfrak{a} = (2, 1 + \sqrt{-3})_{\mathcal{O}}$ is not proper. Indeed, we see that $\mathfrak{a}$ is actually an $\mathcal{O}_K$-ideal, because

$$\frac{1+\sqrt{-3}}{2}\left(2\mathcal{O} + (1+\sqrt{-3})\mathcal{O}\right) \subset (1+\sqrt{-3})\mathcal{O} + \frac{-2+2\sqrt{-3}}{2}\mathcal{O} \subset \mathfrak{a}.$$

By the previous example, we get that $\{x \in K : x\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K \neq \mathcal{O}$.

The following technical lemma will be useful to prove the next theorem.

Notation 2.13. For $x, y \in K$ a field, we denote by $[x, y]$ the set $\mathbb{Z}x + \mathbb{Z}y$.

Lemma 2.14. *Let $\mathcal{O}$ be an order in K and let $\tau \in K$ be of degree 2 with minimal polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$.*

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

Proof. Note that $\mathcal{O}_2$ is an order, because $a\tau \in \mathcal{O}_K$ (its minimal polynomial being $x^2 + abx + ca \in \mathbb{Z}[x]$) and $1, \tau$ are linearly independent, so they form a $\mathbb{Q}$-basis of K. Additionally, $\mathfrak{a}$ is a fractional ideal of $\tilde{\mathcal{O}}$, since $(a\tau)\tau = -b\tau - c \in \mathfrak{a}$.

Let us show that $\mathfrak{a}$ is a proper fractional ideal of $\tilde{\mathcal{O}}$, i.e. $\{x \in K : x\mathfrak{a}_f \subset \mathfrak{a}_f\} \subset \tilde{\mathcal{O}}$. Let $x \in K$ be such that $x\mathfrak{a} \subset \mathfrak{a}$. In particular, there exist $m_1, m_2, n_1, n_2 \in \mathbb{Z}$ such that

$$\begin{aligned} x &= m_1 + n_1\tau \\ x\tau &= m_2 + n_2\tau. \end{aligned}$$

Since $a\tau^2 + b\tau + c = 0$, we find that

$$x\tau = \tau(m_1 + n_1\tau) = \frac{-cn_1}{a} + \tau\left(m_1 - \frac{bn_1}{a}\right).$$

Because 1 and τ are linearly independent, this implies that $a|cn_1$ and $a|bn_1$. But a, b, c are relatively prime, so $a|n_1$, whence $x \in \mathbb{Z} + a\mathbb{Z}\tau = \tilde{\mathcal{O}}$.

If $\mathfrak{a}$ is proper, then $\mathcal{O} = \{x \in K : x\mathfrak{a} \subset \mathfrak{a}\} = \tilde{\mathcal{O}}$. □

Finally, we give the main result of this section, generalizing the fact that invertible ideals in the maximal orders (i.e. all of them) are proper.

Proposition 2.15. *Let $\mathcal{O}$ be an order in K and $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then $\mathfrak{a}$ is invertible in $\mathcal{O}$ if and only if it is proper. Moreover, in this case, its inverse is given by*

$$\mathfrak{a}'/N(\mathfrak{a}),$$

where $\mathfrak{a}'$ is the conjugate ideal *of $\mathfrak{a}$, given by $\mathfrak{a}' = \{x' : x \in \mathfrak{a}\}$.*

Proof. Note that $\mathfrak{a}'$ is an ideal because conjugation is a $\mathbb{Q}$-isomorphism which preserves $\mathcal{O}$.

Suppose that $\mathfrak{a}$ is a proper ideal. Let us write $\mathfrak{a} = [\alpha, \beta]$ with $\alpha, \beta \in \mathfrak{a}$, so $\mathfrak{a} = \alpha[1, \tau]$ with $\tau = \beta/\alpha$. Let $ax^2 + bx + c \in \mathbb{Z}[x]$ be the minimal polynomial of τ as above (so $(a, b, c) = 1$). By the second assertion of Lemma 2.14, we get that $\mathcal{O} = [1, a\tau]$. Moreover,

$$\mathfrak{a}\mathfrak{a}' = N(\alpha)[1, \tau][1, \tau'] = N(\alpha)[1, \tau, \tau', \tau\tau'].$$

Since $a(\tau + \tau') = -b$ and $a\tau\tau' = c$, we also consequently have that

$$a\mathfrak{a}\mathfrak{a}' = N(\alpha)[a, a\tau, a\tau', a\tau\tau'] = N(\alpha)[a, a\tau, -b, c].$$

Using that fact that a, b, c are relatively prime, we finally get that $a\mathfrak{a}\mathfrak{a}' = N(\alpha)[1, a\tau] = N(\alpha)\mathcal{O}$. But $N(a\mathfrak{a}) = N(\alpha[a, a\tau]) = N(\alpha)|[1, a\tau]/[a, a\tau]| = aN(\alpha)$, so $N(\mathfrak{a}) = N(\alpha)/a$, which concludes the proof. □

1.3. Picard groups and class numbers, a first glance of the correspondence with forms

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

Recall that we defined the *Picard group* of $\mathcal{O}$ as

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

d_K	$h(d_K)$	d_K	$h(d_K)$	d_K	$h(d_K)$	d_K	$h(d_K)$
-3	①	-55	4	-116	6	-168	4
-4	①	-56	4	-119	10	-179	5
-7	①	-59	3	-120	4	-183	8
-8	①	-67	①	-123	2	-184	4
-11	①	-68	4	-127	5	-187	2
-15	2	-71	7	-131	5	-191	13
-19	①	-79	5	-132	4	-195	4
-20	2	-83	3	-136	4	-199	9
-23	3	-84	4	-139	3	-203	4
-24	2	-87	6	-143	10	-211	3
-31	3	-88	2	-148	2	-212	6
-35	2	-91	2	-151	7	-215	14
-39	4	-95	8	-152	6	-219	4
-40	2	-103	5	-155	4	-223	7
-43	①	-104	6	-159	10	-227	5
-47	5	-107	3	-163	①	-228	4
-51	2	-111	8	-164	8	-231	12
-52	2	-115	2	-167	11	-232	2

Table 2.1: Values of $h(d_K)$ for fundamental discriminants $-232 \leq D \leq 1$.

where $J(\mathcal{O})$ is the set of invertible fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ the set of principal fractional $\mathcal{O}$-ideals. We also have the narrow *Picard group* of $\mathcal{O}$, defined by

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

where $P^+(\mathcal{O}) \subset P(\mathcal{O})$ the set of principal fractional $\mathcal{O}$-ideals with a generator of positive norm.

If $\mathcal{O}$ is the maximal order $\mathcal{O}_K$, we called $Pic(\mathcal{O})$ the ideal class group $\mathcal{C}l(d)$ and its cardinality is the **class number** $h(d)$. In Table 2.1, we give the class numbers of the first fundamental discriminants (we will see later how to compute them easily). Comparing with Tables 1.1 and 1.2, we see a first reflection of a correspondence between classes of forms and (narrow) Picard group of quadratic fields, which can motivate what will follow.

In the following sections, we will employ ourselves to make this correspondence explicit.

2. Associating binary quadratic forms to ideals

As before, we let K be a quadratic number field. The first step is to associate a (primitive) binary quadratic form to each (invertible) ideal of an order of

K.

Recall that every ideal of an order in a quadratic field is a free abelian group of rank 2 (see Appendix A), so the following makes sense.

Proposition 2.16. *Let $\mathcal{O}$ be the order in K of conductor $F \geq 1$ and let $\mathfrak{a}$ be an invertible ideal of $\mathcal{O}$ with the choice of an ordered $\mathbb{Z}$-basis (α, β). Then*

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

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

Before being able to prove Proposition 2.16 entirely, we need the following Lemma, adapted from [Shi94, Prop. 4.11].

Lemma 2.17. *Let $\mathcal{O}$ and $\mathfrak{a}$ as above. Then there exists $x \in K^*$ such that $x\mathfrak{a} + F\mathcal{O} = \mathcal{O}$.*

Proof. Let $\tau \in \mathcal{O}_K$ such that $\mathcal{O}_K = [1, \tau]$. We consider the $\mathbb{Q}$-linear map $f : K \to \mathbb{Q}$ defined as $f(a + b\tau) = a$. Let $\mathfrak{b}$ be such that $\mathfrak{ab} = \mathcal{O}$, since $\mathfrak{a}$ is invertible by hypothesis, so that $f(\mathfrak{ab}) = f(\mathcal{O}) = \mathbb{Z}$. For all $p \in \mathbb{Z}$ prime, the set $f(\mathfrak{ab})$ is therefore not contained in $p\mathbb{Z}$, so there exists $x_p \in \mathfrak{b}$ such that $f(\mathfrak{a}x_p) \not\subset p\mathbb{Z}$.

Let us write $F = p_1^{n_1} \dots p_r^{n_r}$ with $p_1, \dots, p_r$ the prime numbers dividing F. By the Chinese Theorem,

$$\mathfrak{b}/F\mathfrak{b} \cong \mathfrak{b}/p_1^{n_1}\mathfrak{b} \times \cdots \times \mathfrak{b}/p_r^{n_r}\mathfrak{b}$$

as abelian groups, so we can find $x \in \mathfrak{b}$ such that $x = x_i + p_i b_i$ with some $b_i \in \mathfrak{b}$, for $i = 1, \dots, r$. Now, $f(\mathfrak{a}x)$ is not contained in $p_i\mathbb{Z}$ for all $i = 1, \dots, r$, since for all $i = 1, \dots, r$ $f(\mathfrak{a}x) = f(\mathfrak{a}x_{p_i}) + p_i f(b_i\mathfrak{a})$. As a subgroup of $\mathbb{Z}$, $f(\mathfrak{a}x) = m\mathbb{Z}$ for some $m \in \mathbb{Z}$, coprime with F by the preceding discussion. Hence,

$$f(\mathfrak{a}x + F\mathcal{O}_K) = m\mathbb{Z} + F\mathbb{Z} = \mathbb{Z}.$$

Let $\alpha \in \mathcal{O}$. Because $f(\mathfrak{a}x + F\mathcal{O}_K) = \mathbb{Z}$, there exists $\beta \in \mathfrak{a}x + F\mathcal{O}_K$ such that $f(\alpha) = f(\beta)$, so $\alpha - \beta \in F\mathbb{Z}\tau \subset F\mathcal{O}_K$. But

$$\alpha = \beta + (\beta - \alpha) \in F\mathcal{O}_K + x\alpha,$$

so $\mathcal{O} = x\mathfrak{a} + F\mathcal{O}_K$. To replace $\mathcal{O}_K$ by $\mathcal{O}$ in the righthand side, we remark that

$$\mathcal{O} = (x\mathfrak{a} + F\mathcal{O}_K)(x\mathfrak{a} + F\mathcal{O}_K) \subset x\mathfrak{a} + F\mathcal{O},$$

thus $\mathcal{O} = x\mathfrak{a} + F\mathcal{O}$. □

Proof of Proposition 2.16. Explicitly, we have that

$$\begin{aligned} N(\alpha X+\beta Y) &= \alpha\alpha' X^2 + (\alpha\beta'+\alpha'\beta)XY + \beta\beta' Y^2 && (2.1)\\ &= N(\alpha)X^2 + \mathrm{Tr}(\alpha\beta')XY + N(\beta)Y^2. && (2.2)\end{aligned}$$

By Proposition 2.15, because all three coefficients lie in $\mathfrak{a}\mathfrak{a}'$, there exist $a, b, c \in \mathcal{O}$ such that $N(\alpha) = aN(\mathfrak{a})$, $\mathrm{Tr}(\alpha\beta') = bN(\mathfrak{a})$ and $N(\beta) = cN(\mathfrak{a})$. Since norms and traces of algebraic integers are integers, we get that $a, b, c \in \mathcal{O} \cap \mathbb{Q} \subset \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, whence the form is integral. Its discriminant is given by

$$\frac{\mathrm{Tr}(\alpha\beta')^2 - 4N(\alpha\beta)}{N(\mathfrak{a})^2} = \frac{(\alpha\beta'+\alpha'\beta)^2 - 4\alpha\alpha'\beta\beta'}{N(\mathfrak{a})^2} = \frac{(\alpha\beta'-\alpha'\beta)^2}{N(\mathfrak{a})^2} = F^2 d_K$$

by Proposition A.32. The coefficient of x^2 of $f_{\mathfrak{a},(\alpha,\beta)}$ is $N(\alpha)/N(\mathfrak{a})$, so the form is positive definite if $d_K < 0$, since in this case all norms are positive.

The harder part is to prove that $f_{\mathfrak{a},(\alpha,\beta)}$ is primitive. Note that it suffices to prove that there exists an element $a \in \mathfrak{a}$ such that

$$N(a)/N(\mathfrak{a})$$

is coprime to F. Indeed, if a prime p divides the three coefficients of $f_{\mathfrak{a},(\alpha,\beta)}$, then $p^2 | F^2 d_K$, its discriminant. Since d_k is squarefree, we get that $p|F$. But $N(a)/N(\mathfrak{a})$ is the value of $f_{\mathfrak{a},(\alpha,\beta)}$ at some point in $\mathbb{Z}^2$, so $p|N(a)/N(\mathfrak{a})$. This would contradict the fact that $N(a)/N(\mathfrak{a})$ are coprime.

Note that again, it is sufficient to show that there exists an ideal $\mathfrak{b}$ in $\mathcal{O}$ equivalent to $\mathfrak{a}$ such that there exists $b \in \mathfrak{b}$ with $N(b)/N(\mathfrak{b})$ coprime to F.

By Lemma 2.17, there exists an ideal $\mathfrak{b}$ in $\mathcal{O}$ equivalent to $\mathfrak{a}$ such that $\mathfrak{b} + F\mathcal{O} = \mathcal{O}$. This means that the multiplication by F in $\mathcal{O}/\mathfrak{b}$ is surjective, so it is an isomorphism since $\mathcal{O}/\mathfrak{a}$ is finite. Since $\mathcal{O}/\mathfrak{b}$ is a finite abelian group, this implies that $|\mathcal{O}/\mathfrak{b}| = N(\mathfrak{b})$ is coprime to F by the structure Theorem. Thus we can choose $b = N(\mathfrak{b})$.

□

2.1. Correctly ordered bases

Note that the definition above seems to depend on the choice and order of a $\mathbb{Z}$-basis for the ideal. We will now determine "good" choices of ordered bases such that two "good" choices yield to equivalent forms.

By Proposition A.32, we have that

$$\alpha\beta' - \alpha'\beta = \pm N(\mathfrak{a})F\sqrt{d_K},$$

where $\sqrt{d_K}$ denotes by convention the square root of d_K with positive imaginary value if $d_k < 0$, the usual square root otherwise. Note that therefore $(\alpha\beta' - \alpha'\beta)/\sqrt{d_K} \in \mathbb{R}^* \cup i\mathbb{R}^*$, which let us do the following definition.

Definition 2.18. Let $\mathcal{O}$ be an order of K and $\mathfrak{a}$ be an ideal in $\mathcal{O}$. A **correctly ordered basis** (α, β) of $\mathfrak{a}$ is an ordered $\mathbb{Z}$-basis of $\mathfrak{a}$ such that

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

Of course, any ideal of $\mathcal{O}$ admits a correctly ordered basis, since permuting the elements of a basis which is not correctly ordered gives a correctly ordered basis.

Example 2.19. Consider the prime ideal $\mathfrak{p} = \langle 2, 1+\sqrt{-17}\rangle$ in $K = \mathbb{Q}(\sqrt{-17})$. Since $-17 \equiv 3 \pmod 4$, the discriminant of K is $d_K = 4 \cdot -17 = -68$ and its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$. Since

$$\frac{2(1-\sqrt{-17}-(1+\sqrt{-17}))}{2i\sqrt{17}} = -2/i = 2i,$$

the $\mathbb{Z}$-basis $(2, 1+\sqrt{-17})$ of $\mathfrak{p}$[1] is correctly ordered.

Example 2.20. The ideal $\mathcal{O}_K$ itself has the correctly ordered basis $(\frac{d_K+\sqrt{d_K}}{2}, 1)$. Indeed,

$$\frac{1}{\sqrt{d_K}}\left(\frac{d_K+\sqrt{d_K}}{2} - \frac{d_K-\sqrt{d_K}}{2}\right) = 1 > 0.$$

By the description of orders in quadratic field, the order of conductor $F \geq 1$ has the the correctly ordered basis $(\frac{d_K+\sqrt{d_K}}{2}, F)$.

The following proposition gives a first idea about why two correctly ordered basis of an ideal will produce equivalent forms.

Proposition 2.21. *Let $\mathcal{O}$ be an order of K and $\mathfrak{a}$ an ideal of $\mathcal{O}$. Any two correctly ordered bases of $\mathfrak{a}$ are equivalent under the action of an element of* $\mathrm{SL}_2(\mathbb{Z})$. *Conversely, the natural action of an element of* $\mathrm{SL}_2(\mathbb{Z})$ *on a correctly ordered basis of $\mathfrak{a}$ viewed as an element of $\mathfrak{a} \times \mathfrak{a}$ gives another correctly ordered basis.*

Proof. Let (α, β) and (δ, γ) be two correctly ordered bases of $\mathfrak{a}$. Let $C \in \mathrm{GL}_2(\mathbb{Z})$ (thus $\det C = \pm 1$) be the change of basis matrix so that $(\alpha, \beta) = (\delta, \gamma)C$. We get that

$$\alpha\beta' - \alpha'\beta = (\delta\gamma' - \gamma\delta')\det C,$$

$$\text{so } \det C = \frac{(\alpha\beta' - \alpha'\beta)/\sqrt{d_K}}{(\delta\gamma' - \gamma\delta')/\sqrt{d_K}} > 0,$$

[1] Note that it is indeed a $\mathbb{Z}$-basis of $\mathfrak{p}$ since $\mathfrak{p}$ has norm 2, $(2, 1+\sqrt{-17}) \subset \mathfrak{p}$ and $|\mathcal{O}_K/(2, 1+\sqrt{-17})| = \det\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

which implies that $C \in \mathrm{SL}_2(\mathbb{Z})$.

Conversely, let (δ, γ) a correctly ordered $\mathbb{Z}$-basis of $\mathfrak{a}$ and $(\alpha, \beta) = (\delta, \gamma)C$ with $C \in \mathrm{SL}_2(\mathbb{Z})$ (thus $\det C = 1$). By the above, we have that

$$\frac{\alpha\beta' - \alpha'\beta}{\sqrt{d_K}} = \det C \cdot \frac{\delta\gamma' - \gamma\delta'}{\sqrt{d_K}} > 0$$

□

2.2. Independence of bases and equivalence classes

We can now show that, up to equivalence of forms, the choice of a correctly ordered basis does not matter when associating a form to an ideal, as in Proposition 2.31.

Proposition 2.22. *Let $\mathcal{O}$ be an order in K and $\mathfrak{a}$ an ideal of $\mathcal{O}$ with two correctly ordered bases (α, β) and (δ, γ). Then $f_{\mathfrak{a},(\alpha,\beta)}$ and $f_{\mathfrak{a},(\delta,\gamma)}$ are properly equivalent.*

Proof. By Proposition 2.21, we can suppose that $(\alpha, \beta) = (\delta, \gamma)\sigma$ with $\sigma \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$N(\alpha X + \beta Y) = N((X, Y)(\alpha, \beta)^T) = N((X, Y)\sigma^T(\delta, \gamma)^T),$$

which means exactly that $f_{\mathfrak{a},(\alpha,\beta)} = \sigma^T f_{\mathfrak{a},(\delta,\gamma)}$. □

For an ideal $\mathfrak{a}$ of an order $\mathcal{O}$ in K, we will therefore denote by $\overline{f_{\mathfrak{a}}}$ the equivalence class of the binary quadratic form $f_{\mathfrak{a},(\alpha,\beta)}$, where (α, β) is any correctly ordered basis for $\mathfrak{a}$.

Finally, we prove that two equivalent ideals give equivalent forms *under the restriction that this equivalence is in a* narrow *Picard group.* We will discuss this restriction further at the end of the chapter.

Proposition 2.23. *If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in an order $\mathcal{O}$ of K that are equivalent in Pic$^+(\mathcal{O})$, then $\overline{f_{\mathfrak{a}}} = \overline{f_{\mathfrak{b}}}$.*

Proof. Suppose that $\mathfrak{b} = \mathfrak{a}(x)$ with $x \in K$ of positive norm and let (α, β) be a correctly ordered basis for $\mathfrak{a}$. Then $(x\alpha, x\beta)$ is a basis for $\mathfrak{b}$. Since

$$\frac{x\alpha x'\beta' - x\beta x'\alpha'}{\sqrt{d_K}} = N(x)\frac{\alpha\beta' - \beta\alpha'}{\sqrt{d_K}},$$

and $N(x) > 0$, this is a correctly-ordered basis. Therefore, because $N(\mathfrak{a}(x)) = N(\mathfrak{a})|N(x)|$,

$$\overline{f_{\mathfrak{b}}(X, Y)} = \overline{\frac{N(x\alpha X + x\beta Y)}{N(\mathfrak{b})}} = \overline{\frac{N(x)}{|N(x)|} f_{\mathfrak{a}}(X, Y)} = \overline{f_{\mathfrak{a}}(X, Y)}.$$

□

To sum up this section, we proved that, up to equivalence, the form obtained from an ideal does not depend on the choice of an ordered basis nor on ideal equivalence.

Note that since any class of the Picard group of an order $\mathcal{O}$ in K contains an ideal of $\mathcal{O}$, we can also define a mapping from $Pic(\mathcal{O})$ to equivalence classes of binary quadratic forms.

