Quadratic Forms
and
Elliptic Curves

Ernst Kani
Queen's University

Fall 2008

Revised: January 2010

Contents

Part I

Quadratic Forms and Lattices

Chapter 1

Binary Quadratic Forms

1.1 Introduction

In this chapter we shall study the elementary theory of (integral) binary quadratic forms

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

where a, b, c are integers. This theory was founded by Fermat, Euler, Lagrange, Legendre and Gauss, and its development is synonymous with the early development of number theory.[1]

However, problems involving binary quadratic forms were already studied in antiquity. For example, around 400BC people in India and Greece found successive approximations $\frac{a}{b}$ to $\sqrt{2}$ which satisfied the equation

$$a^2 - 2b^2 = 1,$$

(cf. [Di], II, p. 341), and a Greek epigram which is attributed to Archimedes (ca. 150BC) (but which was only discovered in 1773) leads to the equation

$$x^2 - ay^2 = 1$$

in which $a \approx 4 \times 10^{14}$; cf. [Di] II, p. 342, [We], p. 19. It is not known if Archimedes knew how to solve such equations.

As is well-known, Fermat's "birth of number theory" was inspired by Bachet's translation (1621) of the *Arithmetica* of Diophantus (ca. 250AD). In that text one finds many problems involving sums of squares, often in connection with triangles and the Theorem of Pythagoras. For example, in Book V, Problem 12, Diophantus poses a problem which is equivalent to solving the equation

$$x^2 + y^2 = n \quad (n \text{ odd}), \tag{1.1}$$

[1] According to Weil[We], p. 1-2, (modern) number theory was born first around 1630 by Fermat and then reborn in 1730 by Euler.

and remarks that we must have $n \neq 4k+3$; cf. [Di], II, p. 225, [We], p. 30. (He himself considers the case $n = 13$.) This led readers of Diophantus study the following problem.

Problem A. *When can a given number n be written as a sum of two squares?*

This problem was studied by a number of people during the middle ages and some solutions (often incorrect) were proposed (cf. [Di], II, p. 225-7). However, the correct answer only found in 1625 by Girard (but without proof).

Because of the identity

$$(x^2+y^2)(z^2+t^2) = (xz-yt)^2 + (xt+yz)^2, \tag{1.2}$$

which was probably known to Diophantus (cf. [We], p. 11) but which was first written down explictly by Fibonacci (1225) (cf. [Di] II, p. 226), one can reduce Problem A to case that n is a prime number. Fermat proved in 1640 the following result ([We], p. 67):

Theorem 1.1 (Fermat) *If p is a prime, then*

$$p = x^2 + y^2 \text{ with } x, y, \in \mathbb{Z} \quad \Leftrightarrow \quad p \equiv 1 \pmod 4 \text{ or } p = 2.$$

He did not write down a proof of this result, but mentioned in a letter that he proved it by his "method of infinite descent". Such a proof was found by Euler around 1745: if $p \equiv 1 \pmod 4$, then

1) There exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 \equiv 0 \pmod p$, so $x^2 + y^2 = mp$ for some $m \in \mathbb{Z}$;

2) If $x^2 + y^2 = mp$ for some $m > 1$, then there are $x_1, y_1, m_1 \in \mathbb{Z}$ with $1 \leq m_1 < m$ such that $x_1^2 + y_1^2 = m_1 p$. ("Method of descent")

It is clear that Fermat's theorem follows from these two steps. We shall later see in §1.3.4 how to prove this result by a related but slightly different method.

Throughout his life, Euler studied the following generalization of the above problem and/or Fermat's theorem (cf. [We], p. 204):

Problem B. *Given a number $N \neq 0$, when does the equation*

$$x^2 + Ny^2 = p, \quad p \text{ a prime},$$

have a solution (in integers)? Can these primes p be described by congruence conditions on p?

Euler solved this problem (positively) for $N = 1, \pm 2, 3$,[2] and obtained some partial results for other N's. For example, he observed:

$$x^2 + Ny^2 = p,\ p \nmid 2N \ \Rightarrow \begin{cases} x^2 \equiv -N \pmod p & \text{has a solution} \\ x^2 \equiv p \pmod N & \text{has a solution} \end{cases}$$

[2] In fact, the cases $N = 1, 2, 3$ were already done by Fermat; cf. [We], p. 205.

and for a while thought that the converse of the second implication might be true ([We], p. 214). However, this is already false for $N = 5, 6$ as he later realized, and so he was very far from establishing a general theory of such equations.

In 1773 Lagrange was able to greatly clarify the piecemeal results of Euler. The main idea of Lagrange was that one should not only study a fixed form such as $x^2 + Ny^2$, but also certain "related" binary quadratic forms $ax^2 + bxy + cy^2$. More precisely, he proved

Theorem 1.2 (Lagrange) *If $-N$ is not a square, then there is an (explicitly computable) finite list of binary quadratic forms*

$$f_1(x, y) = x^2 + Ny^2,\ f_2(x, y),\ \ldots,\ f_h(x, y)$$

such that for every prime number $p \nmid 2N$ we have:

$f_k(x, y) = p$ has a solution for some k, $1 \leq k \leq h$, $\Leftrightarrow$ $x^2 \equiv -N \pmod{p}$ has a solution.

From this theorem the aforementioned results of Fermat and Euler follow (almost) immediately because one has $h = 1$ when $N = 1, \pm 2, 3$. On the other hand, for $N = 5, 6$ we have $h > 1$, so this explains why Euler's "converse" failed in those cases.

Note that the above congruence condition $x^2 \equiv -N \pmod{p}$ is not *a priori* a congruence condition on p, so further work is necessary to analyze this condition. It turns out, however, that by the famous *Law of Quadratic Reciprocity* [3] this condition can be rewritten as a list of congruences mod $4N$, and so Theorem 2 does give a partial resolution of Problem 2.

Lagrange's theory was further refined and developed by Legendre (1785) and particularly by Gauss (1801), who introduced the theory of genera and the composition of forms. Later Dirichlet (around 1850