2.3. Injectivity up to equivalences

If we consider equivalence of forms *and* ideals, then the mapping from Proposition 2.16 is injective:

Proposition 2.24. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of an order $\mathcal{O}$ in K. If $\overline{f_{\mathfrak{a}}} = \overline{f_{\mathfrak{b}}}$, then $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.*

Proof. Let $B_1 = (\alpha_1, \beta_1)$ and $B_2 = (\alpha_2, \beta_2))$ be correctly ordered bases for the ideals $\mathfrak{a}$, respectively $\mathfrak{b}$. Since $f_{\mathfrak{a},B_1}$ and $f_{\mathfrak{b},B_2}$ are properly equivalent forms, there exists $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $f_{\mathfrak{a},B_1} = \sigma f_{\mathfrak{b},B_2}$, namely

$$f_{\mathfrak{a},B_1}(x,y) = \frac{N(\alpha_1 x + \beta_1 y)}{N(\mathfrak{a})} = \frac{N(\alpha_2(ax+cy) + \beta_2(bx+dy))}{N(\mathfrak{b})}. \tag{2.3}$$

The zeroes of $f_{\mathfrak{a},B_1}(\,\cdot\,,1)$ are $-\beta_1/\alpha_1$ and $-\beta_1'/\alpha_1'$. By the above equation, they are equal (up to the order) to the ones of the rightmost hand side of (2.3), which are

$$-\frac{c\alpha_2 + d\beta_2}{a\alpha_2 + b\beta_2} \text{ and } -\frac{c\alpha_2' + d\beta_2'}{a\alpha_2' + b\beta_2'}.$$

Therefore, there exists $\lambda \in K$ such that

$$\begin{cases} a\alpha_2 + b\beta_2 = \lambda\alpha_1 \\ c\alpha_2 + d\beta_2 = \lambda\beta_1 \end{cases} \quad \text{or} \quad \begin{cases} a\alpha_2 + b\beta_2 = \lambda\alpha_1' \\ c\alpha_2 + d\beta_2 = \lambda\beta_1'. \end{cases} \tag{2.4}$$

Plugging λ into equation (2.3) gives $\lambda\lambda' = N(\mathfrak{a})/N(\mathfrak{b}) > 0$. Remark that in the second case of (2.4), we would have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha_2 & \alpha_2' \\ \beta_2 & \beta_2' \end{pmatrix} = \begin{pmatrix} \lambda\alpha_1' & \lambda'\alpha_1 \\ \lambda\beta_1' & \lambda'\beta_1 \end{pmatrix}.$$

Taking determinants would give $\frac{\alpha_2\beta_2' - \alpha_2'\beta_2}{\alpha_1\beta_1' - \alpha_1'\beta_1} = -\lambda\lambda' < 0$, contradictory to the hypothesis that (α_1, β_1) and (α_2, β_2) are correctly ordered. Consequently, the first case of (2.4) holds. Since $(\lambda\alpha_1, \lambda\beta_1)$ arises from a $\mathrm{SL}_2(\mathbb{Z})$-transformation of the basis (α_2, β_2) of $\mathfrak{b}$, it is also a basis of $\mathfrak{b}$. Therefore $\mathfrak{a} = (\lambda)\mathfrak{b}$, whence $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent ideals as wanted. □

3. Associating ideals to binary quadratic forms

Let $\mathcal{O}$ be the order of conductor $F \geq 1$ in a quadratic field K of discriminant d_k. We showed in the previous section that there is an injection from $Pic^+(\mathcal{O})$ to $C_p^+(d)$ with $d = F^2 d_K$.

We now prove that this mapping is actually onto and we give its inverse.

Proposition 2.25. *Let $f = [a, b, c]$ be an primitive binary quadratic form of discriminant $d = F^2 d_K$, with d_K a fundamental discriminant, and let K be the quadratic field of discriminant d_K. Suppose that f is positive definite if $d < 0$. Then*

$$\mathfrak{a}_f = \left[\lambda a, \lambda \frac{b - F\sqrt{d_K}}{2}\right] \text{ with } \lambda = \begin{cases} 1 & \text{if } a > 0 \\ F\sqrt{d_K} & \text{otherwise} \end{cases}$$

is a fractional ideal of the order of conductor F in K, such that $\overline{f_{\mathfrak{a}_f}} = \overline{f}$. Moreover, the ideal $\mathfrak{a}_f$ is invertible if f is primitive.

Proof. By Proposition 2.7, the order of conductor F in $K = \mathbb{Q}(\sqrt{d})$ is $\mathcal{O} = \mathbb{Z} + F\mathcal{O}_K$. In the first place, we check that $\beta := (b - F\sqrt{d_K})/2 \in \mathcal{O}$. Note that by assumption $b^2 - 4ac = F^2 d_K$, so $F^2 d \equiv b^2 \pmod 2$, thus $Fd \equiv b \pmod 2$. We can therefore write

$$\beta = \frac{b + Fd_K}{2} - F\left(\frac{d_K + \sqrt{d_K}}{2}\right) \in \mathbb{Z} + F\mathcal{O}_K = \mathcal{O},$$

so we even have $\mathcal{O} = [1, \beta]$ by Proposition 2.5. Note that we also have $\lambda \in \mathcal{O}$.

Since $a \in \mathbb{Z}$ and $\beta \notin \mathbb{Z}$, it is obvious that these are $\mathbb{Z}$-linearly independent elements of $\mathcal{O}$. The set $[\lambda a, \lambda\beta]$ is a fractional ideal of $\mathcal{O}$, because

$$[\lambda a, \lambda\beta]\mathcal{O} = [\lambda a, \lambda\beta][1, \beta] \subset [\lambda a, a\lambda\beta, \lambda\beta, \lambda\beta^2]$$

and, since $b^2 - 4ac = F^2 d_K$,

$$\beta^2 = \frac{F^2 d_K - b^2}{4} + b\beta = -ac + b\beta \in [a, \beta].$$

The discriminant of the $\mathbb{Z}$-basis (a, β) is given by

$$\Delta(\alpha, \beta) = \det \begin{pmatrix} a & (b - F\sqrt{d_K})/2 \\ a & (b + F\sqrt{d_K})/2 \end{pmatrix}^2 = a^2 F^2 d_K.$$

Now, $(\lambda a, \lambda\beta)$ is by definition a basis for $\mathfrak{a}_f$ with discriminant $\Delta(\lambda a, \lambda\beta) = N(\lambda)^2 \Delta(a, \beta)$. The norm of $\mathfrak{a}_f$ is, by Proposition A.32,

$$N(\mathfrak{a}_f) = \left|\frac{\Delta(\lambda a, \lambda\beta)}{F^2 d_K}\right|^{\frac{1}{2}} = |aN(\lambda)|.$$

The basis $(\lambda a, \lambda\beta)$ is correctly ordered if $adN(\lambda)/\sqrt{d_K} = N(\lambda)a\sqrt{d_K}$ belongs to $\mathbb{R}_{>0} \cup i\mathbb{R}_{>0}$. Since $N(\lambda) = 1$ if $a > 0$ and $N(\lambda) = -F^2 d_K$ if $a < 0$, the basis is always correctly ordered, because we suppose that f is positive definite (so $a > 0$) when $d_k^K < 0$.

Note that $N(a) = a^2$, $\mathrm{Tr}(\alpha\beta') = ab$ and $N(\beta) = (b^2 - d_k)/4 = ac$. The class $\overline{f_{\mathfrak{a}_f}}$ is then given, from Equation (2.2), by the class of

$$\begin{aligned} f_{\mathfrak{a}_f,(\lambda a,\lambda\beta)}(X,Y) &= 1/N(\mathfrak{a}_f)\left(N(\lambda a)X^2 + \mathrm{Tr}(\lambda\lambda' a\beta')XY + N(\lambda\beta)Y^2\right) \\ &= N(\lambda)/N(\mathfrak{a}_f)\left(X^2 + \mathrm{Tr}(\alpha\beta')XY + N(\beta)Y^2\right) \\ &= N(\lambda)/(|aN(\lambda)|)\left(a^2X^2 + abXY + acY^2\right) \\ &= \mathrm{sgn}(N(\lambda))\mathrm{sgn}(a)f(X,Y) = f(X,Y). \end{aligned}$$

Finally, we show that $\mathfrak{a}_f$ is invertible if f is primitive. Using Proposition 2.15, it suffices to show that $\mathfrak{a}$ is a proper ideal of $\mathcal{O}$.

Remark that $\tau = \beta/a$ is a root of $f(\,\cdot\,, -1)$ and $[1, a\tau] = [1, \beta] = \mathcal{O}$. By Lemma 2.14, $[1, \tau]$ is a proper fractional ideal of $\mathcal{O}$, thus $\mathfrak{a} = a[1, \tau]$ is a proper ideal of $\mathcal{O}$. □

Remark 2.26. Note that in the above proof, any element of $\mathcal{O}$ with negative norm would have been suitable for the value of λ when $a < 0$.

The following Corollary finally shows that we get a mapping from $C_p^+(d)$ to $\mathrm{Pic}^2(\mathcal{O})$, with d and $\mathcal{O}$ as above.

Corollary 2.27. *If f and g are two equivalent primitive forms, then $\overline{\mathfrak{a}_f} = \overline{\mathfrak{a}_g}$.*

Proof. By Proposition 2.25, we have that $\overline{f_{\mathfrak{a}_f}} = \overline{f}$ and $\overline{f_{\mathfrak{a}_g}} = \overline{g}$, whence $\overline{\mathfrak{a}_f} = \overline{\mathfrak{a}_g}$ by Proposition 2.24. □

4. The correspondence

Let $d \in \mathbb{Z}$ be a fundamental discriminant. Let us denote by $C^+(d)$ the set of classes of (positive definite if $d < 0$) primitive binary quadratic forms.

We sum up the results obtained above in the following theorem.

Theorem 2.28. *Let $d \in \mathbb{Z}$ be an integer such that $d \equiv 0, 1 \pmod 4$ and write $d = F^2 d_K$ with d_k a fundamental discriminant. Let K be the quadratic field of discriminant d_K and $\mathcal{O}$ its order of conductor F. Then there is a bijection between*

$$\mathit{Pic}^+(\mathcal{O}) \text{ and } C_p^+(d).$$

Explicitly, we define $\phi : \mathit{Pic}^+(\mathcal{O}) \to C_p^+(d)$ and $\psi : C_p^+(d) \to \mathit{Pic}^+(\mathcal{O})$ by:

- *If $\overline{\mathfrak{a}}$ is an ideal class of Pic$^+(\mathcal{O})$, let $[\alpha, \beta]$ a correctly ordered basis of any ideal of $\mathcal{O}$ contained in $\overline{\mathfrak{a}}$ and let*

$$\phi(\overline{\mathfrak{a}}) = \overline{\frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}} \in C_p^+(d).$$

- *If $\overline{f} = \overline{[a, b, c]}$ is a class of $C_p^+(d)$, let*

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

Proof. The two maps are well-defined by Propositions 2.16 and 2.22 (ideals to forms) and Propositions 2.25, 2.27, 2.23 (forms to ideals). The second claim of Proposition 2.25 gives that $\phi \circ \psi = \mathrm{id}_{C(d)}$, so ϕ is surjective. By Proposition 2.24, ϕ is injective, whence we have a bijective correspondence and $\phi^{-1} = \psi$. □

Note that in both cases, real and imaginary, we have to make a restriction on one of the sets, Pic$(\mathcal{O})$ or $C_p(d)$. Recall that of course, if $\mathcal{O}$ is an order in an *imaginary* quadratic field, then Pic$^+(\mathcal{O}) =$ Pic$(\mathcal{O})$, since all norms are positive. Conversely, we have that $C^+(d) = C(d)$ if $d > 0$ by definition.

In the following sections, we treat some particular cases and work a little on these restrictions.

4.1. Narrow Picard groups

In the imaginary case, norms are all always negative, so Picard group and narrow Picard groups of orders are equal.

In the real case, we only have a correspondence with a narrow Picard group. In this case, how do they relate to Picard groups?

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

$$\begin{aligned} \mathrm{Pic}(\mathcal{O}) &= J(\mathcal{O})/P(\mathcal{O}) \cong \left(J(\mathcal{O})/P^+(\mathcal{O})\right) / \left(P(\mathcal{O})/P^+(\mathcal{O})\right) \\ &= \mathrm{Pic}^+(\mathcal{O}) / \left(P(\mathcal{O})/P^+(\mathcal{O})\right), \end{aligned}$$

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

We note that $|P(\mathcal{O})/P^+(\mathcal{O})| \leq 2$. Indeed, choose two elements $x_+, x_- \in K^+$ with positive and negative norm, respectively. This is possible since we are in a *real* quadratic field (for example, take $x_+ = 1$, $x_- = \sqrt{d}$) Then every element of $P(\mathcal{O})$ with positive (resp. negative) is equivalent to x_+ (resp. x_-) in $P(\mathcal{O})/P^+(\mathcal{O})$. Moreover, x_+ and x_- are equivalent if and only if $\mathcal{O}^*$ has an element of negative norm, this is, an element of norm -1. So

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

On the other hand, we can also lift the restriction on the Picard group (i.e. consider the Picard group instead of the narrow one) and put it on the class group of form, which is useful when we are interested in the Picard group.

To do that, let $d > 0$ be a positive discriminant and let us consider the group action of $\mathbb{Z}/2$ on $C(d)$ defined as follows

$$\begin{aligned} 0 \cdot \overline{[a,b,c]} &= \overline{[a,b,c]}, \\ 1 \cdot \overline{[a,b,c]} &= \overline{[-a,b,-c]} \end{aligned}$$

for all forms $[a,b,c]$ of discriminant d. This is well-defined since if $\sigma f = g$ for two forms f, g with $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \delta & \gamma \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $\left(\begin{smallmatrix} -\alpha & \beta \\ \delta & -\gamma \end{smallmatrix}\right)(1 \cdot f) = 1 \cdot g$. Of course, this action restricts to an action on $C_p(d)$ and we can consider the quotient set $C(d)/(\mathbb{Z}/2)$. In other words, we identify the class of a form $[a,b,c]$ with the class of the form $[-a,b,-c]$.

Note that this implies that we identify the class of a form $f(x,y)$ with the class of the form $-f(y,x)$. Indeed, if $f = [a,b,c]$, then f is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $[c,-b,a]$, which is $\mathbb{Z}/2$-equivalent to $[-c,-b,-a] = -[c,b,a]$ (see Chapter 1, reduction of forms). We then have the following result

Corollary 2.29. *Let $d > 0$ be an integer such that $d \equiv 0, 1 \pmod 4$ and write $d = F^2 d_K$ with d_k a fundamental discriminant. Let K be the real quadratic field of discriminant d_K and $\mathcal{O}$ its order of conductor F. Then there is a bijection between*

$$\textit{Pic}(\mathcal{O}) \textit{ and } C_p(d)/(\mathbb{Z}/2).$$

Proof. The restriction to the narrow Picard group had to be introduced in Proposition 2.23. Indeed, suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two equivalent ideals in $\mathrm{Pic}(\mathcal{O})$, this is $\mathfrak{b} = \mathfrak{a}(x)$ with $x \in K^*$. Let (α, β) be a correctly ordered basis for $\mathfrak{a}$ and it follows that $(x\alpha, x\beta)$ is a basis for $\mathfrak{b}$. Since

$$\frac{x\alpha x'\beta' - x\beta x'\alpha'}{\sqrt{d_K}} = N(x)\frac{\alpha\beta' - \beta\alpha'}{\sqrt{d_K}},$$

the couple $(x\alpha, x\beta)$ is a correctly ordered basis for $\mathfrak{b}$ when $N(x) > 0$ and we saw that in this case $\overline{f_{\mathfrak{b}}} = \overline{f_{\mathfrak{a}}}$. Now, if $N(x) < 0$, then $(x\beta, x\alpha)$ is a correctly ordered basis for $\mathfrak{b}$ and

$$\overline{f_{\mathfrak{b}}(X,Y)} = \overline{\frac{N(x\beta X + x\alpha Y)}{N(\mathfrak{b})}} = \overline{\frac{N(x)}{|N(x)|} f_{\mathfrak{a}}(Y,X)} = \overline{-f_{\mathfrak{a}}(Y,X)}.$$

Since we identify $\overline{f_{\mathfrak{a}}(Y,X)}$ with $\overline{-f_{\mathfrak{a}}(X,Y)}$ in $C_p(d)/(\mathbb{Z}/2)$, we obtain that $\overline{f_{\mathfrak{a}}} = \overline{f_{\mathfrak{b}}}$ in $C_p(d)/(\mathbb{Z}/2)$. In a similar manner than before, we consider the maps $\phi : \mathrm{Pic}(\mathcal{O}) \to C_p(d)/(\mathbb{Z}/2)$ and $\psi : C_p(d)/(\mathbb{Z}/2) \to \mathrm{Pic}(\mathcal{O})$ defined by:

- If $\overline{\mathfrak{a}}$ is an ideal class of $\mathrm{Pic}(\mathcal{O})$, let $[\alpha, \beta]$ a correctly ordered basis of any ideal of $\mathcal{O}$ contained in $\overline{\mathfrak{a}}$ and let

$$\phi(\overline{\mathfrak{a}}) = \overline{\frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}} \in C_p(d)/(\mathbb{Z}/2).$$

- If $\overline{f} = \overline{[a,b,c]}$ is a class of $C_p(d)/(\mathbb{Z}/2)$, let

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

By Propositions 2.16, 2.22 (ideals to forms), 2.25, 2.27 and the above (forms to ideals), these maps are well-defined, noting that the definition ψ also doesn't depend on the $\mathbb{Z}/2$-class of the element of $C_p(d)$. The second claim of Proposition 2.25 gives that $\phi \circ \psi = \mathrm{id}_{C(d)}$, so ϕ is surjective. By Proposition 2.24, ϕ is injective, whence we have a bijective correspondence and $\phi^{-1} = \psi$. □

4.2. Negative-definite forms

In the definite case, we only considered *positive*-definite forms. However, this is not a restriction, because, if we let $C^-(d)$ be the equivalence classes of negative-definite forms of discriminant $d < 0$, the following result holds:

Proposition 2.30. *Let $d < 0$ be a negative discriminant. Then $C^+(d)$ is in a one-to-one correspondence with $C^-(d)$ through the following map*

$$\begin{array}{ccc} C^+(d) & \to & C^-(d) \\ \overline{f} & \mapsto & \overline{-f} \end{array}$$

Proof. Since $-I \in \mathrm{SL}_2(\mathbb{Z})$, it is clear that this map is well-defined. Indeed, it certainly sends positive-definite forms to negative-definite forms and if f is a f be positive-definite form of discriminant d equivalent, then $\sigma(-f) = -\sigma(f)$ for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$. Moreover, the map is clearly bijective. □

4.3. Primitivity

Finally, we remark that in the case of fundamental discriminants, the primitivity hypothesis drops.

Proposition 2.31. *Let d_K be a fundamental discriminant. Then any binary quadratic form of discriminant d_K is primitive.*

Proof. Let $f = [a, b, c]$ be a binary quadratic form with discriminant $d_K = \Delta(f) = b^2 - 4ac$. Let $K = \mathbb{Q}(\sqrt{d})$ be the quadratic field of discriminant d_K. Suppose that a positive integer k divides a, b, c. Then k^2 divides d_K. If $d \equiv 1 \pmod 4$, then $d_K = d$ and since d is squarefree, we have $k = 1$. If $d \equiv 2, 3 \pmod 4$, then $d_k = 4d$ and $k = 2$. In this case, let $a_1, b_1, c_1 \in \mathbb{Z}$ such that $a = 2a_1, b = 2b_1$ and $c = 2c_1$. Substituting and dividing by 4, we get that $d \equiv b_2^2 \pmod 4$. Since the quadratic residues modulo 4 are 0 and 1 and because d is squarefree, we get $d \equiv 1 \pmod 4$, a contradiction. □

In other words, $C_p^+(d) = C^+(d)$ if d is a fundamental discriminant.

Corollary 2.32. *If K is a quadratic field of discriminant d, then the narrow class group $\mathcal{C}l^+(d)$ is in a bijective correspondence with $C^+(d)$.*

CHAPTER 3

USING THE TWO POINTS OF VIEW

If d is the discriminant of a quadratic form, we proved in the previous chapter the existence of a one-to-one correspondence between $C_p^+(d)$ and the narrow Picard group of a certain order in a quadratic field and conversely, the narrow Picard group of any order in a quadratic field is in a one-to-one correspondence with $C_p^+(d)$ for some discriminant d.

This correspondence is very interesting, since it allows one to transpose questions and structures from one side to the other, simplifying some problems or providing new ideas.

In this chapter, we will study the most important consequences of the correspondence, focusing on class numbers, class groups and number of representations, preparing at the same time the proof of Dirichlet class number formula, which will be done in the next chapter.

1. Gauss composition law and the group structure

The main theorem of elementary algebraic number theory is that $Cl(K)$ is a *finite* abelian *group* for any number field K. More generally, if $\mathcal{O}$ is an order of K, we also defined $\mathrm{Pic}(\mathcal{O})$ to be an abelian group, which is also finite (see Appendix A).

By the correspondence of Theorem 2.28, for any $d \equiv 0, 1 \pmod 4$, the set $C_p^+(d)$ is in a one-to-one correspondence with a narrow Picard group of a quadratic field, so *it can be endowed with the structure of an abelian group*! Looking only at forms, this is not clear at all that we can give them a natural group structure!

More precisely, let $d \equiv 0, 1 \pmod 4$ be an integer and write $d = F^2 d_K$ with d_K a fundamental discriminant, $F \geq 1$. As always, let K be a quadratic field of discriminant d_K and $\mathcal{O} = \mathbb{Z} + F\mathcal{O}_K$ its order of conductor F.

The group law $\star$ induced on $C_p^+(d)$ is explicitly given by

$$\overline{g} \star \overline{h} = \phi\left(\psi(\overline{g})\psi(\overline{h})\right) \ \ (\overline{g}, \overline{h} \in C_p^+(d))$$

with $\psi : C_p^+(d) \to \mathrm{Pic}^+(\mathcal{O})$ the bijection of Theorem 2.28 and $\phi : \mathrm{Pic}^+(\mathcal{O}) \to C_p^+(d)$ its inverse. The identity element is given by $\phi(\mathcal{O})$ and by Proposition 2.15, the inverse of $\overline{g} \in C_p^+(d)$ is $\phi(\psi(\overline{g})'/N(\mathfrak{a}))$.

Therefore, we have by construction

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

as finite abelian groups.

1.1. Historical remarks and perspectives

In the time of Gauss, the explicit concept of groups or finite abelian groups did not exist, nor ideals or ideal class groups. He actually found *intrinsically* the existence of the composition law and its properties turning equivalence classes of forms of equal discriminant into a group.

Actually, this work of Gauss was part of the thought process that led to the definition of ideals and ideal class groups by Dedekind, who generalized ideas of:

- Gauss (group law on equivalence classes, this is, literally, a *class group*);
- Kummer ("ideal numbers" in cyclotomic fields, special algebraic integers in connection with the now-called ideals);
- Kronecker (who generalized Kummer's ideas to arbitrary number fields).

See [Kle07, Ch 2, §2.2] for a detailed account.

This theory of composition can be found in the Disquisitiones Arithmeticae [Gau86, Art. 235-249], but defining the composition of two forms is very complicated, proving that it respects equivalence and yields a group law is even harder. A particular easier case of Gauss composition was given by Legendre and Dirichlet and can be found in [Cox89, Ch. 1, §3.A], but a lot of work is still required to show that this composition is associative.

Two centuries after Gauss, Manjul Bhargava (Princeton University) discovered during his PhD (2001) a very elegant way to look at Gauss composition law, which he was able to generalize to objects such as binary *cubic* forms or *pairs* of binary quadratic forms, along with interpretations in class groups of orders in quadratic fields (see [Bha04a])!

Bhargava's first idea is the following[1]: consider the free abelian group of rank 8 defined by $\mathcal{C}_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. If (v_1, v_2) is the canonical basis for $\mathbb{Z}^2$, any element in $\mathcal{C}_2$ can be written uniquely as

$$\begin{aligned} & av_1 \otimes v_1 \otimes v_1 + bv_1 \otimes v_2 \otimes v_1 + cv_2 \otimes v_1 \otimes v_1 + dv_2 \otimes v_2 \otimes v_1 \\ + \quad & ev_1 \otimes v_1 \otimes v_2 + fv_1 \otimes v_2 \otimes v_2 + gv_2 \otimes v_1 \otimes v_2 + hv_2 \otimes v_2 \otimes v_2 \end{aligned}$$

[1] In the following paragraphs, we give a brief description of the main ideas leading to the second view of Gauss composition, rather than a detailed treatment.

with $a, b, c, e, e, f, g, h \in \mathbb{Z}$, so we can view it as a cube with side 2 centered at the origin, whose vertex (i, j, k) is labelled with the coefficient of $v_i \otimes v_j \otimes v_k$ for $0 \leq i, j, k \leq 1$, $|i| + |j| + |k| = 1$ (see Figure 3.1).

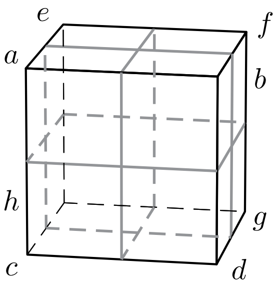


Figure 3.1: A cube of integers and its three slicings.

Such a cube can be sliced in three ways, through the planes orthogonal to the axes, and each slicing yields a pair of faces, the two parallel to the cutting plane. Hence, the three slicings can be viewed as the three pairs of matrices

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$
$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix}, \quad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$$
$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix}, \quad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}.$$

Note that any of these pairs of matrices entirely defines the element, so we have a bijection between $\mathcal{C}_2$ and the set of pairs of 2×2 integer matrices. An action of the group $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ can be defined on $\mathcal{C}_2$ in the following manner:

- For $i = 1, 2, 3$, $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{C}_2$ by acting on (M_i, N_i) by

$$\mathrm{SL}_2(\mathbb{Z}) \ni \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \cdot (M_i, N_i) \mapsto (rM_i + sN_i, tM_i + uN_i),$$

  where we identify $\mathcal{C}_2$ with pairs of 2×2 integer matrices.

- For $(\sigma_1, \sigma_2, \sigma_3) \in \Gamma$ and $z \in \mathcal{C}_2$, we define

$$(\sigma_1, \sigma_2, \sigma_3) \cdot z = \sigma_1 \cdot (\sigma_2 \cdot (\sigma_3 \cdot z)).$$

  Using the fact that row and column operations on square matrices commute, we prove that the order of composition on the right-hand side does not matter. Therefore, it defines a group action of Γ on $\mathcal{C}_2$.

Then, we can associate to any element $z \in \mathcal{C}_2$ three binary quadratic forms

$$Q_i^z(x,y) = -\det(xM_i - N_i y) \ (i = 1,2,3),$$

whose discriminants are equal (which can be checked by a simple computation). We can therefore define the *discriminant* of z as the discriminant of Q_i^z for $i = 1,2,3$. Bhargava's first result is the following:

Theorem 3.1. *Let $d \equiv 0,1 \pmod 4$ be an integer and let $Q_{id,d}$ be any primitive binary quadratic form of discriminant d such there is an element $z \in \mathcal{C}_2$ with $Q_1^z = Q_2^z = Q_3^z = Q_{id,d}$. Then there exists a unique group law on $C_p(d)$ such that*

1. *$\overline{Q}_{id,d}$ is the additive identity;*
2. *For any $w \in \mathcal{C}_2$ with discriminant d such that Q_1^w, Q_2^w, Q_3^w are primitive,*

$$\overline{Q_1^w} + \overline{Q_2^w} + \overline{Q_3^w} = \overline{Q_{id,d}}.$$

Conversely, given binary quadratic forms Q_1, Q_2, Q_3 with $\overline{Q_1} + \overline{Q_2} + \overline{Q_3} = \overline{Q_{id,d}}$, there exists an element $w \in \mathcal{C}_2$ with discriminant d, unique up to Γ-equivalence, such that $Q_i^w = Q_i$.

Notice the striking similarity with the group law on points on elliptic curves: a base point O is chosen, we define a first composition law $*$ on the points of the curve and for all points P_1, P_2 on the curve, we prove that there exists an unique group law $+$ on the points of the curve such that

$$P_1 + P_2 + P_1 * P_2 = O.$$

For an elementary account of this, see [ST10].

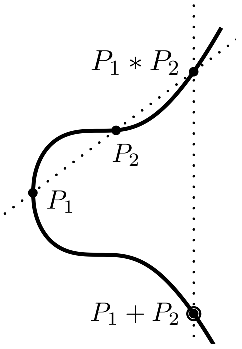


Figure 3.2: A case of the composition law on an elliptic curve.

The natural choice for the identity element in Theorem 3.1 is the principal form (1.1) (as the point $\infty \in \mathrm{P}^1(\mathbb{C})$ is a natural choice for elliptic curves in the Weierstrass normal form). In this case, the group law obtained is precisely Gauss's one!

Proposition 3.2. *Let $d \equiv 0, 1 \pmod 4$ be an integer and let $(C_p(d), +)$ be the abelian group obtained from Theorem 3.1 with the principal form* (1.1) *of discriminant d. Then $(C_p(d), +)$ is the abelian group obtained with Gauss's group law.*

Therefore, the group $(C_p(d), +)$ arising from Gauss's complicated composition law can simply be viewed as the free abelian group generated by elements of $C_p(d)$ modulo the relation where the principal form of discriminant d is identified to 0 and where for all $w \in \mathcal{C}_2$ with discriminant d, the element $\overline{Q_1^w + Q_2^w + Q_3^w}$ is identified with 0.

Bhargava proves these results either using the correspondence with quadratic fields or using Dirichlet's version of Gauss composition (see [Bha04a]).

In his second paper [Bha04b], Bhargava also developed composition laws on other spaces of forms of higher orders (such as *ternary cubic* forms), with interpretations in class groups of orders of *cubic* fields. Finally, the third and fourth paper of this series, [Bha04c] and [Bha08], extend these ideas toward the question of the parametrizations of quartic and quintic rings.

1.2. Explicit formulas

Using some calculations already done, we can easily explicitly determine the identity element and inverses of the group law on $C_p^+(d)$.

By Example 2.20, a correctly ordered basis for the $\mathcal{O}$-ideal $\mathcal{O}$ is

$$\begin{cases} (F\sqrt{d_K}, 1) & \text{if } d_K \equiv 2, 3 \pmod 4 \\ (F\frac{1+\sqrt{d_K}}{2}, 1) & \text{if } d_K \equiv 1 \pmod 4. \end{cases} \tag{3.1}$$

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

$$\begin{cases} \overline{[-d_K, 0, 1]} & \text{if } d_K \equiv 2, 3 \pmod 4 \\ \overline{[(F - d_K)/4, F, 1]} & \text{if } d_K \equiv 1 \pmod 4. \end{cases} \tag{3.2}$$

For inverses, using that the inverse of the class of an ideal $\mathfrak{a}$ is simply given by the class of $\mathfrak{a}'$ (Proposition 2.15), we can use the calculations done in the proof of Proposition 2.25 to get that for all $[a, b, c] \in C_p^+(d)$,

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

(note that a and c get inverted because the basis of $\mathfrak{a}'$ naturally obtained from a correctly ordered basis of $\mathfrak{a}$ is not correctly ordered). Applying the transformation $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we get that

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

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

1.3. Explicit determination of Picard groups

A practical use of the correspondence is that it allows one to compute Picard groups and class numbers of orders in quadratic fields easily and explicitly.

Indeed, such computations in the setting of quadratic field are usually tedious. For example, to determine the class group of a quadratic field, we can use the bound given by Minkowski's theorem on the norm of ideals in a certain system of representatives, then determine all nonequivalent ideals of that norm (see Example 3.4 below). In a non-maximal order, the method is even more complicated.

If we work from the point of view of binary quadratic forms, it is easy to determine a complete system of representatives, as we have seen in Chapter 1 (reduction of forms). It suffices then to transpose the results with the correspondence.

Example 3.3. We computed in Example 1.48 that $|C_p^+(-47)| = 5$, representatives of the classes being given by

$$[1,1,12], [2,1,6], [2,-1,6], [3,1,4], [3,-1,4].$$

Let's give the correspondence between $\mathcal{C}l(-47)$ and $C_p^+(-47)$ (which are therefore both isomorphic to the cyclic group $\mathbb{Z}/5$) explicitly.

Let $K = \mathbb{Q}(\sqrt{-47})$, which is a quadratic field of discriminant -47 (note that $-47 \equiv 1 \pmod 4$). By Example 2.20, a correctly ordered $\mathbb{Z}$-basis of $\mathcal{O}_K$ is given by $(\frac{1+\sqrt{d}}{2}, 1)$. By Equation (3.2), the class of $\mathcal{O}_K$ in $\mathcal{C}l(-47)$ corresponds to

$$\overline{[12,1,1]} = \overline{[1,1,12]}.$$

The ideal class associated to the class $\overline{[2,1,6]}$ is

$$\overline{[2,(1-\sqrt{-47})/2]},$$

whence $\overline{[2,-1,6]}$ is associated to the ideal

$$\overline{[2,(1+\sqrt{-47})/2]}$$

(note that since $1+\sqrt{-47}$ and $1-\sqrt{-47}$ belong to the product of these two ideals, their classes are inverses as predicted). In the same way, it can be shown that $\overline{[3,1,4]}$ is associated to the ideal $\overline{[3,(1-\sqrt{-47})/2]}$, and that $\overline{[3,-1,4]}$ is associated to the ideal $\overline{[3,(1+\sqrt{-47})/2]}$. Note that we've thus determined a complete system of representatives of the ideal class group in a very easy systematical way.

Example 3.4. To compute a complete system of representatives of $\mathcal{C}l(-47)$ (as in the previous example), but staying in the setting of quadratic fields, we could use the fact that any class of $\mathcal{C}l(-47)$ contains an ideal with norm smaller than

$$\frac{4}{\pi} \cdot \frac{2!}{2^2} \cdot \sqrt{47} \leq 4.5$$

(by Minkowski's bound). Therefore, we would have to determine all ideals of norm 2, 3 and 4 in $K = \mathbb{Q}(\sqrt{-47})$. For example, let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ of norm 2, with K. Because $2 \in \mathfrak{a}$, we have that $\mathfrak{a}|(2)$. By Kummer-Dedekind Theorem (Proposition A.23),

$$(2) = \mathfrak{p}_1\mathfrak{p}_2$$

with $\mathfrak{p}_1 = (2) + ((1+\sqrt{-47})/2)$ and $\mathfrak{p}_2 = (2) + ((\sqrt{-47}-1)/2)$ non-equivalent prime ideals. Therefore, there are exactly two ideals of norm 2 in $\mathcal{C}l(-47)$, given by $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We can see that this process is tedious and not systematical with non-prime norms.

Example 3.5. In Example 1.62, we proved that a complete reduced set of representatives of $C_p^+(12)$ is given by

$$[-2, 2, 1], [-1, 2, 2].$$

We have $12 = 2^2 \cdot 3$, so the order of conductor 2 in $\mathbb{Q}(\sqrt{3})$ has narrow Picard group of order 2 and we can easily compute the ideals associated to the forms above, as before. If we consider $C_p^+(12)/\mathbb{Z}/2$, the class of $[-2, 2, 1]$ is identified with the class of $[2, 2, -1]$, which is equal to the class of $[-1, 2, 2]$. Consequently, the Picard group of this order has cardinality 1.

Example 3.6. In Tables 3.1, 3.2 (imaginary case) and 3.3 (real case), we give, by implementing (in *Sage*) the above ideas on a computer, the explicit correspondence between $C_p^+(d)$ and the associated Picard group for all form discriminants $-68 \leq d \leq -3$.

2. Class numbers

In the previous section, we dealt with the first consequences of the correspondence on the structure of $C_p^+(d)$ and narrow Picard groups in quadratic fields.

In this section, we explore the cardinalities of these sets, in particular class numbers, and their relationships.

Recall that we defined:

d	$h_f(d)$	Quadratic field	Conductor of $\mathcal{O}$	Repr. of $C_p^+(d)$	Repr. of $Pic(\mathcal{O})$
-3	1	$\mathbb{Q}(\sqrt{-3})$	1	$[1,1,1]$	$\left[1,-\frac{1}{2}\sqrt{-3}+\frac{1}{2}\right]$
-4	1	$\mathbb{Q}(\sqrt{-1})$	2	$[1,0,1]$	$\left[1,-\sqrt{-1}\right]$
-7	1	$\mathbb{Q}(\sqrt{-7})$	1	$[1,1,2]$	$\left[1,-\frac{1}{2}\sqrt{-7}+\frac{1}{2}\right]$
-8	1	$\mathbb{Q}(\sqrt{-2})$	2	$[1,0,2]$	$\left[1,-\sqrt{-2}\right]$
-11	1	$\mathbb{Q}(\sqrt{-11})$	1	$[1,1,3]$	$\left[1,-\frac{1}{2}\sqrt{-11}+\frac{1}{2}\right]$
-12	1	$\mathbb{Q}(\sqrt{-3})$	2	$[1,0,3]$	$\left[1,-\sqrt{-3}\right]$
-15	2	$\mathbb{Q}(\sqrt{-15})$	1	$[1,1,4]$ $[2,1,2]$	$\left[1,-\frac{1}{2}\sqrt{-15}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-15}+\frac{1}{2}\right]$
-16	1	$\mathbb{Q}(\sqrt{-1})$	4	$[1,0,4]$	$\left[1,-2\sqrt{-1}\right]$
-19	1	$\mathbb{Q}(\sqrt{-19})$	1	$[1,1,5]$	$\left[1,-\frac{1}{2}\sqrt{-19}+\frac{1}{2}\right]$
-20	2	$\mathbb{Q}(\sqrt{-5})$	2	$[1,0,5]$ $[2,2,3]$	$\left[1,-\sqrt{-5}\right]$ $\left[2,-\sqrt{-5}+1\right]$
-23	3	$\mathbb{Q}(\sqrt{-23})$	1	$[1,1,6]$ $[2,1,3]$ $[2,-1,3]$	$\left[1,-\frac{1}{2}\sqrt{-23}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-23}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-23}-\frac{1}{2}\right]$
-24	2	$\mathbb{Q}(\sqrt{-6})$	2	$[1,0,6]$ $[2,0,3]$	$\left[1,-\sqrt{-6}\right]$ $\left[2,-\sqrt{-6}\right]$
-27	1	$\mathbb{Q}(\sqrt{-3})$	3	$[1,1,7]$	$\left[1,-\frac{3}{2}\sqrt{-3}+\frac{1}{2}\right]$
-28	1	$\mathbb{Q}(\sqrt{-7})$	2	$[1,0,7]$	$\left[1,-\sqrt{-7}\right]$
-31	3	$\mathbb{Q}(\sqrt{-31})$	1	$[1,1,8]$ $[2,1,4]$ $[2,-1,4]$	$\left[1,-\frac{1}{2}\sqrt{-31}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-31}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-31}-\frac{1}{2}\right]$
-32	2	$\mathbb{Q}(\sqrt{-2})$	4	$[1,0,8]$ $[3,2,3]$	$\left[1,-2\sqrt{-2}\right]$ $\left[3,-2\sqrt{-2}+1\right]$
-35	2	$\mathbb{Q}(\sqrt{-35})$	1	$[1,1,9]$ $[3,1,3]$	$\left[1,-\frac{1}{2}\sqrt{-35}+\frac{1}{2}\right]$ $\left[3,-\frac{1}{2}\sqrt{-35}+\frac{1}{2}\right]$
-36	2	$\mathbb{Q}(\sqrt{-1})$	6	$[1,0,9]$ $[2,2,5]$	$\left[1,-3\sqrt{-1}\right]$ $\left[2,-3\sqrt{-1}+1\right]$
-39	4	$\mathbb{Q}(\sqrt{-39})$	1	$[1,1,10]$ $[2,1,5]$ $[2,-1,5]$ $[3,3,4]$	$\left[1,-\frac{1}{2}\sqrt{-39}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-39}+\frac{1}{2}\right]$ $\left[2,-\frac{1}{2}\sqrt{-39}-\frac{1}{2}\right]$ $\left[3,-\frac{1}{2}\sqrt{-39}+\frac{3}{2}\right]$
-40	2	$\mathbb{Q}(\sqrt{-10})$	2	$[1,0,10]$ $[2,0,5]$	$\left[1,-\sqrt{-10}\right]$ $\left[2,-\sqrt{-10}\right]$

Table 3.1: Explicit correspondence between $C_p^+(d)$ and Picard groups for $-40 \leq d \leq -3$, $d \equiv 0, 1 \pmod 4$

d	$h_f(d)$	Quadratic field	Conductor of $\mathcal{O}$	Repr. of $C_p^+(d)$	Repr. of $Pic(\mathcal{O})$
-43	1	$\mathbb{Q}(\sqrt{-43})$	1	$[1,1,11]$	$[1, -\frac{1}{2}\sqrt{-43}+\frac{1}{2}]$
-44	3	$\mathbb{Q}(\sqrt{-11})$	2	$[1,0,11]$ $[3,2,4]$ $[3,-2,4]$	$[1, -\sqrt{-11}]$ $[3, -\sqrt{-11}+1]$ $[3, -\sqrt{-11}-1]$
-47	5	$\mathbb{Q}(\sqrt{-47})$	1	$[1,1,12]$ $[2,1,6]$ $[2,-1,6]$ $[3,1,4]$ $[3,-1,4]$	$[1, -\frac{1}{2}\sqrt{-47}+\frac{1}{2}]$ $[2, -\frac{1}{2}\sqrt{-47}+\frac{1}{2}]$ $[2, -\frac{1}{2}\sqrt{-47}-\frac{1}{2}]$ $[3, -\frac{1}{2}\sqrt{-47}+\frac{1}{2}]$ $[3, -\frac{1}{2}\sqrt{-47}-\frac{1}{2}]$
-48	2	$\mathbb{Q}(\sqrt{-3})$	4	$[1,0,12]$ $[3,0,4]$	$[1, -2\sqrt{-3}]$ $[3, -2\sqrt{-3}]$
-51	2	$\mathbb{Q}(\sqrt{-51})$	1	$[1,1,13]$ $[3,3,5]$	$[1, -\frac{1}{2}\sqrt{-51}+\frac{1}{2}]$ $[3, -\frac{1}{2}\sqrt{-51}+\frac{3}{2}]$
-52	2	$\mathbb{Q}(\sqrt{-13})$	2	$[1,0,13]$ $[2,2,7]$	$[1, -\sqrt{-13}]$ $[2, -\sqrt{-13}+1]$
-55	4	$\mathbb{Q}(\sqrt{-55})$	1	$[1,1,14]$ $[2,1,7]$ $[2,-1,7]$ $[4,3,4]$	$[1, -\frac{1}{2}\sqrt{-55}+\frac{1}{2}]$ $[2, -\frac{1}{2}\sqrt{-55}+\frac{1}{2}]$ $[2, -\frac{1}{2}\sqrt{-55}-\frac{1}{2}]$ $[4, -\frac{1}{2}\sqrt{-55}+\frac{3}{2}]$
-56	4	$\mathbb{Q}(\sqrt{-14})$	2	$[1,0,14]$ $[2,0,7]$ $[3,2,5]$ $[3,-2,5]$	$[1, -\sqrt{-14}]$ $[2, -\sqrt{-14}]$ $[3, -\sqrt{-14}+1]$ $[3, -\sqrt{-14}-1]$
-59	3	$\mathbb{Q}(\sqrt{-59})$	1	$[1,1,15]$ $[3,1,5]$ $[3,-1,5]$	$[1, -\frac{1}{2}\sqrt{-59}+\frac{1}{2}]$ $[3, -\frac{1}{2}\sqrt{-59}+\frac{1}{2}]$ $[3, -\frac{1}{2}\sqrt{-59}-\frac{1}{2}]$
-60	2	$\mathbb{Q}(\sqrt{-15})$	2	$[1,0,15]$ $[3,0,5]$	$[1, -\sqrt{-15}]$ $[3, -\sqrt{-15}]$
-63	4	$\mathbb{Q}(\sqrt{-7})$	3	$[1,1,16]$ $[2,1,8]$ $[2,-1,8]$ $[4,1,4]$	$[1, -\frac{3}{2}\sqrt{-7}+\frac{1}{2}]$ $[2, -\frac{3}{2}\sqrt{-7}+\frac{1}{2}]$ $[2, -\frac{3}{2}\sqrt{-7}-\frac{1}{2}]$ $[4, -\frac{3}{2}\sqrt{-7}+\frac{1}{2}]$
-64	2	$\mathbb{Q}(\sqrt{-1})$	8	$[1,0,16]$ $[4,4,5]$	$[1, -4\sqrt{-1}]$ $[4, -4\sqrt{-1}+2]$
-67	1	$\mathbb{Q}(\sqrt{-67})$	1	$[1,1,17]$	$[1, -\frac{1}{2}\sqrt{-67}+\frac{1}{2}]$
-68	4	$\mathbb{Q}(\sqrt{-17})$	2	$[1,0,17]$ $[2,2,9]$ $[3,2,6]$ $[3,-2,6]$	$[1, -\sqrt{-17}]$ $[2, -\sqrt{-17}+1]$ $[3, -\sqrt{-17}+1]$ $[3, -\sqrt{-17}-1]$

Table 3.2: Explicit correspondence between $C_p^+(d)$ and Picard groups for $-68 \le d \le -41$, $d \equiv 0, 1 \pmod 4$

d	$h_f(d)$	Quadratic field	Conductor of $\mathcal{O}$	Repr. of $C_p^+(d)/(\mathbb{Z}/2\mathbb{Z})$	Repr. of $Pic(\mathcal{O})$
5	1	$\mathbb{Q}(\sqrt{5})$	1	$[-1,1,1]$	$\left[-\sqrt{5}, \frac{1}{2}\sqrt{5}-\frac{5}{2}\right]$
8	1	$\mathbb{Q}(\sqrt{2})$	2	$[-1,2,1]$	$\left[-2\sqrt{2}, 2\sqrt{2}-4\right]$
12	1	$\mathbb{Q}(\sqrt{3})$	2	$[-2,2,1]$	$\left[-4\sqrt{3}, 2\sqrt{3}-6\right]$
13	1	$\mathbb{Q}(\sqrt{13})$	1	$[-1,3,1]$	$\left[-\sqrt{13}, \frac{3}{2}\sqrt{13}-\frac{13}{2}\right]$
17	1	$\mathbb{Q}(\sqrt{17})$	1	$[-2,1,2]$	$\left[-2\sqrt{17}, \frac{1}{2}\sqrt{17}-\frac{17}{2}\right]$
20	2	$\mathbb{Q}(\sqrt{5})$	2	$[-2,2,2]$ $[-1,4,1]$	$\left[-4\sqrt{5}, 2\sqrt{5}-10\right]$ $\left[-2\sqrt{5}, 4\sqrt{5}-10\right]$
21	1	$\mathbb{Q}(\sqrt{21})$	1	$[-3,3,1]$	$\left[-3\sqrt{21}, \frac{3}{2}\sqrt{21}-\frac{21}{2}\right]$
24	1	$\mathbb{Q}(\sqrt{6})$	2	$[-2,4,1]$	$\left[-4\sqrt{6}, 4\sqrt{6}-12\right]$
28	1	$\mathbb{Q}(\sqrt{7})$	2	$[-3,2,2]$	$\left[-6\sqrt{7}, 2\sqrt{7}-14\right]$
29	1	$\mathbb{Q}(\sqrt{29})$	1	$[-1,5,1]$	$\left[-\sqrt{29}, \frac{5}{2}\sqrt{29}-\frac{29}{2}\right]$
32	2	$\mathbb{Q}(\sqrt{2})$	4	$[-4,4,1]$ $[-2,4,2]$	$\left[-16\sqrt{2}, 8\sqrt{2}-16\right]$ $\left[-8\sqrt{2}, 8\sqrt{2}-16\right]$
33	1	$\mathbb{Q}(\sqrt{33})$	1	$[-3,3,2]$	$\left[-3\sqrt{33}, \frac{3}{2}\sqrt{33}-\frac{33}{2}\right]$
37	1	$\mathbb{Q}(\sqrt{37})$	1	$[-3,1,3]$	$\left[-3\sqrt{37}, \frac{1}{2}\sqrt{37}-\frac{37}{2}\right]$
40	2	$\mathbb{Q}(\sqrt{10})$	2	$[-3,2,3]$ $[-1,6,1]$	$\left[-6\sqrt{10}, 2\sqrt{10}-20\right]$ $\left[-2\sqrt{10}, 6\sqrt{10}-20\right]$
41	1	$\mathbb{Q}(\sqrt{41})$	1	$[-4,3,2]$	$\left[-4\sqrt{41}, \frac{3}{2}\sqrt{41}-\frac{41}{2}\right]$
44	1	$\mathbb{Q}(\sqrt{11})$	2	$[-2,6,1]$	$\left[-4\sqrt{11}, 6\sqrt{11}-22\right]$
45	2	$\mathbb{Q}(\sqrt{5})$	3	$[-3,3,3]$ $[-5,5,1]$	$\left[-9\sqrt{5}, \frac{9}{2}\sqrt{5}-\frac{45}{2}\right]$ $\left[-15\sqrt{5}, \frac{15}{2}\sqrt{5}-\frac{45}{2}\right]$
48	2	$\mathbb{Q}(\sqrt{3})$	4	$[-4,4,2]$ $[-3,6,1]$	$\left[-16\sqrt{3}, 8\sqrt{3}-24\right]$ $\left[-12\sqrt{3}, 12\sqrt{3}-24\right]$
52	2	$\mathbb{Q}(\sqrt{13})$	2	$[-4,2,3]$ $[-2,6,2]$	$\left[-8\sqrt{13}, 2\sqrt{13}-26\right]$ $\left[-4\sqrt{13}, 6\sqrt{13}-26\right]$
53	1	$\mathbb{Q}(\sqrt{53})$	1	$[-1,7,1]$	$\left[-\sqrt{53}, \frac{7}{2}\sqrt{53}-\frac{53}{2}\right]$
56	1	$\mathbb{Q}(\sqrt{14})$	2	$[-5,4,2]$	$\left[-10\sqrt{14}, 4\sqrt{14}-28\right]$
57	1	$\mathbb{Q}(\sqrt{57})$	1	$[-4,3,3]$	$\left[-4\sqrt{57}, \frac{3}{2}\sqrt{57}-\frac{57}{2}\right]$
60	2	$\mathbb{Q}(\sqrt{15})$	2	$[-6,6,1]$ $[-3,6,2]$	$\left[-12\sqrt{15}, 6\sqrt{15}-30\right]$ $\left[-6\sqrt{15}, 6\sqrt{15}-30\right]$
61	1	$\mathbb{Q}(\sqrt{61})$	1	$[-3,5,3]$	$\left[-3\sqrt{61}, \frac{5}{2}\sqrt{61}-\frac{61}{2}\right]$
65	2	$\mathbb{Q}(\sqrt{65})$	1	$[-4,1,4]$ $[-5,5,2]$	$\left[-4\sqrt{65}, \frac{1}{2}\sqrt{65}-\frac{65}{2}\right]$ $\left[-5\sqrt{65}, \frac{5}{2}\sqrt{65}-\frac{65}{2}\right]$

Table 3.3: Explicit correspondence between $C_p^+(d)/(\mathbb{Z}/2\mathbb{Z})$ and Picard groups for $1 \leq d \leq 65$, $d \equiv 0, 1 \pmod 4$.

- for $d \equiv 0, 1 \pmod 4$, the class number $h_f(d)$ to be the cardinality of $C_p^+(d)$, which we proved to be finite;
- for d a fundamental discriminant, the class number of the quadratic field K of discriminant d, defined as $h(d) = |\mathcal{C}l(K)|$, which is, as the class number of any number field, finite by Minkowski's theorem;
- more generally, we can also consider cardinalities of (narrow) Picard groups of orders in quadratic fields.

By the correspondence (Theorem 2.28), we can immediately relate these notions, as Tables 1.1 and 1.2 suggested:

Proposition 3.7. *Let $d \equiv 0, 1 \pmod 4$ and write $d = F^2 d_K$ with d_K a fundamental discriminant and $F \geq 1$. Let $\mathcal{O}$ be the order of conductor F in the quadratic field K of discriminant d_K. Then*

$$|Pic(\mathcal{O})| = \begin{cases} h_f(d) & \text{if } d < 0 \\ h_f(d) & \text{if } d > 0 \text{ and } \mathcal{O} \text{ has a unit of norm } -1 \\ h_f(d)/2 & \text{otherwise.} \end{cases}$$

Proof. By Theorem 2.28, the narrow Picard group $\mathrm{Pic}^+(\mathcal{O})$ is in a one-to-one correspondence with $C_p^+(d)$. If $d < 0$, $\mathrm{Pic}^+(\mathcal{O}) = \mathrm{Pic}(\mathcal{O})$ and if $d > 0$, then, by Section 2.4.1 of the previous chapter, $|\mathrm{Pic}(\mathcal{O})| = 2|\mathrm{Pic}^+(\mathcal{O})|$ or $|\mathrm{Pic}(\mathcal{O})| = |\mathrm{Pic}^+(\mathcal{O})|$ depending on the existence of a unit with norm -1. □

In the point of view of quadratic fields, the class number measures in a certain way by how much the ring of integers fails to be an UFD (see Proposition A.27). For binary quadratic forms, class numbers can help to determine which integers are represented by some forms (see Section 1.5 of Chapter 1), so this notion is doubly interesting.

The following questions arise naturally (and they transpose for h by Proposition 3.7):

1. Does there exist infinitely many $d \equiv 0, 1 \pmod 4$ such that $h_f(d) = 1$? (*class number one problem*)
2. More generally, does there exist infinitely many $d \equiv 0, 1 \pmod 4$ such that $h_f(f) = n$ for a given integer $n \geq 1$? Can an efficient way to find them be given?
3. What is the asymptotic behavior of $h_f(d)$ with $d \equiv 0, 1 \pmod 4$?

We see in Table 1.1 that $h_f(d)$ seems to grow as $-d$ grows and that $h_f(d) = 1$ for $d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$.

In his *Disquisitiones arithmeticae* [Gau86, Art 303-304], Gauss made several conjectures about these questions:

1. $h(d) \to \infty$ when $d \to -\infty$,
2. There are no other negative discriminants with class number one than the thirteen above,
3. For some small integer, he claims to give complete list of negative discriminants with this class number,
4. There are infinitely many positive discriminants with class number one.

The first conjecture has been proved by Hans Heilbronn (1908-1975) in 1934. The class number problems for small integers have been solved between 1952 and 2004 for integers up to 100. The class number one problem for imaginary quadratic field has been solved by Heegner, Stark and Baker in 1967, who proved that the above list is indeed complete, as Gauss guessed. The fourth question, class number one problem for real quadratic fields, is still open.

2.1. Class number one problem for even negative discriminants

We've already seen in the previous section how computation of class numbers and Picard groups from the point of view of forms is easier. In this section, we will treat more theoretical points.

Indeed, we answer the class number one problem for even negative discriminants, in a theorem proven by Landau in 1903. To do it, we use the point of view of forms.

Theorem 3.8 (Class number one problem for even negative discriminants)**.** *For $d < 0$, we have that $h_f(4d) = 1$ if and only if $d = -1, -2, -3, -4, -7$.*

As a Corollary, we will get, by Proposition 3.7,

Corollary 3.9. *If $d \equiv 2, 3 \pmod 1$ is a squarefree negative integer, then $h(d) = 1$ if and only if $d = -4$ or $d = -8$.*

Proof. If $d \equiv 2, 3 \pmod 1$ is squarefree and negative, then $h_f(4d) = h(4d)$. The result follows since only -1 and -2 are congruent to $2, 3$ modulo 4 among $-1, -2, -3, -4, -7$. □

First, we prove the following lemma:

Lemma 3.10. *Let $\Delta = -4d$ with $d \in \mathbb{N}$. If $1 < n < d$ and if there exists $\beta \in \mathbb{Z}$ such that $\beta^2 \equiv -d \pmod n$ and $(n, (b^2 + d)/n) = 1$, then $h_f(\Delta) > 1$.*

Proof. Suppose that $h_f(\Delta) = 1$. By assumption, let $c \in \mathbb{Z}$ be such that $d = \beta^2 - nc$. Multiplying by 4, this gives $(2\beta)^2 = \Delta + 4nc$. Since $(n, c) = 1$ by hypothesis, the form $[n, 2\beta, c]$ is primitive with discriminant Δ and properly represents n. Note that this argument is a variation of the one given in the proof of Proposition 1.28. Because $h(\Delta) = 1$ the form $[n, 2\beta, c]$ is equivalent to the principal form 1.1 of discriminant Δ, namely $[1, 0, d]$. By Corollary 1.26, n is properly represented by $[1, 0, d]$, i.e. there exists $x, y \in \mathbb{Z}$ coprime such that

$$x^2 + dy^2 = n.$$

But this is clearly impossible being given that $1 < n < d$. □

Proof of Theorem 3.8. We begin by proving the three following points:

- *If $h_f(\Delta) = 1$, either $d = 1$, either d is a prime power.* Indeed, we could otherwise write $d = d_1 d_2$ with $1 < d_1, d_2 < d$ and $(d_1, d_2) = 1$. Using Lemma 3.10 with $n = d_1$ (noting that $-d \equiv 0 \pmod{d_1}$ and $(d_1, d/n) = 1$ by hypothesis) would give $h_f(\Delta) = 1$, a contradiction;

- *If $d = 2^\alpha$ with $\alpha \geq 3$, then $h_f(\Delta) > 1$.* Indeed, we simply apply Lemma 3.10 with $n = 4$, remarking that $-2^\alpha \equiv 2^2 \equiv 0 \pmod 4$ and that $(4, 4 + 2^\alpha) = (4, 2^{\alpha-2} + 1) = 1$.

- *If $d > 7$ is odd, then $h_f(\Delta) > 1$.* We use Lemma 3.10 with $n = 2, 4, 8$, depending on the congruence class of d modulo 16:

  - If $d \equiv 1, 5, 9, 13 \pmod{16}$, we can take $n = 2$ and $\beta = 1$. Indeed, for $k \in \mathbb{Z}$ and $c = 1, 5, 9, 13$, we have

  $$\frac{d + \beta^2}{2} = \frac{16k + c + 1}{2} = 8k + \frac{c + 1}{2} \equiv 1 \pmod 2.$$

  - If $d \equiv 3, 11 \pmod{16}$, we can take $n = 4$ and $\beta = 1$. Indeed, $-3 \equiv -11 \equiv 1^2 \pmod 4$ and for $k \in \mathbb{Z}$ and $c = 3, 11$, we similarly have

  $$\frac{d + \beta^2}{4} = 4k + \frac{c + 1}{4} \equiv 1, 3 \pmod 4.$$

  - If $d \equiv 7, 15 \pmod{16}$, we can take $n = 8$ and $\beta = 1$ (in the first case) or $\beta = 3$ (in the second case). Indeed, $-7 \equiv -15 \equiv 1 \equiv 3^2 \pmod 8$ and for $k \in \mathbb{Z}$ and $c = 7, 15$, we have $\frac{d+\beta^2}{4} \equiv 1 \pmod 2$.

By the above, if $h_f(\Delta) = 1$, then $d = 1$ or $d = 2, 4$ (power of 2) or $d = 3, 7$ (power of an odd prime, $d < 7$). By the calculations of Table 1.1, the converse follows. □

3. Units, automorphisms and Pell's equation

Let $d \equiv 0, 1 \pmod 4$ be an integer and let us consider the set $\mathrm{Form}_p(d)$ of primitive integral binary quadratic forms.

Recall that an automorphism of a form $f \in \mathrm{Form}_p(d)$ is an element of the isotropy group $\mathrm{Aut}(f)$ of f under the action of $\mathrm{SL}_2(\mathbb{Z})$. We will shortly see that automorphisms play an important role in the questions concerning representation of integers by certain forms.

The first questions that arise are: does a given form have infinitely many automorphisms? Otherwise how many? Can they parametrized?

These questions can be easily answered using the correspondence of the previous chapter, as we will now see.

The corresponding concept involved in the context of quadratic fields is **units** of orders (as subrings of maximal orders).

Proposition 3.11. *Let K be a quadratic field, $\mathcal{O}$ an order in K. Then $x \in \mathcal{O}$ is a unit if and only if $N(x) = \pm 1$.*

Proof. If x is a unit, there exists $y \in \mathcal{O}$ such that $xy = 1$. Taking norms gives $N(x)N(y) = 1$. Since $\mathcal{O} \subset \mathcal{O}_K$ and norms of algebraic integers are integers, we get that $N(x) = \pm 1$.

Suppose now that $N(x) = \pm 1$. Since $xx' = N(x) = \pm 1$, we have that $x^{-1} = \pm x'$. But $\mathcal{O} = \mathbb{Z} + F\mathcal{O}_K$ for an integer $F \geq 1$, so $\mathcal{O}$ is stable by conjugation and $x^{-1} = x' \in \mathcal{O}$. □

Remark 3.12. The result is still true in any number field K for the *maximal* order $\mathcal{O}_K$. Indeed, if $N(x) = 1$, Proposition A.9 gives that the characteristic polynomial of x has a constant coefficient equal to ± 1, which is true if and only if the same holds for the minimal polynomial of x, by Proposition A.9. Suppose that the latter is

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X \pm 1 \in \mathbb{Z}[X].$$

Then $1/x$ is a root of the monic integral polynomial

$$\pm X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + 1 \in \mathbb{Z}[X],$$

therefore $1/x \in \mathcal{O}_K$ and x is a unit in K.

Proposition 3.13. *Let d be a form discriminant and $g \in Form_p^+(d)$. Let us write $d = F^2 d_K$ with d_K the discriminant of a quadratic field K and $F \geq 1$. Let $\mathcal{O}$ be the order of K of conductor F. Then there is an isomorphism between $Aut(g)$ and $\mathcal{O}^*$.*

Proof. By the correspondence (Theorem 2.28 and previous results), there exists a proper ideal $\mathfrak{a} = [\alpha, \beta]$ of $\mathcal{O}$ such that g is equivalent to $f_{\mathfrak{a},(\alpha,\beta)}$. Since the groups of automorphisms of two equivalent forms are conjugate, we can suppose without loss of generality that $g = f_{\mathfrak{a},(\alpha,\beta)}$.

If $x \in \mathcal{O}^*$ is a unit, then $(x\alpha, x\beta)$ is another basis for $\mathfrak{a}$. Let $\sigma_x \in \mathrm{SL}_2(\mathbb{Z})$ be the change of basis matrix. By Proposition 2.22, we have that $\sigma_x^T g = g$, so $\sigma_x^T \in \mathrm{Aut}(g)$. The map

$$\begin{array}{rcl} \mathcal{O}^* & \rightarrow & \mathrm{Aut}(f) \\ x & \mapsto & \sigma_x^T \end{array}$$

is of course injective (if $\sigma_x = \sigma_y$ for two units x, y of $\mathcal{O}$, then $x\alpha = y\alpha$, so $x = y$). Moreover, it is clearly a group homomorphism.

Also, if $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Aut}(g)$, then $f_{[\alpha,\beta]} = \sigma f_{[\alpha,\beta]}$. By the proof of Proposition 2.24, we find $\lambda \in K$ such that

$$\begin{cases} \lambda\alpha = a\alpha + b\beta \\ \lambda\beta = c\alpha + d\beta \end{cases}$$

and $[\alpha, \beta] = (\lambda)[\alpha, \beta]$. Taking norms gives $N(\lambda) = \pm 1$. Note that $\lambda \in \{x \in K : x\mathfrak{a} \subset x\}$ by the equations above, so $\lambda \in \mathcal{O}$ since $\mathfrak{a}$ is proper. Consequently, $\lambda \in \mathcal{O}^*$ (Proposition 3.11) and $\sigma = \sigma_\lambda^T$, so we get that the above map is surjective. □

Since all groups of automorphisms are isomorphic to the same group of units, we have the following result:

Corollary 3.14. *Let d be a form discriminant. Then for all $f, g \in Form_p^+(d)$,*

$$Aut(f) \cong Aut(g).$$

3.1. Determination of the groups of units and automorphisms

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant d_K and $\mathcal{O}$ its order of conductor $F \geq 1$. By the previous section, determining the automorphisms of a binary quadratic form of discriminant $F^2 d_K$ amounts to determining the group of units of $\mathcal{O}$. This is a relatively simple problem, which we will now solve.

By Proposition 2.5, a $\mathbb{Z}$-basis of $\mathcal{O}$ is given by $(1, F(d_K + \sqrt{d_K})/2)$. Therefore, by Proposition 3.11, the units of $\mathcal{O}$ are in a one-to-one correspondence with the solutions $(m, n) \in \mathbb{Z}^2$ to the equations

$$N(m + nF(d_K + \sqrt{d_K})/2) = \pm 1.$$

Explicitly, this amounts to the diophantine equations

$$(2m + nFd_k)^2 - d_K(nF)^2 = \pm 4.$$

This can be reparametrized as all integral solutions $(u, n) \in \mathbb{Z}^2$

$$u^2 - dn^2 = \pm 4 \tag{3.3}$$

with $u = 2m + nFd_K$. Indeed, if $u^2 - dn^2 = \pm 4$, then $u^2 \equiv F^2 d_K n^2 \pmod 2$, so $u \equiv Fd_K n \pmod 2$.

The family of diophantine equations $\mathcal{P}_{m,n} : x^2 - ny^2 = m$ with m, n integers and n nonsquare is known as (generalizations of) **Pell's equations** and is very famous historically.

Proposition 3.15 (Units in imaginary quadratic fields)**.** *Let $d < 0$ be a squarefree negative integer and $K = \mathbb{Q}(\sqrt{d})$. Moreover, let $F \geq 1$ and $\mathcal{O}$ the order of K of conductor F. Then the group of units of $\mathcal{O}$ is given by*

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

Proof. For the sake of clarity, let $D = -d > 0$. By Equation (3.3), a general element $x = m + nF(d_K + \sqrt{d_K})/2 \in \mathcal{O}$ is a unit if and only if

$$u^2 + Dn^2 = \pm 4 \tag{3.4}$$

with $m, n \in \mathbb{Z}$, $u = 2m + nFd_k$. Of course, there are no solutions with the right hand side equal to -4. For the other equation, the solutions $(u, n) \in \mathbb{Z}$ to (3.4) are, using that $\sqrt{2}, \sqrt{3} \notin \mathbb{Q}$,

$$\begin{aligned} (u, n) &= (\pm 2, 0) \\ (u, n) &= (\pm 1, \pm 3/\sqrt{D}) \text{ if } \sqrt{3}/\sqrt{D} \in \mathbb{Z} \\ (u, n) &= (0, \pm 2/\sqrt{D}) \text{ if } 2/\sqrt{D} \in \mathbb{Z}. \end{aligned}$$

Therefore, the couples $(m, n) = (\pm 1, 0)$ are always associated (as above) to units. Note that $\sqrt{D} = F\sqrt{-d_K}$, thus, since $d_K \equiv 1, 2, 3 \pmod 4$:

- $\sqrt{3}/\sqrt{D} \in \mathbb{Z}$ if and only if $d = -3$ (i.e. $d_K = -3$ and $F = 1$).
- $2/\sqrt{D} \in \mathbb{Z}$ if and only if $d = -1$ (i.e. $d_K = -4$ and $F = 1$).

Therefore $\mathcal{O}^*$ has cardinality 2 (and thus isomorphic to $\mathbb{Z}/2$) with the units associated to $(m, n) = (\pm 1, 0)$, except when

1. $d = -1$: in this case, $(u, n) = (0, \pm 1)$ are the two other solutions to (3.3), so we have have two more units, associated to $(m, n) = \pm(2, 1)$. Since i has order 4, we have that $\mathcal{O}^* \cong \mathbb{Z}/4$.
2. $d = -3$: in this case, $(u, n) = (\pm 1, \pm 1)$ are the four other solutions to (3.3) and we have have four more units, associated to $(m, n) = \pm(2, 1)$ and $(m, n) = \pm(1, 1)$. A small calculation shows that the unit $\frac{1}{2}(1+\sqrt{-3})$ associated to $(m, n) = (2, 1)$ has order 6, so $\mathcal{O}^* \cong \mathbb{Z}/6$.

□

As a direct consequence of Propositions 1.35, 3.13 and 3.15, we get the following description of automorphism groups of forms of negative discriminants:

Corollary 3.16. *Let f be a primitive binary quadratic form of discriminant $d < 0$. Then*

$$Aut(f) \cong \begin{cases} \mathbb{Z}/4 & \text{if } d = -4 \\ \mathbb{Z}/6 & \text{if } d = -3 \\ \mathbb{Z}/2 & \text{otherwise.} \end{cases}$$

Example 3.17. Let us give explicitly the group of automorphisms of a form f of discriminant $d < 0$ (and the associated units).

We already gave the two general automorphisms of any form

$$\text{id and } \sigma_1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

so if $d \neq -3, -4$, then $\mathrm{Aut}(f) = \{\mathrm{id}, \sigma_1\}$.

For $d = -4$, the associated order is $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ and the proof of Proposition 3.15 gives the four units

$$(m - 2n) + ni$$

with $(m, n) = (\pm 1, 0), \pm(2, 1)$. Recall that $h(-4) = 1$, so it suffices, by Proposition 1.35, to determine the automorphisms of the principal form $[1, 0, 1]$, whose associated ideal is simply $\mathcal{O}_K$. By the proof of Proposition 3.13, the automorphism associated to a unit $x \in \mathcal{O}$ is given by the transpose of the change of basis matrix from $(1, -i)$ to $(x, -xi)$.

Explicitly, after a few simple calculations, we find the following correspondence:

Unit	Automorphism
1	id
-1	σ_1
i	$\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
$-i$	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Similarly, for $d = -3$, $K = \mathbb{Q}(\sqrt{-3})$, the units of $\mathcal{O}_K$ are given by $(m-3n/2)+n\sqrt{-3}/2$ for $(m,n) = (\pm 1, 0), \pm(2,1), \pm(1,1)$ (Proposition 3.15). We also have $h(-4) = 1$ (see Chapter 1), so it again suffices to determine the automorphisms of the principal form $f = [1,1,1]$ associated to the ideal $[1, (1-\sqrt{-3})/2]$. We find the following correspondence:

Unit	Automorphism
1	id
-1	σ_1
$1/2(1+\sqrt{-3})$	$\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$-1/2(1+\sqrt{-3})$	$\left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
$1/2(1-\sqrt{-3})$	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$
$-1/2(1-\sqrt{-3})$	$\left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$.

In particular, we see that $\mathrm{Aut}(f)$ is the cyclic group (of order 6) generated by $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Remark 3.18. It is also possible to deduce these results only in the context of forms. See for example [Gra07, ex. 4.1f, p. 3].

Proposition 3.19 (Units in real quadratic fields)**.** *Let $d > 0$ be a squarefree positive integer and $K = \mathbb{Q}(\sqrt{d})$. Moreover, let $F \geq 1$ and $\mathcal{O}$ be the order of K of conductor F. Then there are infinitely many units in $\mathcal{O}$ and more precisely,*

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

Sketch of the proof. By Equation (3.3), an element $x = m + nF(d_K + \sqrt{d_K})/2 \in \mathcal{O}$ is a unit if and only if

$$u^2 - dn^2 = \pm 4.$$

with $u = 2m + nFd_K$. First of all, we deal with $\mathcal{O}^*_+$, the elements of $\mathcal{O}^*$ with positive norms, this is when the right hand side of the above equation is equal to 4. From the theory of Pell equations, there exists an element $x \in \mathcal{O}^*_+ \subset \mathbb{R}$ such that $x > 1$. Then, it can be shown[2] that there exists an minimal element among elements strictly bigger than 1 in $\mathcal{O}^*_+$, say z. Then for any $y \in \mathcal{O}^*_+$ there exists $n \in \mathbb{Z}$ such that $z^n \leq y < z^{n+1}$, by monotonicity of $n \mapsto z^n$. By minimality of z, this implies that $y = z^n$, so we have an isomorphism of groups

$$\begin{array}{rcl} \mathbb{Z} & \to & \mathcal{O}^*_+ \\ n & \mapsto & z^n. \end{array}$$

Finally, since any element $x \in \mathcal{O}$ can be written as $x = \pm y$ with $y \in \mathcal{O}^*_+$, the result follows. □

[2] See [Fla89, Chapter 4.3] for details.

Remark 3.20. Note that Propositions 3.19 and 3.15 are particular cases of Dirichlet unit theorem, in quadratic fields.

As a direct consequence of Propositions 1.35, 3.13 and 3.19, we get:

Corollary 3.21. *Let $f \in Form_p^+(d)$ with $d > 0$. Then*

$$Aut(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Example 3.22. In the same way that we gave a list of all automorphisms in in the case of negative discriminants (Example 3.17), we can parametrize them for positive discriminants. Let $f = [a, b, c]$ be a form of positive discriminant $d \equiv 0, 1 \pmod 4$ and write $d = F^2 d_K$ with $F \geq 1$, d_K the discriminant of a quadratic field K. The ideal associated to f is

$$\mathfrak{a}_f = \left[\lambda a, \lambda \frac{b - F\sqrt{d_K}}{2}\right] \text{ with } \lambda = \begin{cases} 1 & \text{if } a > 0 \\ F\sqrt{d_K} & \text{otherwise} \end{cases},$$

which admits the correctly $\mathbb{Z}$-basis $(\alpha, \beta) = (\lambda a, \lambda(b - F\sqrt{d_K})/2)$ by Proposition 2.25.

By Equation (3.3), an element $x = m + nF(d_K + \sqrt{d_K})/2$ of $\mathcal{O}$ is a unit if and only if

$$u^2 - dn^2 = \pm 4.$$

with $m, n \in \mathbb{Z}$, $u = 2m + nFd_K$. We compute that for a solution $(m, n) \in \mathbb{Z}^2$ of one of the above equations, the transpose of the change of basis matrix from (α, β) to $(x\alpha, x\beta)$ with x the unit associated to (u, n) is

$$\begin{pmatrix} (u + nb)/2 & -na \\ nc & (u - nb)/2 \end{pmatrix}.$$

Therefore,

$$\mathrm{Aut}(f) = \left\{ \begin{pmatrix} (u + nb)/2 & -na \\ nc & (u - nb)/2 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : u^2 - dn^2 = \pm 4 \right\}.$$

Remark 3.23. As a consequence of the above results, it can be shown that the set of solutions of some Pell equations (namely the above ones) also has the structure of an abelian group! For details, see [Fla89, Chapter 4.3].

Remark 3.24. As with the imaginary case, it is also possible to determine the automorphism group without looking at quadratic fields, but it is less straightforward. An idea is to consider at first things in a bigger group than $\mathrm{SL}_2(\mathbb{Z})$, e.g. $\mathrm{GL}_2(\mathbb{Q}(\sqrt{d}))$, were groups of automorphisms can be diagonalized. There, any form is equivalent to a multiple of $[0, 1, 0]$, whose group of automorphisms is easy to determine. Then, it is possible to express the automorphism group of any form (in $\mathrm{SL}_2(\mathbb{Z})$) from the one of $[0, 1, 0]$ in $\mathrm{GL}_2(\mathbb{Q}(\sqrt{d}))$.

3.2. Actions of automorphism groups

For any binary quadratic form f, we can consider the natural (right) action of $\mathrm{Aut}(f) \subset \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Z}^2$. This action is interesting because of its links with representations of integers by forms. Indeed, note for example that if n is represented by f and $\sigma \in \mathrm{Aut}(f)$, then $f(x,y) = \sigma f(x,y) = f((x,y)\sigma)$, so $(x,y)\sigma$ is another representation of n by f. In other words, $\mathrm{Aut}(f)$ acts on the set of representations of n by f. Note that $\mathrm{Aut}(f)$ preserves proper representations, since the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Z}^2$ preserves the gcd[3]

We will discuss this in details in the following sections. For now, we give the following Lemma about fixed points of this action, which will be useful later.

Lemma 3.25. *For $f \in Form_p^+(d)$ a binary quadratic form of discriminant $d \neq 0$, the only point of $\mathbb{Z}^2$ fixed by an element $\sigma \in Aut(f)$ is 0.*

Proof. Suppose that there exists $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) - \mathrm{id}$ such that $(x,y)\sigma = (x,y)$ for some $(x,y) \in \mathbb{Z}^2 - 0$. This implies that

$$0 = \det \begin{pmatrix} a-1 & b \\ c & d-1 \end{pmatrix} = ad - a - d + 1 - bc = 2 - a - d,$$

i.e. $a + d = 2$. By looking at the explicit descriptions of Examples 3.17 and 3.22, we see that it can happen if and only if $\sigma = \mathrm{id}$. □

4. Integers represented by forms and by norms of ideals

We finally come back to the study of representation of integers by forms, where we will use the correspondence and our knowledge of quadratic fields to get interesting results.

Let $d \equiv 0, 1 \pmod 4$ be an integer and write $d = F^2 d_K$ with d_K the discriminant of a quadratic field K and $F \geq 1$. Moreover, let $\mathcal{O}$ be the order of K with conductor F.

The following two questions arise naturally:

1. Which integers are represented by norms of ideals in $\mathcal{O}$?
2. Which integers are represented by forms of discriminant d?

We already obtained a few results about the second one in Chapter 1, staying in the point of view of forms. The next Proposition shows that the two problems are equivalent and its proof gives an explicit method to pass from one to the other.

[3] If $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $(x,y) \in \mathbb{Z}^2$, then $(x,y)\sigma = (ax + cy, bx + dy)$ and remark that if an integer divides $ax + cy, bx + dy$, then it divides $d(ax + cy) - c(bx + dy) = x$. The same holds for y and the other way is clear.

Proposition 3.26. *An integer $n \in \mathbb{Z}$ is properly represented by a form of $Form_p^+(d)$ if and only if n is the norm of an invertible ideal in $\mathcal{O}$.*

Proof. Let $f \in \mathrm{Form}_p^+(d)$ be a primitive form representing n. By Proposition 1.25, f is equivalent to a form $g = [n, b, c]$ of discriminant d with $b, c \in \mathbb{Z}$. We saw in the proof of Proposition 2.25 that $N(\mathfrak{a}_g) = n$, so n is the norm of the ideal $\mathfrak{a}_g$ of $\mathcal{O}$.

Conversely, let $\mathfrak{a}$ be an ideal in $\mathcal{O}$ with a basis (α, β) and $n = N(\mathfrak{a})$. Since $N(\mathfrak{a}) \in \mathfrak{a}$, we choose $x, y \in \mathbb{Z}$ such that $N(\mathfrak{a}) = x\alpha + y\beta$. By definition,

$$f_{\mathfrak{a},(\alpha,\beta)}(x, y) = \frac{N(N(\mathfrak{a}))}{N(\mathfrak{a})} = N(\mathfrak{a}) = n.$$

□

The correspondence of Proposition 3.26 can be refined with respect to representations as follows:

Definition 3.27. If f is a form of discriminant d and $n \geq 1$, we denote by $R(f, n)$ the set $\{(x, y) \in \mathbb{Z}^2 : f(x, y) = n\}$ of representations of n by f and by $R_p(f, n)$ the set $R(f, n) \cap \{(x, y) \in \mathbb{Z}^2 : x, y \text{ coprime}\}$ of proper representations.

Proposition 3.28. *Let $n \geq 1$ be an integer and $f_1, \ldots, f_r$ be a complete system of representatives of $C_p^+(d)$, with $d \equiv 0, 1 \pmod 4$ a discriminant. Then there is a one-to-one correspondence between*

$$\coprod_{i=1}^{r} R(f_i, n)/Aut(f_i) \text{ and } \{\mathfrak{a} \text{ proper ideal of } \mathcal{O} : N(\mathfrak{a}) = n\}.$$

To prove it, we use the following Lemma:

Lemma 3.29. *If an integer $n \in \mathbb{Z}$ is represented properly by a binary quadratic form f through $(x, y) \in \mathbb{Z}^2$, there exists a unique $\sigma = \left(\begin{smallmatrix} x & y \\ * & * \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma f = [n, b, c]$ with $0 \leq b < 2n$.*

Proof. Let f be a binary quadratic form of discriminant d and $(x, y) \in R_p(n, f)$. So there exists a solution $(\alpha, \beta) \in \mathbb{Z}^2$ to the diophantine equation

$$\alpha x + \beta y = 1.$$

Moreover, all solutions are given by $\{(\alpha + ky, \beta - kx) : k \in \mathbb{Z}\}$, as it is well known from elementary number theory. As we saw in the proof of Lemma 1.25,

$$\sigma_k = \begin{pmatrix} x & y \\ -(\beta - kx) & (\alpha + ky) \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

verifies $\sigma_k f = [n, b_k, c_k]$ for all $k \in \mathbb{Z}$, with $b_k, c_k \in \mathbb{Z}$. Since discriminants are preserved through equivalence, we have that $d = b^2 - 4ac$, so $b^2 \equiv d \pmod{4n}$. A simple calculation then shows that, for $\sigma_k f = [n, b_k, c_k]$, we have $b_k = 2kn + b_0$ for all $k \in \mathbb{Z}$, whence the conclusion. □

Proof of Proposition 3.28. We first define maps

$$h_i : R(f_i, n) \to \{\mathfrak{a} \text{ proper ideal of } \mathcal{O} : N(\mathfrak{a}) = n\} \ (i = 1, \dots, r)$$

by the following: if $(x, y) \in R(f_i, n)$, write $(x, y) = e(x', y')$ with $x', y' \in \mathbb{Z}$ coprime and $e \geq 1$. Of course, $(x', y') \in R_p(f, n/c^2)$. By Lemma 3.29, there exists a unique matrix $\sigma = \left(\begin{smallmatrix} x' & y' \\ * & * \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma f = [n^2/e, b, c]$ with $0 \leq b < 2n$. By Proposition 3.26, $N(\mathfrak{a}_{\sigma f}) = n/e^2$. We set $h_i(x, y) = c\mathfrak{a}_{\sigma f}$, so that $N(h_i(x, y)) = n$.

We show that this map does not depend on the automorphism class of the representation. If $\tau \in \mathrm{Aut}(f_i)$ and $(x, y) \in R(f_i, n)$, then $(w, z) = (x, y)\tau$ is another representation of n by f_i. Let us write $(x, y) = e(x', y')$ with $x', y' \in \mathbb{Z}$ coprime and $e \geq 1$. Since $\mathrm{SL}_2(\mathbb{Z})$ preserves the gcd (see the preceding section), we can also write $(w, z) = e(w', z')$ with $e \geq 1$. Let $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ be the matrix associated to $(x', y') \in R(f_i, n/e^2)$ as above. Note that $f = \tau f$, so we have $\sigma\tau f = [n/e^2, b, c]$ and

$$\sigma\tau = \begin{pmatrix} x' & y' \\ * & * \end{pmatrix},$$

so $h_i((x, y)\tau) = e\mathfrak{a}_{\sigma\tau f} = e\mathfrak{a}_{\sigma f} = h(x, y)$.

Therefore, we can induce maps $\overline{h}_i : R(f_i, n)/\mathrm{Aut}(f_i) \to \{\mathfrak{a} \text{ proper ideal of } \mathcal{O} : N(\mathfrak{a}) = n\}$, and then a map

$$h = \coprod_{i=1}^{r} \overline{h}_i : \coprod_{i=1}^{r} R(f_i, n)/\mathrm{Aut}(f_i) \to \{\mathfrak{a} \text{ proper ideal of } \mathcal{O} : N(\mathfrak{a}) = n\}.$$

We show that h is injective. Indeed, suppose that $(x_1, y_1) \in R(f_i, n)$ and $(x_2, y_2) \in R(f_j, n)$ are such that

$$h([(x_1, y_1)]) = \mathfrak{b} = h([(x_2, y_2)]).$$

For $l = 1, 2$, we write $(x_l, y_l) = e_l(x'_l, y'_l)$ with $e_l \geq 1$ and $x'_l, y'_l \in \mathbb{Z}$ coprime. By definition, there exist $\sigma_1, \sigma_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\sigma_1 f_i = [n/e_1^2, b_1, c_1] \text{ and } \sigma_2 f_i = [n/e_2^2, b_2, c_2]$$

with $0 \leq b_1, b_2 < 2n$, $c_1, c_2 \in \mathbb{Z}$, satisfying

$$\mathfrak{b} = e_1\mathfrak{a}_{\sigma_1 f_i} = e_2\mathfrak{a}_{\sigma_2 f_j}.$$

By Theorem 2.28, $\sigma_1 f_i$ and $\sigma_2 f_j$ are equivalent forms. Since $f_1, \dots, f_r$ forms a complete reduced system of representatives of the class of forms in $C_p^+(d)$, we get that $i = j$ and $\sigma_1^{-1}\sigma_2 \in \mathrm{Aut}(f_i)$. Since $(1,0)\sigma_l = (x_l, y_l)$ for $l = 1, 2$, we finally obtain

$$(x_1, y_1) = (1,0)\sigma_1 = (x_2, y_2)\sigma_1\sigma_2^{-1},$$

whence the injectivity.

We finally prove that h is surjective. Let $\mathfrak{b}$ be a proper ideal in $\mathcal{O}$ of norm $N(\mathfrak{b}) = n$ and choose a correctly ordered $\mathbb{Z}$-basis (α, β) of $\mathfrak{b}$. Since $N(\mathfrak{b}) \in \mathfrak{b}$, there exists $x, y \in \mathbb{Z}$ such that $x\alpha + y\beta = N(\mathfrak{b})$. Again, write $(x, y) = e(x', y')$ with $e \geq 1$ and $x', y' \in \mathbb{Z}$ coprime. Then, the primitive form $f_{\mathfrak{b},(\alpha,\beta)}$ properly represents n/e^2 through $(x', y') \in \mathbb{Z}^2$, since

$$f_{\mathfrak{b},(\alpha,\beta)}(x', y') = \frac{N(x'\alpha + y'\beta)}{N(\mathfrak{b})} = \frac{N(\mathfrak{b})^2/e^2}{N(\mathfrak{b})} = n/e^2.$$

Without loss of generality, suppose that $f_{\mathfrak{b},(\alpha,\beta)}$ is equivalent to f_1 and let $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma f_1 = f_{\mathfrak{b},(n,\alpha)}$. Note that f_1 represents n/e through $(w, z) = (x', y')\sigma^T$. Let $\tau = \left(\begin{smallmatrix} w & z \\ * & * \end{smallmatrix}\right)$ such that $\tau f_1 = [n/e^2, b', c']$ with $0 \leq b' < 2n$. By definition,

$$h_1((x, y)\tau) = e\mathfrak{a}_{\tau f_1} = e\mathfrak{a}_{\tau\sigma^{-1} f_{\mathfrak{b},(\alpha,\beta)}},$$

which is equivalent to $\mathfrak{b}$ by the correspondence theorem. In other words, there exists $\lambda \in K^*$ such that $(x)\mathfrak{b} = h_1((x, y)\tau)$. Since $h_1((x, y)\tau)$ and $\mathfrak{b}$ have norm n, we conclude that $N(x) = 1$.

Finally, since $\mathfrak{b}$ is proper, we have by definition $\{z \in K : x\mathfrak{a} \subset \mathfrak{b}\} = \mathcal{O}$, so $\lambda \in \mathcal{O}^*$ and $\mathfrak{b} = h_1((1, 0)\tau)$, which gives the surjectivity.

□

We will illustrate this proposition extensively at the end of the next section.

5. Number of representations of an integer by forms of given discriminant

In the previous section, we determined a strong relationship between representations of an integers by binary quadratic forms and norms of ideals. We will now use this to determine explicitly the number of representations of an integer by binary quadratic forms of given discriminant.

First of all, we have to be more exact with this notion, because:

1. Equivalent forms represent the same integers, therefore if an integer is represented by a form, it is represented by infinitely many of them.

2. The number of representations of an integer by a given form can be infinite, since the group of automorphisms of forms of positive discriminant is infinite and acts on sets of representations of an integer by a given form.

To avoid these two problems, we will study the sets of representations by primitive *nonequivalent* forms *modulo automorphisms.* Formally, this is, for $d \equiv 0, 1 \pmod 4$ a discriminant:

$$R_d(n) = \coprod_{i=1}^{r} R(f_i, n)/\mathrm{Aut}(f_i),$$

where $f_1, \ldots, f_r$ is a complete system of representatives of $C_p^+(d)$. Recall that equivalent form represent the same integers, so this does not depend on the choice of the representatives and is hence well-defined.

The main theorem of this section is

Theorem 3.30. *Let $d \equiv 0, 1 \pmod 4$ be a discriminant and $n \geq 1$ an integer. Then*

$$r_d(n) := |R_d(n)| = \sum_{m|n} \left(\frac{d}{m}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol.

In other words, the *global* question of determining the number of representations of an integer by all equivalent forms modulo automorphisms has a remarkably nice answer. In the next chapter, we will also work on representations by a *given* form and we will see that the problem is harder.

Remark 3.31. Note that it is sufficient to work for representations of *positive* integers since if $n < 0$ is an integer, then $r_d(-n) = r_d(n)$, since a representations $(x, y) \in \mathbb{Z}^2$ of $-n$ by a form $f = [a, b, c]$ of discriminant d yields to a representation of n by $-f = [-a, -b, -c]$ of discriminants d through (x, y). Since f is equivalent to a form g if and only if $-f$ is equivalent to $-g$, whence the claim.

As an immediate corollary, we will have for the definite case:

Corollary 3.32. *Let $d \equiv 0, 1 \pmod 4$ be a positive discriminant and $n \geq 1$ an integer. Then the number of representations of n by equivalent positive forms of discriminant d is*

$$w \sum_{m|n} \left(\frac{d}{m}\right),$$

where w is the number of automorphisms of a positive form of discriminant d as given by Corollary 3.16.

Proof. Immediately follows from Proposition 3.28 since no non-trivial automorphism of a form fixes a non-zero element of $\mathbb{Z}^2$ (Lemma 3.25). Indeed, in the notations of Proposition 3.28, we have that $|R(f_i, p)/\mathrm{Aut}(f_i)| = |R_p(f_i, p)|/|\mathrm{Aut}(f_i)|$ and by Corollary 3.16, $|\mathrm{Aut}(f_1)| = \cdots = |\mathrm{Aut}(f_r)| := w$. □

In the next section, we will use this explicit expression for $|R_d(n)|$ to obtain the Dirichlet class number formula and other interesting results.

We give two proofs of this theorem: a first, straightforward and elegant, using the point of view of quadratic fields and the second, longer and less insightful, using only the point of view of binary quadratic forms. Thus, we will be able to appreciate the efforts put into obtaining the correspondence between binary forms and ideals of quadratic fields.

5.1. Proof from the point of view of quadratic fields

Let $d \equiv 0, 1 \pmod 4$ be a negative integer and write $d = F^2 d_K$ with d_K a fundamental discriminant and $F \geq 1$. Let $\mathcal{O}$ be the order of conductor F in the quadratic field of discriminant d.

Let us restate the result of Proposition 3.28 in terms of cardinalities:

Corollary 3.33. *For $n \geq 1$ an integer, we have that*

$$r_d(n) = |\{\mathfrak{a} \text{ proper ideal of } \mathcal{O} : N(\mathfrak{a}) = n\}| .$$

If d is a fundamental discriminant, we will be able to determine explicitly the left hand side of the above equation, using the fact that maximal orders are Dedekind domains. Therefore, we suppose from now that d is a fundamental discriminant.

Corollary 3.34. *For $d < 0$ a fundamental discriminant, $r_d(n)$ is a multiplicative function.*

Proof. Let $m, n \in \mathbb{Z}$ be coprime integers. For $k \in \mathbb{N}$, we define $E(k) = \{\mathfrak{a} \text{ ideal of } \mathcal{O}_K : N(\mathfrak{a}) = k\}$ and we give a bijective map

$$f : E(mn) \to E(m) \times E(n).$$

If $\mathfrak{a} \in E(mn)$, then $mn = N(\mathfrak{a}) \in \mathfrak{a}$, so $\mathfrak{a}$ divides $(mn) = (m)(n)$. By unique factorization, we can write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ in a unique way with $\mathfrak{b}, \mathfrak{c}$ ideals of $\mathcal{O}_K$ such that $\mathfrak{b}|(m)$ but $\mathfrak{b} \not|(n)$ and $\mathfrak{c}|(n)$ but $\mathfrak{c} \not|(m)$. Since $N(\mathfrak{b})|\mathfrak{b}$ and $N(\mathfrak{c})|\mathfrak{c}$, we must have $N(\mathfrak{b}) = m$ and $N(\mathfrak{c}) = n$. Therefore, we can define $f(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{c})$. Then f is clearly injective. Moreover, if $\mathfrak{b} \in E(n)$ and $\mathfrak{c} \in E(m)$, then $\mathfrak{b}\mathfrak{c} \in E(mn)$ and $f(\mathfrak{b}\mathfrak{c}) = (\mathfrak{b}, \mathfrak{c})$, so we have a bijection and the result follows. □

Therefore, it suffices to determine r_d at powers of prime numbers, which we do now.

Corollary 3.35. *For $d < 0$ a fundamental discriminant, p a prime number and $k \geq 1$, we have that*

$$r_d(p^k) = \sum_{i=0}^{k} \left(\frac{d}{p^i}\right).$$

Proof. By Corollary 3.34, we need to determine

$$\left|\{\mathfrak{a} \text{ ideal of } \mathcal{O}_K : N(\mathfrak{a}) = p^k\}\right|.$$

If $\mathfrak{a}$ is an ideal of norm p^k, then $p^k \in \mathfrak{a}$, so $\mathfrak{a}$ divides (p^k). By Kummer-Dedekind Theorem (Proposition A.23), we have that

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 \ (\mathfrak{p}_1 \text{ prime, } \mathfrak{p}_1 \neq \mathfrak{p}_2) & \text{if } (d/p) = 1 \\ \mathfrak{p}^2 \ (\mathfrak{p} \text{ prime}) & \text{if } (d/p) = 0 \\ (p) \ ((p) \text{ prime}) & \text{if } (d/p) = -1. \end{cases}$$

Indeed, we have $\mathcal{O}_K = \mathbb{Z}[(d + \sqrt{d})/2]$ (Proposition 2.5) and the minimal polynomial of $(d + \sqrt{d})/2$ is

$$f = X^2 - dX + \frac{d(d-1)}{4} \in \mathbb{Z}[X]$$

with discriminant d. Consequently, viewed in $\mathbb{Z}_p[X]$, f is irreducible if and only if $(d/p) = -1$, factors into two distinct irreducibles if and only if $(d/p) = 1$ and factors into the square of an irreducible if and only if $p|d$.

Note that in the first case, $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$ and in the second case $N(\mathfrak{p}) = p$ too. Consequently, we see that

- if $(d/p) = 1$, there are $k+1$ ideals of norm p, given by $\mathfrak{p}_1^k, \mathfrak{p}_1^{k-1}\mathfrak{p}_2, \ldots, \mathfrak{p}_2^k$, where $(p) = \mathfrak{p}_1\mathfrak{p}_2$.
- if $(d/p) = 0$, there is one ideal of norm p, given by $\mathfrak{p}^k$, where $(p) = \mathfrak{p}^{2k}$.
- if $(d/p) = -1$, there is one ideal of norm p if k is even, given by $\mathfrak{p}^{k/2}$ where (p) is prime, and zero ideals of norm p if k is odd.

In the three cases, we have that $r_d(p^k) = \sum_{i=0}^{k} \left(d/p^i\right)$ and the result follows by Corollary 3.34. □

We are now able to prove Theorem 3.30 easily.

Proof of Theorem 3.30. We write $n = p_1^{v_1} \dots p_r^{v_r}$, where $p_1, \dots, p_r$ are the distinct primes dividing n. By the multiplicativity of r_d, Corollary 3.35 and the properties of the Kronecker symbol, we have that

$$r_d(n) = \prod_{i=1}^{r} r_d(p_i^{v_i}) = \prod_{i=1}^{r} \sum_{j=0}^{k} \left(\frac{d}{p^i}\right) = \sum_{m|n} \left(\frac{d}{m}\right).$$

□

Remark 3.36. The restriction to fundamental discriminants could perhaps be lifted, but it would not be straightforward, since orders are usually not Dedekind domains. By lack of time and space, this has not been researched further. Anyway, the same result will be proved below in the general case and we only need fundamental discriminants to get to Dirichlet class number formula.

5.2. Proof from the point of view of forms

To compare with the preceding approach (i.e. using the correspondence with quadratic fields) and appreciate its elegance, we do another proof of Theorem 3.30 staying in the point of view of forms.

The first idea is to refine Proposition 1.28 and Lemma 1.25 to get a result similar to Proposition 3.28.

Proposition 3.37. *Let $n \geq 1$ be an integer and $d \equiv 0, 1 \pmod 4$ be a discriminant. Then if $f_1, \dots, f_r$ is a complete reduced system of representatives of $C_p^+(d)$, then*

$$\coprod_{i=1}^{r} R_p(f_i, n)/Aut(f_i) \text{ and } \{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}$$

are in a one-to-one correspondence.

Proof. The proof is quite similar to the one of Proposition 3.28 (except that we work with proper representations).

Let $f_1, \dots, f_r$ be a complete reduced system of representatives of $C^+(d)$. We first define maps

$$h_i : R_p(f_i, n)/\mathrm{Aut}(f_i) \to \{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}$$

by $h_i(x, y) = b'$, where b is such that $\sigma f = [n, b', c']$ with $\sigma = \left(\begin{smallmatrix} x & y \\ * & * \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ the unique matrix for which $0 \leq b' < 2n$ (Lemma 3.29).

If $\tau \in \mathrm{Aut}(f_i)$, then $(x', y') = (x, y)\tau$ is another representation of n by f_i. As in the proof of Proposition 3.28, we see that $h_i((x, y)\tau) = h_i(x, y)$.

Therefore, we can induce maps $\overline{h}_i : R(f_i, p)/\mathrm{Aut}(f_i) \to \{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}$, and then a map

$$h = \coprod_{i=1}^{r} \overline{h}_i : R_d(n) \to \{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}.$$

We show that this map is injective. Indeed, suppose that $(x_1, y_1) \in \mathbb{Z}^2$ and $(x_2, y_2) \in \mathbb{Z}^2$ are representations of n by f_i, respectively f_j, such that

$$h([(x_1, y_1)]) = [b]_{\mathbb{Z}/2n} = h([(x_2, y_2)])$$

with $0 \leq b < 2n$. By definition, there exists $\sigma_1, \sigma_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma_1 f_i = [n, b, c_1]$ and $\sigma_2 f_i = [n, b, c_2]$ with $c_1, c_2 1\mathbb{Z}$. Consequently, since c_1, c_2 are determined by n, b and d, we get that

$$\sigma_1 f_i = \sigma_2 f_j, \text{ this is } \sigma_2^{-1}\sigma_1 f_i = f_j.$$

As in the proof of Proposition 3.28, we conclude that $i = j$ and $\sigma_1\sigma_2^{-1}(x_1, y_1) = (x_2, y_2)$ with $\sigma_1\sigma_2^{-1} \in \mathrm{Aut}(f_i)$, whence the injectivity.

We finally prove that h is surjective. Let $0 \leq b < 2n$ such that $b^2 \equiv d \pmod{4n}$, i.e. $d = b^2 - 4nc$ for some $c \in \mathbb{Z}$. The form $[n, b, c]$ has discriminant d, so it is equivalent to one of the f_i, say f_1 without loss of generality. Let $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma f_1 = [n, b, c]$. Note that n is properly represented by f_1 through $\sigma^T(1, 0)$. By definition, we consequently get that $h(\overline{\sigma^T(1, 0)}) = b$. □

The next step is to determine the cardinality of $\{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}$ for n, d as above.

Definition 3.38. For $m, n \geq 1$, let $S_m(n) = |\{x \in \mathbb{Z}/m : x^2 \equiv n \pmod{m}\}|$ be the number of solutions to $x^2 \equiv n$ in $\mathbb{Z}/m$.

Lemma 3.39. *Let p be a prime number, $r \geq 1$ and $n \geq 1$ an integer coprime to p. Then*

$$S_{p^r}(n) = 1 + \left(\frac{n}{p}\right) \text{ for } p > 2,\ r \geq 1$$

and if n is odd, $r > 2$,

$$S_2(n) = 1,\ S_4(n) = \begin{cases} 0 & \text{if } n \equiv 3 \pmod{4} \\ 2 & \text{if } n \equiv 1 \pmod{4} \end{cases},\ S_{2^r}(n) = \begin{cases} 4 & \text{if } n \equiv 1 \pmod{8} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. See [Lan99, Theorem 87, p. 62]. □

Lemma 3.40. *Let $d \equiv 0, 1 \pmod{4}$ be an integer and $n > 0$ coprime to d. Then*

$$S_{4n}(d) = 2 \sum_{m|n \text{ squarefree}} \left(\frac{d}{m}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol.

Proof. We write $n = 2^{d_0}p_1^{d_1} \cdots p_r^{d_r}$ with $p_1, \ldots, p_r > 2$ the prime numbers dividing n and $d_1, \ldots, d_2 \geq 0$. By the Chinese Theorem,

$$\mathbb{Z}/4n \cong \mathbb{Z}/2^{d_0+2} \times \mathbb{Z}/p_1^{d_1} \times \cdots \times \mathbb{Z}/p_r^{d_r}$$

as rings. The number $S_{4n}(d)$ can therefore be deduced from Lemma 3.39. Looking at the different cases for $S_{2^{d_0+2}}(d)$, we see that it equals $2\left(1 + \left(\frac{d}{2}\right)\right)$ if $d_0 \geq 1$ (i.e. $2|n$) and 2 if $d_0 = 0$ (i.e. $2 \not| n$). Therefore

$$S_{4n}(d) = 2\prod_{p|n}\left(1 + \left(\frac{d}{p}\right)\right) = \sum_{m|n \text{ squarefree}} \left(\frac{d}{m}\right)$$

by the multiplicative properties of the Kronecker symbol. □

Proof of Theorem 3.30. By Proposition 3.37, we have that

$$\sum_{i=1}^{r} |R_p(f_i, p)/\mathrm{Aut}(f_i)| = \left|\{b \in \mathbb{Z}/2n : b^2 \equiv d \pmod{4n}\}\right|.$$

Note that

$$|\{x \in \mathbb{Z}/4n : x^2 \equiv d \pmod{4n}\}| = 2|\{x \in \mathbb{Z}/2n : x^2 \equiv d \pmod{4n}\}|.$$

Indeed, we can define a map $\varphi : \{x \in \mathbb{Z}/4n : x^2 \equiv d \pmod{4n}\} \to \mathbb{Z}/2 \times \{x \in \mathbb{Z}/2n : x^2 \equiv d \pmod{4n}\}$, where $\varphi([x]) = (0, [x])$ if $0 \leq x < 2n$ and $\varphi([x]) = (1, [x])$ if $2n \leq x < 4n$. It is well-defined, injective, and surjective because for all $0 \leq x < 2n$ such that $x^2 \equiv d \pmod{4n}$, we have $(x + 2n)^2 \equiv d \pmod{4n}$ and then

$$\varphi([x]) = (0, [x]),\ \varphi([x + 2n]) = (1, [x]).$$

We can now count the number of proper representations of n, combining Proposition 3.37 and Lemma 3.40:

$$\sum_{i=1}^{r} |R_p(f_i, n)/\mathrm{Aut}(f_i)| = \sum_{\substack{m|n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right).$$

If $(x, y) \in \mathbb{Z}^2$ is any (proper or improper) representation of n by f_i, we can write $x = lx'$ and $y = ly'$ with $l = (x, y)$ and $x', y' \in \mathbb{Z}$ coprime. So we have $n = f_i(x, y) = l^2 f_i(x', y')$, this is (x', y') is a proper representation of the integer n/l^2. Conversely, if $1 \leq l|n^2$ and $(x', y') \in \mathbb{Z}^2$ is a proper representation of n/l^2 by f_i, then $l(x', y')$ is an improper representation n by f_i. Hence we see that there is a bijection between

$$R(f_i, n) \text{ and } \coprod_{1 \leq l|n^2} R_p(f_i, n/l^2).$$

Hence, permuting sums, we finally obtain that

$$\begin{aligned} r_d(n) = \sum_{i=1}^{r} |R_p(f_i, n)/\mathrm{Aut}(f_i)| &= \sum_{i=1}^{r} \sum_{1 \le l | n^2} |R_p(f_i, n/l^2)/\mathrm{Aut}(f_i)| \\ &= \sum_{1 \le l | n^2} \sum_{\substack{m | \frac{n}{l^2} \\ m \text{ squarefree}}} \left(\frac{d}{m}\right) \\ &= \sum_{1 \le l | n^2} \sum_{\substack{ml^2 | n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right) = \sum_{m|n} \left(\frac{d}{m}\right). \end{aligned}$$

□

5.3. Examples

Note that Propositions 3.28 and 3.37 with their proofs give explicit methods to determine all representations of an integer by a given form and invertible ideals of given norm in orders of quadratic fields.

In this paragraph, we illustrate these on a couple of examples.

Example 3.41. We compute the correspondence of Proposition 3.37 explicitly for $d = -3$ and $n = 309$. We know that $h(-3) = 1$ all primitive positive-definite forms of discriminant à -3 being equivalent to $[1, 1, 1]$. Theorem 3.30 gives

$$r_d(n) = w \sum_{m|n} \left(\frac{d}{m}\right) = 6 \cdot 2 = 12.$$

There are two solutions to $b^2 \equiv -3 \pmod{4 \cdot 309}$ for $b \in \mathbb{Z}/(2 \cdot 309)$, given by $b = 93, 525$. As in the proof of Proposition 3.37, the forms attached are, respectively,

$$f_1 = [309, 93, 7] \text{ and } f_2 = [309, 525, 223].$$

Using the method of Proposition 1.43, we find that $f_i = \sigma_i[1, 1, 1]$ with

$$\sigma_1 = \begin{pmatrix} 20 & -7 \\ 3 & -1 \end{pmatrix} \text{ and } \sigma_2 = \begin{pmatrix} -13 & -7 \\ -11 & -6 \end{pmatrix}$$

The proper representations of 309 by $[1, 1, 1]$ nonequivalent under automorphisms are then given by $(20, -7)$ and $(-11, -6)$. Using the explicit list of automorphisms computed in Example 3.17, we find that all proper representations of 309 by f_1 are given by the $6 \cdot 2 = 12$ solutions

$$(-20, 7), (11, 6), (20, -7), (-11, -6), (13, -20), (-17, 11), (-13, 20), (17, -11),$$

$$(-7, -13), (-6, 17), (7, 13), (6, -17).$$

Since $309 = 3 \cdot 103$ is squarefree, there are no unproper representations of 309 by $[1,1,1]$. Otherwise, we'd also have to determine the representations of $309/l^2$ for each l square dividing 309.

Let $K = \mathbb{Q}(\sqrt{-3})$. By Proposition 3.28, there are exactly 2 ideals of norm 309, given by $\mathfrak{a}_{f_1}$ and $\mathfrak{a}_{f_2}$, namely

$$[309, (93 - \sqrt{-3})/2] \text{ and } [309, (525 - \sqrt{-3})/2].$$

Example 3.42. We illustrate the correspondence of Proposition 3.37 for $d = -23$ and $n = 16$. We saw in Table 3.1 that $h(-23) = 3$, with the reduced forms

$$f_1 = [1,1,6], \;\; f_2 = [2,1,3], \;\; f_3 = [2,-1,3].$$

There are two solutions to $b^2 \equiv -23 \pmod{4 \cdot 16}$ for $b \in \mathbb{Z}/(2 \cdot 16)$, given by $b = 13, 19$. The forms attached are, respectively,

$$g_1 = [16, 13, 3] \text{ and } g_2 = [16, 19, 6].$$

We have $f_1 = \sigma_1 g_2$ and $f_2 = \sigma_1 g_3$ with

$$\sigma_1 = \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} \text{ and } \sigma_2 = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}.$$

The proper representations of 16 by f_1 and f_2 nonequivalent under automorphisms are therefore given by $(-1,-2)$, respectively $(1,-2)$. We proceed as before to get them all. Also, there are two ideals of norm 16 in $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-23})$ by Proposition 3.28, given by

$$[16, (13 - \sqrt{-23})/2] \text{ and } [16, (19 - \sqrt{-23})/2].$$

Example 3.43. To illustrate the indefinite case, we compute the correspondence of Proposition 3.37 explicitly for $d = 28$ and $n = 333$. There are four solutions to $b^2 \equiv 28 \pmod{4 \cdot 333}$ for $b \in \mathbb{Z}/(2 \cdot 333)$, given by $b = 278, 314, 352, 388$. The forms attached are, respectively,

$$g_1 = [333, 278, 58], g_2 = [333, 314, 74], g_3 = [333, 352, 93], g_4 = [333, 388, 113].$$

Using reduction of indefinite forms (see Chapter 1), we see that they are all equivalent to the form $f = [1, 4, -3]$ (see Example 1.57), i.e. $g_i = \sigma_i f$ with

$$\sigma_1 = \begin{pmatrix} 12 & 7 \\ 5 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} -15 & -2 \\ -7 & -1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 23 & -2 \\ 12 & -1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 40 & -7 \\ 23 & -4 \end{pmatrix}.$$

Therefore, proper representations of 333 by f nonequivalent under automorphisms of f are given by

$$s_1 = (12, 7), \;\; s_2 = (-15, -2), \;\; s_3 = (23, -2), \;\; s_4 = (40, -7).$$

Using the explicit description of the automorphisms of f given in Example 3.22, we can parametrize all proper representations of 333 by f, namely

$$s_i \begin{pmatrix} (m-4n)/2 & -n \\ -3n & (m+4n)/2 \end{pmatrix}$$

with $m, n \in \mathbb{Z}$ solutions to the Pell equations $m^2 - 28n^2 = \pm 4$ and $i = 1, \dots, 4$. Let $K = \mathbb{Q}(\sqrt{7})$ and $\mathcal{O} = \mathbb{Z} + 2\mathcal{O}_K$ the order of conductor 2 in K. By Proposition 3.28, there are four invertible ideals of norm 333 in $\mathcal{O}$, given by

$$[333, (278 - 2\sqrt{7})], [333, (314 - 2\sqrt{7})], [333, (352 - 2\sqrt{7})], [333, (388 - 2\sqrt{7})].$$

CHAPTER 4

DIRICHLET CLASS NUMBER FORMULA

With the theory developed and the results obtained in the previous chapter, we are now in position to prove the famous *Dirichlet class number formula*, which gives an explicit formula for $h_f(d)$, the number of classes of forms of discriminant d (or equivalently, up to a constant, the cardinality of the Picard group of an order in a quadratic field/class number $h(d)$ if d is a fundamental discriminant), in terms of a Dirichlet L-series.

The main result of the previous chapter is Theorem 3.30, which gives an explicit expression for the global problem of counting all representations of an integer by nonequivalent forms modulo automorphisms. More precisely, if $n \geq 1$ and $d \equiv 0, 1 \pmod 4$ is a discriminant, then

$$r_d(n) = \sum_{m|n} \left(\frac{d}{m}\right). \tag{4.1}$$

The idea which will lead to the class number formula is to approximate the average

$$A_d(N) := \frac{1}{N} \sum_{n \leq N} r_d(n)$$

in two ways, working form by form, by counting lattice points in geometrical shapes, and globally (i.e. considering a whole system of representatives at the same time), using Formula (4.1).

1. A global estimation with L-series

1.1. Dirichlet characters and L-series

First of all, we briefly recall some facts and definitions about Dirichlet characters and L-series, for the record.

Definition 4.1. A **Dirichlet character** modulo $q \geq 1$ is a character of the group $(\mathbb{Z}/n)^*$, this is a group homomorphism $\chi : (\mathbb{Z}/q)^* \to \mathbb{C}^*$.

Example 4.2. If q is an nonzero integer such that $q \equiv 0, 1 \pmod 4$, then the Kronecker symbol $\left(\frac{\cdot}{\cdot}\right)$ gives a character χ modulo q defined by

$$\chi(n) = \left(\frac{q}{n}\right).$$

We extend the domain of all Dirichlet characters χ modulo q to $\mathbb{Z}/q$ by setting $\chi(x) = 0$ if $(n, x) > 1$, so we get arithmetic functions. We denote by χ_0 the trivial character modulo q (i.e. $\chi(x) = 1$ for all $x \in (\mathbb{Z}/q)^*$)

Proposition 4.3. *If χ is a Dirichlet character modulo q, then $|\chi(x)| \leq 1$ for all $x \in \mathbb{Z}/q$ and*

$$\left|\sum_{x\in I} \chi(x)\right| \leq q$$

for all bounded interval $I \subset \mathbb{N}$.

Proof. See [Dav00, Ch. 4]. □

Definition 4.4. The **Dirichlet L-series** associated to a Dirichlet character χ is the series

$$L(\chi, s) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} \ (s \in \mathbb{C}).$$

Proposition 4.5. *Let χ be a Dirichlet character modulo q. If χ is not the trivial character, then $L(\chi, s)$ converges uniformly on all compact sets of the half-plane $Re(s) > 0$ and defines an holomorphic function in this domain. Moreover, we have the following estimation for the partial sums:*

$$\sum_{1\leq n\leq N} \frac{\chi(n)}{n^s} = L(\chi, s) + O\left(\frac{q|s|}{\sigma N^\sigma}\right)$$

for all $N \geq 1$ and $s \in \mathbb{C}$ such that $\sigma = Re(s) > 0$.

Proof. See [Dav00, Ch. 4]. □

1.2. The global asymptotic estimation

Using Equation (4.1) and permuting the sums, we obtain

$$\begin{aligned} NA_d(N) = \sum_{n\leq N} r_d(n) &= w \sum_{n\leq N} \sum_{m|n} \left(\frac{d}{m}\right) = w \sum_{m\leq N} \sum_{\substack{n\leq N \\ m|n}} \left(\frac{d}{m}\right) \\ &= w \sum_{m\leq N} \left[\frac{N}{m}\right] \left(\frac{d}{m}\right). \end{aligned}$$

A straightforward way to approximate this sum would be to write $[N/m] = N/m + O(1)$, but this would give $A_d(N) = \text{constant} + O(1)$ and we want an explicit formula. Instead, we split the sum at some $1 < K < N$ (to determine later) and work on the two parts separately (Dirichlet hyperbola method).

For the highest values, note that

$$\sum_{K<m\leq N}\left[\frac{N}{m}\right]\left(\frac{d}{m}\right)=\sum_{K<m\leq N}\sum_{l\leq N/m}\left(\frac{d}{m}\right)\leq\sum_{K<m\leq N}\sum_{l\leq N/K}\left(\frac{d}{m}\right),$$

so we can use Proposition 4.3 to get

$$\left|\sum_{K<m\leq N}\left[\frac{N}{m}\right]\left(\frac{d}{m}\right)\right|\leq|d|\frac{N}{K}.$$

For the lower part, we can use the straightforward approximation of $[N/m]$, to get

$$\sum_{m\leq K}\left[\frac{N}{m}\right]\left(\frac{d}{m}\right)=\sum_{m\leq K}\left(\frac{N}{m}+O(1)\right)\left(\frac{d}{m}\right)=N\sum_{m\leq K}\frac{1}{m}\left(\frac{d}{m}\right)+O(K).$$

Note that here, we will control the error term by a good choice of K.

By Proposition 4.5, the first term of the rightmost expression is $L(\left(\frac{d}{\cdot}\right),1)+O(N|d|/K)$. Therefore,

$$\sum_{m\leq K}\left[\frac{N}{m}\right]\left(\frac{d}{m}\right)=NL((d/\cdot),1)+O(N|d|/K)+O(K)$$

and combining the two parts, we finally get

$$NA_d(N)=\frac{N|d|}{K}+NL((d/\cdot),1)+O(N|d|/K)+O(K).$$

Thus, we can choose $K=\sqrt{N|d|}$ (which is smaller than N as soon as $N\geq|d|$) to obtain

$$\begin{aligned}A_d(N) &= \frac{|d|}{K}+L((d/\cdot),1)+O(|d|/N)+O(K/N)\\ &= L((d/\cdot),1)+o(1). \qquad (4.2)\end{aligned}$$

as $N\to\infty$.

2. A "geometrical" estimation working form by form

After the global estimation done in the previous section, we shall now proceed in an of $A_d(N)$ working form by form. The goal is to obtain an expression

$$A_d(N)=C+o(1)$$

when $N\to\infty$, with C independent from N. Indeed, we would then directly get an explicit expression for $h_f(d)$.

Let $d \equiv 0, 1 \pmod 4$ be a discriminant and $f_1, \ldots, f_{h_f(d)} \in \mathrm{Form}_p^+(d)$ a complete reduced system of representatives of $C_p^+(d)$. We remark that

$$r_d(N) \;=\; \left| \coprod_{i=1}^{h_f(d)} R(f_i, n)/\mathrm{Aut}(f_i) \right| = \sum_{i=1}^{h_f(d)} |R(f_i, n)/\mathrm{Aut}(f_i)|,$$

so permuting the two sums, we obtain problems concerning one form at a time,

$$NA_d(N) = \sum_{i=1}^{h_f(d)} \sum_{n \leq N} |R(f_i, n)/\mathrm{Aut}(f_i)|, \tag{4.3}$$

namely counting the number of proper representations of $0, \ldots, N$ by a given form, modulo automorphisms.

We begin by the case of definite forms, since it is easier. Indeed, if $d < 0$, then $|\mathrm{Aut}(f_1)| = \cdots = |\mathrm{Aut}(f_{h_f(d)})| := w < \infty$ by Corollary 3.16 and hence, Equation (4.3) reads

$$wNA_d(N) = \sum_{i=1}^{h_f(d)} \left(\sum_{n \leq N} r_{f_i}(n) \right),$$

with $r_{f_i}(n) := |R(f_i, n)|$. In other words, we have to count the number of integral points inside the ellipse defined by each of the f_i.

2.1. Integral points inside an ellipse

Let $f = [a, b, c]$ be a reduced form of discriminant $d = b^2 - 4ac < 0$ (in particular, $a > 0$). For an integer $N \geq 1$ fixed, we are interested in the number of integers $(x, y) \in \mathbb{Z}^2$ such that $ax^2 + bxy + cy^2 \leq N$, this is the number $\eta(E)$ of integral points inside the (solid) ellipse $(E) : ax^2 + bxy + cy^2 \leq N$.

To approximate $\eta(E)$, we consider for each $P = (x, y) \in \mathbb{Z}^2$ the square of side $1/2$ centered in P,

$$S_P = \{(z_1, z_2) \in \mathbb{R}^2 : |x - z_1| \leq 1/2, |y - z_2| \leq 1/2\}.$$

Then note that

$$\begin{aligned}
\mathrm{Area}(E) &= \sum_{P \in E \cap B^c \cap \mathbb{Z}^2} 1 - \mathrm{Area}\left(\bigcup_{P \in B \cap E} (S_P \cap E^c) \right) + \mathrm{Area}\left(\bigcup_{P \in B \cap E^c} (S_P \cap E) \right) \\
&= \eta(E) - \sum_{P \in B \cap E} \mathrm{Area}(S_P \cap E^c) + \sum_{P \in B \cap E^C} \mathrm{Area}(S_P \cap E) \\
&\leq \eta(E) + \sum_{P \in B} 1.
\end{aligned}$$

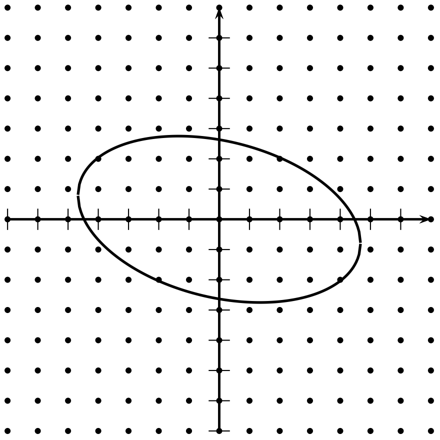


Figure 4.1: Integral points inside an ellipse.

where $B = \{P \in \mathbb{Z}^2 : S_P \cap \partial E \neq \emptyset\}$. Therefore, we could approximate $\eta(E)$ by Area(E) with an error smaller than $|B|$.

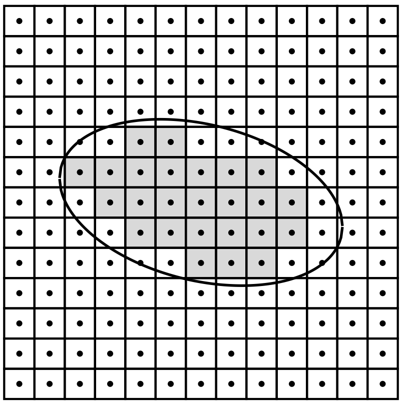


Figure 4.2: Approximating $\eta(E)$ with Area(E).

Note that, completing the square, the relation $ax^2 + bxy + cy^2 \leq N$ can be rewritten as

$$\left(\sqrt{a}x + \frac{b}{2\sqrt{a}}y\right)^2 + \frac{|d|}{4a}y^2 \leq N. \tag{4.4}$$

Hence, we see that

$$|y| \leq \sqrt{4aN/|d|} \text{ and } \left|\sqrt{a}x + \frac{b}{2\sqrt{a}}y\right| \leq \sqrt{\frac{4aN - |d|y^2}{4a}} \leq \sqrt{N}.$$

Geometrically, it means that the ellipse is contained in a parallelogram $ABCD$ with $\overline{AB} = \sqrt{N/a}$ and whose perpendicular height from C has length $\sqrt{4aN/|d|}$ (see Figure 4.3). Less precisely, it also implies that the ellipse is contained in a rectangle of sides $\sqrt{N/a}$ and $\sqrt{4aN/|d|}$.

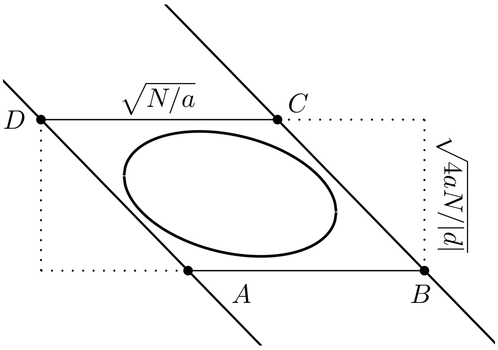


Figure 4.3: Ellipse bounded by a parallelogram.

We prove the following generalization of the classical sum-integral comparison (see [Krä88]):

Proposition 4.6. *Let $D \subset \mathbb{R}^m$ be a measurable set which is contained in a hyper-rectangle $D' \subset \mathbb{R}^n$, $D' = \{\mathbf{x} \in \mathbb{R}^{\mathbf{n}} : |x_i - y_i| \leq r_i\}$ for some $y_i \in \mathbb{R}$, $r_i > 0$, $1 \leq i \leq m$. Then, if $f : D' \to \mathbb{R}$ is a non-negative continuous bounded function monotonic in each variable, we have that*

$$\sum_{\underline{n} \in D} f(\underline{n}) = \int_D f(x_1, \dots, x_m) dx_1 \cdots dx_n + O\left(\sum_{i=1}^{m} \frac{r_1 \dots r_m}{r_i}\right).$$

Proof. We proceed by induction on $m \geq 1$. If $m = 1$, this is the classical integral-series comparison:

$$\sum_{n \in D} f(n) = \int_{x \in D} f(x) dx + O\left(\max_{x \in D} f(x)\right).$$

Suppose that the result holds for some $m - 1 \geq 1$ and let us prove it for m.

Let D, D' and f as above. Then by hypothesis and the case $n = 1$,

$$\begin{aligned}
\sum_{\underline{n}\in D} f(\underline{n}) &= \sum_{(n_1,\dots,n_{m-1})\in\pi(D)} \sum_{(n_1,\dots,n_m)\in D} f(n_1,\dots,n_m) \\
&\ll \int_{\pi(D)} \left(\sum_{\underline{x}=(x_1,\dots,x_{m-1},n_m)\in D} f(\underline{x}) \right) dx_1 \cdots dx_{m-1} + \sum_{i=1}^{m-1} \frac{r_1 \dots r_m}{r_i} \\
&\leq \int_{\pi(D)} \left(\sum_{\underline{x}=(x_1,\dots,x_{m-1},n_m)\in D'} f(\underline{x}) \right) dx_1 \cdots dx_{m-1} + \sum_{i=1}^{m-1} \frac{r_1 \dots r_m}{r_i} \\
&\ll \int_{\pi(D)} \left(\int_D f(x_1,\dots,x_m) dx_m + 1 \right) dx_1 \dots dx_{m-1} + \sum_{i=1}^{m-1} \frac{r_1 \dots r_m}{r_i} \\
&= \int_D f(\underline{x}) d\underline{x} + \sum_{i=1}^{m-1} \frac{r_1 \dots r_m}{r_i} + r_1 \dots r_{m-1} \\
&= \int_D f(\underline{x}) d\underline{x} + \sum_{i=1}^{m} \frac{r_1 \dots r_m}{r_i},
\end{aligned}$$

where $\pi : \mathbb{R}^m \to \mathbb{R}^{m-1}$ is the projection forgetting the m^{th} variable. The reverse inequality is proved similarly. □

By Proposition 4.6 applied to our ellipse contained in a rectangle, we finally get that

$$\eta(E) = \sum_{\underline{n}\in E} 1 = \text{Area}(E) + O\left(\sqrt{aN/|d|} + \sqrt{N/a}\right).$$

The area of E is easily computed with the change of variables $s = \sqrt{a}x + b/(2\sqrt{a})y$ and $t = y$, using Equation (4.4):

$$\text{Area}(E) = \int\int_E dxdy = \frac{1}{\sqrt{a}} \int ds \int dt \ 1_{s^2+|d|/(4a)t^2 \leq N} = \frac{2\pi N}{\sqrt{|d|}},$$

since the area of the ellipse $E' : s^2 + |d|/(4a)t^2 \leq N$ is $2\pi N\sqrt{a/|d|}$.

Thus, we finally obtain that

$$\eta(E) = \frac{2\pi N}{\sqrt{|d|}} + O_d(\sqrt{N}). \tag{4.5}$$

Indeed, a is bounded by a constant depending only on d (see Proposition 1.41) as long as f is reduced.

2.2. Conclusion

We can now return to Equation 4.3 and use the approximation obtained in the last paragraph:

$$NA_d(N) = \sum_{i=1}^{h_f(d)} \sum_{n \le N} r_{f_i}(n) = \sum_{i=1}^{h_f(d)} \left(\frac{2\pi N}{\sqrt{|d|}} + O_d(\sqrt{N}) \right)$$

therefore

$$A_d(N) = \frac{2\pi h_f(d)}{\sqrt{|d|}} + O\left(h_f(d)/\sqrt{N}\right). \tag{4.6}$$

3. The class number formula for imaginary quadratic fields

In the two previous section, we obtained the estimations

$$wA_d(N) = \frac{2\pi h_f(d)}{\sqrt{|d|}} + O\left(h_f(d)/\sqrt{N}\right) \quad \text{(Equation (4.6))}$$

when $d < 0$ and

$$A_d(N) = L((d/\cdot), 1) + o(1) \quad \text{(Equation (4.2))}.$$

Combining the two ones, we immediately get an explicit formula for h_f (which is equal to h for negative fundamental discriminants by Proposition 3.7), *Dirichlet class number formula* for imaginary quadratic fields:

Proposition 4.7 (Dirichlet class number formula for imaginary quadratic fields, 1839)**.** *Let* $d \equiv 0, 1 \pmod 4$ *be a negative discriminant. Then*

$$h_f(d) = \frac{w}{2\pi}\sqrt{|d|}L((d/\cdot), 1).$$

Note that as an immediate corollary, because $h_f(d)$ is the cardinal of a group, we get that

$$L((d/\cdot), 1) \ge \frac{2\pi}{w\sqrt{|d|}}$$

and since $w = 2$ if $d < -4$, this implies $L((d/\cdot), 1) \ge \pi/\sqrt{|d|}$ in this case.

4. The form-by-form estimation in the indefinite case

We return to the form-by-form estimation in the indefinite case. Recall that by Equation (4.3), we want to find an estimation of $\sum_{n \le N} |R(f, n)/\mathrm{Aut}(f)|$

for a given indefinite form f, since

$$NA_d(N) = \sum_{i=1}^{h_f(d)} \sum_{n \leq N} |R(f_i, n)/\mathrm{Aut}(f_i)| \tag{4.7}$$

if $f_1, \ldots, f_{h_f(d)}$ is a complete system of representatives of $C_p^+(d)$. Without loss of generality, we can suppose that the X^2-coefficients of these forms is positive. Indeed, if f is an indefinite form, then f represents a positive number n and by Proposition 1.25, we get that f is equivalent to a form $[n, *, *]$.

The situation is more complicated than in the definite case, because $\mathrm{Aut}(f)$ is infinite and the same holds for $R(f, n)$ as soon as it contains an element.

To overcome this, the idea is, given an indefinite form f, to find a set of representatives of $R(f, n)/\mathrm{Aut}(f)$ (so points in $\mathbb{Z}^2$) characterized in a geometric way so we can count them as what we did in the definite case.

4.1. Determining a set of representatives

Let $f = [a, b, c]$ be an indefinite form. By Example 3.22, the $\mathrm{Aut}(f)$-orbit of an element $(x, y) \in R_p(f, n)$ is given by

$$\left\{ (x, y) \begin{pmatrix} (u + nb)/2 & -na \\ nc & (u - nb)/2 \end{pmatrix} : u^2 - dn^2 = \pm 4 \right\}.$$

Recall that $\mathrm{Aut}(f)$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}$ (Proposition 3.19) and the same holds for the group of solutions $(u, n) \in \mathbb{Z}^2$ to $u^2 - dn^2 = \pm 4$ with the induced group structure from $\mathrm{Aut}(f)$. More precisely, it can be shown (see [Fla89, Ch. 4, §3]) that there exists a real number $\varepsilon_d > 1$ such that

$$\{(u, n) \in \mathbb{Z}^2 : u^2 - dn^2 = \pm 4\} = \left\{ (u, n) \in \mathbb{Z}^2 : \frac{u + n\sqrt{d}}{2} = \pm \varepsilon_d^k,\ k \in \mathbb{Z} \right\}.$$

Explicitly, $\varepsilon_d = (t_0 + u_0\sqrt{d})/2$, with $(t_0, u_0) \in \mathbb{Z}^2$ the solution to the Pell equation $t^2 - du^2$ with $u_0, t_0 > 0$ and u_0 minimal.

Now, let $\rho_\pm = (-b \pm \sqrt{d})/(2a)$ be the two zeroes of $f(\,\cdot\,, 1)$ so that

$$f = a(X - Y\rho_+)(X - Y\rho_-).$$

If (x', y') is another representation of n by f equivalent to (x, y),

$$(x', y') = (x, y) \begin{pmatrix} (u + nb)/2 & -na \\ nc & (u - nb)/2 \end{pmatrix},$$

with $u^2 - dn^2 = \pm 4$ (x, y), then the first factor transforms to

$$\begin{aligned} x' - y'\rho_+ &= \frac{u+nb}{2}x + ncy - \rho_1\left(-nax + \frac{u-nb}{2}y\right) \\ &= \left(\frac{u+\sqrt{d}n}{2}\right)x + \left(\frac{n(4nc-b^2)+bu-\sqrt{d}u+\sqrt{d}nb}{4a}\right)y \\ &= \frac{u+\sqrt{d}n}{2}(x-y\rho_+) = \pm\varepsilon_d^k(x-y\rho_+). \end{aligned}$$

for some $k \in \mathbb{Z}$ and similarly

$$x' - y'\rho_- = \frac{u-\sqrt{d}n}{2}(x-y\rho_-) = \pm\varepsilon_d^{-k}(x-y\rho_-).$$

Therefore, we have the relation

$$\frac{x'-y'\rho_+}{x'-y'\rho_-} = \varepsilon_d^{2k}\frac{x-y\rho_+}{x-y\rho_-},$$

which implies that a representative (x', y') of $R(f, n)/\mathrm{Aut}(f)$ can be uniquely determined with the condition

$$1 \le \frac{x'-y'\rho_+}{x'-y'\rho_-} < \varepsilon_d^2.$$

Recall that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is always an automorphism, so $(-x, -y) \in R(n, f)$ is equivalent to (x, y). Consequently, we may assume that $x' - y'\rho_-$ is positive. A representation satisfying these conditions will be called *f-primary*. By definition, there are finitely many of them.

4.2. Integral points counting

By the previous paragraph, for f an indefinite form,

$$\sum_{n\le N} |R_p(f,n)/\mathrm{Aut}(f)| = \sum_{n\le N}\sum_{\substack{(x,y)\in R_p(f,n)\\ f-\text{primary}}} 1$$

and we are again reduced to computing the number of integral points inside a certain region of the plane, namely

$$E = \left\{(x,y)\in\mathbb{Z}^2 : f(x,y)\le N, x-y\rho_- > 0,\ 1 \le \frac{x-y\rho_+}{x-y\rho_-} < \varepsilon^2\right\}$$

with $\rho_\pm$ are the roots of $f(\,\cdot\,, 1)$ as given in the previous paragraph.

Since this region is still included in the ellipse $f(x,y)=N$, it is, as in Paragraph 4.2.1, contained in a rectangle of sides $\sqrt{N/a}$ and $\sqrt{4aN/|d|}$. We may therefore apply Proposition 4.6:

$$\sum_{(x,y)\in E} 1 = \mathrm{Area}(E) + O\left(\sqrt{N/a} + \sqrt{4aN/|d|}\right).$$

To determine the area of E, we do the change of variables

$$\begin{array}{rcl} u(x,y) & = & x - y\rho_+ \\ v(x,y) & = & x - y\rho_- \end{array}$$

whose Jacobian is $\rho_+ - \rho_- = \sqrt{d}/a$. Since $f(x,y) = a(x-y\rho_+)(x-y\rho_-)$, we see that E can be written in the coordinates as

$$E = \left\{(x,y)\in\mathbb{Z}^2 : au(x,y)v(x,y) \le N, v(x,y) > 0,\ 1 \le \frac{u(x,y)}{v(x,y)} < \varepsilon^2\right\}.$$

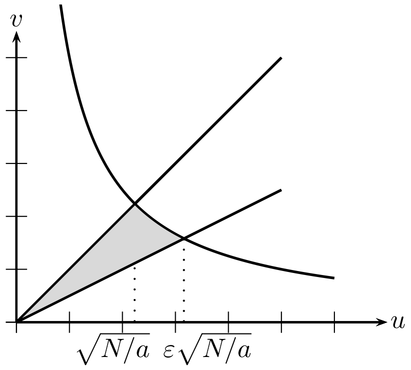


Figure 4.4: The region E in coordinates (u,v).

Consequently,

$$\begin{array}{rcl} \mathrm{Area}(E) & = & \dfrac{a}{\sqrt{d}}\left(\displaystyle\int_0^{\sqrt{N/a}}\left(u - \frac{u}{\varepsilon^2}\right)du + \int_{\sqrt{N/a}}^{\varepsilon\sqrt{N/a}}\left(\frac{N}{au} - \frac{u}{\varepsilon^2}\right)du\right) \\ & = & \dfrac{a}{\sqrt{d}}\left(\left(1 - \dfrac{1}{\varepsilon^2}\right)\dfrac{N}{a} + \dfrac{N}{a}\log\varepsilon - \varepsilon^2\dfrac{N}{a\varepsilon^2} + \dfrac{N}{a\varepsilon^2}\right) \\ & = & \dfrac{N}{\sqrt{d}}\log\varepsilon. \end{array}$$

Hence,

$$\begin{array}{rcl} \displaystyle\sum_{(x,y)\in E} 1 & = & \dfrac{N}{\sqrt{d}}\log\varepsilon + O\left(\sqrt{N/a} + \sqrt{4aN/|d|}\right) \\ & = & \dfrac{N}{\sqrt{d}}\log\varepsilon + O_d(\sqrt{N}), \end{array} \tag{4.8}$$

since a is bounded by a constant depending on d (see Proposition 1.52).

4.3. Conclusion

By Equation (4.7) and our form-by-form estimation (Equation (4.8)), we obtain that

$$NA_d(N) = \sum_{i=1}^{h_f(d)} \sum_{n\leq N} |R(f_i,n)/\mathrm{Aut}(f_i)| = \sum_{i=1}^{h_f(d)} \left(\frac{N}{\sqrt{d}} \log\varepsilon + O_d(\sqrt{N}) \right),$$

therefore

$$A_d(N) = \frac{h_f(d)}{\sqrt{d}} \log\varepsilon + O_d\left(h_f(d)/\sqrt{N}\right). \tag{4.9}$$

5. The class number formula for real quadratic fields

In a similar manner than for positive discriminants, we obtained the estimation

$$A_d(N) = \frac{h_f(d)}{\sqrt{d}} \log\varepsilon + O_d\left(h_f(d)/\sqrt{N}\right) \text{ Equation (4.9)}$$

and we still have the global estimation

$$A_d(N) = L((d/\cdot),1) + o(1) \quad \text{(Equation (4.2))}.$$

Combining these, we directly obtain

Proposition 4.8 (Dirichlet class number formula for real quadratic fields, 1839)**.** *Let $d \equiv 0,1 \pmod 4$ be a positive squarefree discriminant. Then*

$$h_f(d) = \frac{1}{\log\varepsilon_d} \sqrt{d}\, L((d/\cdot),1),$$

where $\varepsilon_d = (t_0 + u_0\sqrt{d})/2$, with $(t_0,u_0) \in \mathbb{Z}^2$ is the solution to Pell equation $t^2 - du^2$ with $u_0, t_0 > 0$ and u_0 minimal.

Remark that the only difference with the imaginary case is that the factor $w/(2\pi)$ is replaced by $1/\log\varepsilon_d$.

By Proposition 3.7, we get a similar formula for $h(d)$ when $d > 0$ is a fundamental discriminant (namely the same one, multiplied by a factor of 1 or 1/2, depending on whether the ring of integers of $\mathbb{Q}(\sqrt{d})$ has a unit of norm -1 or not), *Dirichlet class number formula for real quadratic fields.*

5.1. A lower bound for $L((d/\cdot),1)$

As in the imaginary case, we can use the class number formula to obtain a lower bound for $L((d/\cdot),1)$ when $d>0$. Indeed, since $h_f(d)$ is the cardinal of a group, we get that

$$L((d/\cdot),1) \geq \frac{\log \varepsilon_d}{\sqrt{d}}.$$

On the other hand,

$$\varepsilon_d = \frac{t_0 + u_0\sqrt{d}}{2} > \sqrt{d},$$

because $t_0^2 = 4 + du_0^2 > du_0^2 \geq d$. Thus

$$L((d/\cdot),1) \geq \frac{\log \sqrt{d}}{\sqrt{d}}.$$

CHAPTER 5

CONCLUSION AND PERSPECTIVES

The aim of this project was to study and present the relationship between binary quadratic forms and quadratic fields. As a final result, we obtained the Dirichlet class number formula, expressing class numbers of quadratic fields in terms of a L-series. In a certain sense, this result and its proof summed up the correspondence between forms and quadratic fields, since the main ingredients of the proof were:

- Using the equality up to a constant of h_f and h to move the problem *between class numbers of forms and class numbers of quadratic fields.* In the point of view of forms, a lattice point counting led to an estimation of the number of representations of some integers by a given form;
- Obtaining a closed expression counting representations of a given integers by forms of given discriminants (modulo equivalence of forms and actions of automorphisms). To do this, we transposed the problem *in the point of view of quadratic fields*, seeing it as the question of integers represented by norms of ideals, where the problem was much easier to understand and solve (observing how ideals generated by prime numbers factorize).

Being without any doubt a beautiful theoretical result, we saw that the correspondence could moreover be used in computations, being of benefit for both points of view. This is, for example:

- Determining Picard groups of orders in quadratic fields explicitly using the theory of reduction of forms;
- Determining and parametrizing representations of integers by given forms, using the parametrization of automorphisms obtained from units in orders of quadratic fields.

Perspectives

The following topics could be studied further to the subjects introduced in this document:

- Asymptotic formulas for averages of class numbers, as conjectured by

Gauss in the *Disquisitiones Arithmeticae* [Gau86, Art. 302 and 304]:

$$\sum_{k\leq N} h(-4k) \sim \frac{4\pi}{21\zeta(3)}N^{3/2}, \quad \sum_{k\leq N} h(4k)\log \epsilon_{4k} \sim \frac{4\pi^2}{21\zeta(3)}N^{3/2}.$$

The first one, in the imaginary case, was proven by Lipschitz in 1865. The second one, in real case, was proven (along with more precise versions and for all discriminants) by Siegel in 1944 ([Sie44]), using the Pólya-Vinogradov inequality.

- We could investigate how the structure of the class groups (forms and Picard groups) can be determined using the two settings (recall that these are finite abelian groups) and complete Tables 3.1 and 3.3 with this information.
- Genus theory, allowing to say much more about representation of integers whose discriminant has class number more than 1 (see [Cox89]).
- Bhargava's articles [Bha04a], [Bha04b], [Bha04c] and [Bha08], introduced in Chapter 3.
- Generalization of Dirichlet class number formula in Picard groups of orders in quadratic fields and Heegner, Stark and Baker's proof for the answer to the class number one problem (see [Cox89, Ch. 2, §7]).
- Siegel's formula: for any $\varepsilon > 0$, there exists a constant $C(\varepsilon) > 0$ (not computable) such that for all fundamental discriminants d,

  $$h(d) > C(\varepsilon)|d|^{1/2-\varepsilon}$$

  or Goldfeld-Gross-Zagier's formula, whose constant is explicit:

  $$h(d) = \frac{\log|d_K|}{7000}\prod_{p|d}\left(\frac{1-\lceil 2\sqrt{p}\rceil}{p+1}\right).$$

BIBLIOGRAPHY

[Bha04a] Manjul Bhargava. Higher composition laws I: A new view on gauss composition, and quadratic generalizations. *Annals of Mathematics*, 159(1):pp. 217–250, 2004.

[Bha04b] Manjul Bhargava. Higher composition laws II: On cubic analogues of gauss composition. *Annals of Mathematics*, 159(2):pp. 865–886, 2004.

[Bha04c] Manjul Bhargava. Higher composition laws III: The parametrization of quartic rings. *Annals of Mathematics*, 159(3):pp. 1329–1360, 2004.

[Bha08] Manjul Bhargava. Higher composition laws IV: The parametrization of quintic rings. *Annals of Mathematics*, 167(1):pp. 53–94, 2008.

[Coh93] Henri Cohen. *A course in computational algebraic number theory.* Springer, Berlin Heidelberg New-York, 1993.

[Cox89] David Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Wiley, New York, 1989.

[Dav00] Harold Davenport. *Multiplicative number theory.* Springer, New York, 2000.

[Fla89] Daniel Flath. *Introduction to number theory.* Wiley, New York, 1989.

[Gau86] Carl Friedrich Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986.

[Gra07] Andrew Granville. Théorie analytique des nombres (course notes). `http://www.dms.umontreal.ca/~andrew/Courses/MAT6684.W07.html`, 2007.

[Hec10] Erich Hecke. *Lectures on the theory of algebraic numbers.* Springer, S.l, 2010.

[Kle07] Israel Kleiner. *A history of abstract algebra.* Birkhäuser Springer, distributor, Boston, Mass. London, 2007.

[Krä88] Ekkehard Krätzel. *Lattice points.* Kluwer Academic Publishers, Dordrecht Boston, 1988.

[Lan99] Edmund Landau. *Elementary number theory.* AMS Chelsea Pub, Providence, R.I, 1999.

[Neu99] Jürgen Neukirch. *Algebraic number theory.* Springer, Berlin, New York, 1999.

[S^+11] W. A. Stein et al. *Sage Mathematics Software (Version 4.6.2).* The Sage Development Team, 2011. `http://www.sagemath.org`.

[Sam71] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, Paris, 1971.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, Princeton, N.J, 1994.

[Sie44] Carl Ludwig Siegel. The average measure of quadratic forms with given determinant and signature. *Annals of Mathematics*, 45(4):pp. 667–685, 1944.

[ST10] Joseph Silverman and John Tate. *Rational points on elliptic curves.* Springer-Verlag, New York, 2010.

[Ste03] William Stein. Elementary number theory and elliptic curves. `http://modular.math.washington.edu/edu/Fall2002/124/stein/`, 2003.

[Sti10] John Stillwell. *Mathematics and its history.* Springer, New York, 2010.

APPENDIX A

NUMBER FIELDS

Definition A.1. An (algebraic) **number field** is a finite extension of $\mathbb{Q}$.

Proposition A.2. *Any number field K is a simple extension, i.e. there exists $x \in K$ such that $K = \mathbb{Q}(x)$.*

In the rest of this chapter, let K be a number field.

1. Ring of integers

Definition A.3. An element of K is an **algebraic integer** if it is the root of an monic polynomial with integer coefficients.

Proposition A.4. *An element of K is an algebraic integer if and only if its minimal polynomial on $\mathbb{Q}$ has integer coefficients.*

Proof. See sections 2.1-2.3 of [Sam71] or section I.2 of [Neu99]. □

Proposition A.5. *The set of algebraic integers of K is a ring, denoted by $\mathcal{O}_K$, the **ring of integers**. We have that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ and K is the field of fractions of $\mathcal{O}_K$. More precisely, every element of K can be written as a/b where $a \in \mathcal{O}_K$ and $b \in \mathbb{Q}^*$*

Proof. See sections 2.1-2.3 of [Sam71] or section I.2 of [Neu99]. □

Proposition A.6. *The ring of integers of K is a free abelian group of rank the degree of K. In particular, K possesses a $\mathbb{Q}$-basis consisting of algebraic integers.*

Speaking of free abelian group, let us recall the following result:

Proposition A.7. *Let G be a free abelian group of rank n with basis $(x_1, \ldots, x_n)$. Let C a $n \times n$ matrix with integer entries and define $y_i = \sum_{j=1}^{n} c_{ij} x_j \in G$ for $1 \leq i \leq n$. Then $(y_1, \ldots, y_n)$ is a basis for G if and only if $C \in \mathrm{GL}_n(\mathbb{Z})$.*

2. Norm, trace and characteristic polynomial

Definition A.8. Let K an algebraic number field. For all $x \in K$, we can consider the $\mathbb{Q}$-linear map $m_x : K \to K$ given by $m_x(y) = xy$. Then for all $x \in K$, we define

- $N_K(x) = \det(m_x) \in \mathbb{Q}$, the **norm** of x;
- $\mathrm{Tr}_K(x) = \mathrm{Tr}(m_x) \in \mathbb{Q}$, the **trace** of x;
- $\Delta_K(x) = \det(X \,\mathrm{id} - m_x) \in \mathbb{Q}[X]$ the **characteristic polynomial** of x.

Proposition A.9. *Let K an algebraic number field and $x, x' \in K$, $a \in \mathbb{Q}$. Then*

- *The trace is a $\mathbb{Q}$-linear function;*
- *The norm is a multiplicative function and $N(a) = a^n$, $N(ax) = a^n N(x)$;*
- *The characteristic polynomial of x verifies $\Delta(x) = X^n - \mathrm{Tr}(x)X^{n-1} + \cdots + (-1)^n N(x)$.*

Proposition A.10. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n and $x \in K$. If $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ are the n distinct K-homomorphisms, then*

$$N(x) = \prod_{i=1}^{n} \sigma_i(x),\ \mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x),\ \Delta(x) = \prod_{i=1}^{n}(X - \sigma_i(x)).$$

Corollary A.11. *If x is an algebraic integer of a number field, then the same holds for $N_K(x)$ and $\mathrm{Tr}_K(x)$.*

3. Discriminants

Definition A.12. Let K be an algebraic number field and let $(x_1, \dots, x_n)$ be a $\mathbb{Q}$-basis of K. The **discriminant** of $(x_1, \dots, x_n)$ is

$$D(x_1, \dots, x_n) = \det(\mathrm{Tr}(x_i x_j))_{ij}.$$

Proposition A.13. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n and $(x_1, \dots, x_n)$ a $\mathbb{Q}$-basis of K. If $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ are the n distinct K-homomorphisms, then*

1. $D(x_1, \dots, x_n) = (\det(\sigma_i(x_j))_{ij})^2 \neq 0$*;*
2. $D(x_1, \dots, x_n)$ *is a nonzero rational integer;*
3. *If $(y_1, \dots, y_n)$ is another $\mathbb{Q}$-basis, then*

$$D(y_1, \dots, y_n) = \det(M)^2 D(x_1, \dots, x_n),$$

where $(y_1, \dots, y_n)^T = M(x_1, \dots, x_n)^T$.

Proposition A.14. *Let K be an algebraic number field of degree n and $(x_1, \dots, x_n)$ a $\mathbb{Q}$-basis of K. If $D(x_1, \dots, x_n)$ is squarefree, then $(x_1, \dots, x_n)$ is an **integral basis** (i.e. a basis for the free abelian group $\mathcal{O}_K$).*

Note that any integral basis is a $\mathbb{Q}$-basis for the number field (by the last part of Proposition A.5). Moreover, the discriminants of any such basis are all equal. Indeed, if $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ are two integral basis for a number field K, let M be the transition matrix. Then M is an unimodular matrix and $\det M = \pm 1$, which gives the result by Proposition A.13.

Thus we can define the following:

Definition A.15. The **discriminant** d_K of a number field K is the discriminant of any integral basis.

4. Ideals

Proposition A.16. *For every ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the index $[\mathcal{O}_K : \mathfrak{a}]$ is finite and $\mathfrak{a}$ is a free abelian group of rank the degree of K.*

Unfortunately, the ring of integers of a number field is generally not a unique factorization domain. Nonetheless, we get such a property if we look at a generalization of ideals:

Definition A.17. Let K be a number field. A **fractional ideal** of K is a set of the form

$$a^{-1}\mathfrak{a},$$

where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and a a nonzero element of $\mathcal{O}_K$. We denote by $\mathcal{I}_K$ the set of nonzero fractional ideals of K.

The product of two fractional ideals is then defined in the same way than for ideals and it is a composition law in $\mathcal{I}_K$.

Theorem A.18. *Let $\mathfrak{a} \in \mathcal{I}_K$ be a nonzero fractional ideal. Then:*

1. *The ideal $\mathfrak{a}$ has an inverse with respect to the multiplication in $\mathcal{I}_K$, denoted by $\mathfrak{a}^{-1}$. Therefore, $\mathcal{I}_K$ has an abelian group structure for the multiplication with identity $\mathcal{O}_K$;*
2. *There exist distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of $\mathcal{O}_K$ and integers $n_1, \dots, n_r \in \mathbb{Z}$ such that*
$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}.$$
Moreover, this decomposition is unique up to permutation of the factors.

Proof. See section 3.4 of [Sam71] or section II.3 of [Neu99]. □

Definition A.19. We say that $\mathfrak{b}$ **divides** $\mathfrak{a}$ (written $\mathfrak{a}|\mathfrak{b}$) if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Proposition A.20. *If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of K, then $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{a} \supset \mathfrak{b}$.*

Proposition A.21. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Then $\mathcal{O}/\mathfrak{a}$ is finite and we call its cardinality the **norm** $N(\mathfrak{a})$ of the ideal. More precisely, if $(x_1, \dots, x_n)$ is any $\mathbb{Z}$-basis for $\mathfrak{a}$, then*

$$N(\mathfrak{a})^2 = \frac{D(x_1, \dots, x_n)}{d_K}.$$

The terminology norm is meaningful by the first point of the following proposition.

Proposition A.22. *Let $\mathfrak{a}, \mathfrak{b}$ nonzero ideals of $\mathcal{O}_K$. Then*

1. *If $\mathfrak{a} = \langle x \rangle$ is a principal ideal, then $N(\mathfrak{a}) = |N(x)|$;*
2. *$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$;*
3. *If $N(\mathfrak{a})$ is a prime number, then $\mathfrak{a}$ is a prime ideal;*
4. *If $\mathfrak{a}$ is a prime ideal, then it divides exactly one prime number p and $N(\mathfrak{a}) = p^m$ with m smaller than the degree of K.*

The Kummer-Dedekind Theorem gives a simple way to compute the decomposition under an hypothesis on $\mathcal{O}_K$ (which holds for example for quadratic or cyclotomic fields):

Proposition A.23 (Kummer-Dedekind)**.** *Suppose that $\mathcal{O}_K = \mathbb{Z}[\theta]$ and let $f \in \mathbb{Z}[X]$ the minimal polynomial of θ over $\mathbb{Q}$. If p is a prime number, let*

$$\overline{f_1^{n_1}} \dots \overline{f_r^{n_r}}$$

be the decomposition into irreducibles of f in $\mathbb{Z}_p[X]$. Then the ideals

$$\mathfrak{p}_i = (p) + (f_i(\theta))$$

of $\mathcal{O}_K$ are prime ($1 \leq i \leq r$) and the decomposition of (p) into prime ideals in $\mathcal{C}l(K)$ is

$$(p) = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}.$$

Proof. See for example [Coh93, Th. 4.8.13]. □

5. Ideal class group

Definition A.24. Let K be a number field and $\mathcal{I}_0$ the subgroup of $\mathcal{I}_K$ consisting of principal fractional ideals (i.e. fractional ideals $x\mathcal{O}_K$ for $x \in K^*$). The **ideal class group** $\mathcal{C}l(K)$ is the quotient group $\mathcal{I}_K/\mathcal{I}_0$.

Theorem A.25 (Minkowski)**.** *The ideal class group of a number field is finite.*

Proof. See section 4.3 or [Sam71] or section I.6 (theorem 6.3) of [Neu99]. □

Definition A.26. The **class number** $h(K)$ of a number field K is the cardinality of its ideal class group.

Proposition A.27. *The ring of integers $\mathcal{O}_K$ of a number field K is an unique factorization domain if and only if $h(K) = 1$.*

6. Orders

It is also interesting to work on subrings of K sharing important properties of the ring of integers $\mathcal{O}_K$, except that they might not be integrally closed, so they might not be Dedekind domain (i.e. factorization of invertible ideals as product of primes ideals) nor verify that all ideals are invertible.

The proof of the following result can be found in [Neu99, Ch. I, §12] or [Cox89, Ch. II, §7].

Definition A.28. An **order** in a number field K is a subring $\mathcal{O} \subset K$ such that

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

By Propositions A.5 and A.6, the ring of integers $\mathcal{O}_K$ itself is an order. We call it the **maximal order** in K.

Proposition A.29. *Any order $\mathcal{O}$ in K is a noetherian ring, a free $\mathbb{Z}$-module of rank the degree of K and is contained in $\mathcal{O}_K$. Moreover, we have that $K = \mathbb{Q}\mathcal{O}$.*

Thus, we see that orders are actually subrings of the ring of integers.

As with $\mathcal{O}_K$, any $\mathbb{Z}$-basis for an order $\mathcal{O}$ is also a $\mathbb{Q}$-basis for K and the discriminants of all such basis are equal. Therefore, we can define the **discriminant** of $\mathcal{O}$ as the discriminant of any $\mathbb{Z}$-basis of $\mathcal{O}$.

6.1. Ideals

As we did in maximal orders, we can also consider ideals and fractional ideals (i.e. subsets of K of the form $x\mathfrak{a}$ where $x \in K^*$ and $\mathfrak{a}$ an $\mathcal{O}$-ideal) in any order. We have the following similar results.

Proposition A.30. *A nonzero fractional ideal in an order is a free $\mathbb{Z}$-module of rank the degree of K.*

Proposition A.31. *All prime ideals in an order of a number field are maximal.*

Proposition A.32. *Let $\mathfrak{a}$ be an ideal of an order $\mathcal{O}$ in K. Then $\mathcal{O}/\mathfrak{a}$ is finite and we call its cardinality the* ***norm*** *$N(\mathfrak{a})$ of the ideal. The following properties hold:*

1. *For all $x \in \mathcal{O}$, $N((x)) = |N(x)|$.*
2. *For all invertible ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$, $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$*
3. *If $(x_1, \ldots, x_n)$ is any $\mathbb{Z}$-basis of an ideal $\mathfrak{a}$ in $\mathcal{O}$, then*

$$N(\mathfrak{a})^2 = \frac{D(x_1, \ldots, x_n)}{d_K}.$$

However, we will not generally have a property of unique factorization of ideals as prime ideals or invertibility with fractional ideals.

6.2. Picard groups

Still, we define a generalized version of the class group, restricting ourselves to invertible ideals. Let $\mathcal{O}$ be an order in K. Denote by $J(\mathcal{O})$ the set of invertible fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ the set of principal fractional $\mathcal{O}$-ideals. Clearly, $P(\mathcal{O}) \subset J(\mathcal{O})$.

Definition A.33. The **Picard group** of $\mathcal{O}$ is the quotient group

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

We will also need a "bigger" version of the Picard group:

Definition A.34. The **narrow Picard group** of $\mathcal{O}$ is the quotient group

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

where $P^+(\mathcal{O})$ is the ideals in $P(\mathcal{O})$ with a generator of positive norm.

Example A.35. The Picard group of the maximal order is of course the ideal class group of K.

Theorem A.36. *The groups $\mathcal{O}_K^*/\mathcal{O}^*$, $Pic(\mathcal{O})$ and $Pic^+(\mathcal{O})$ are finite.*

Proof. See [Neu99, Theorem 12.12]. □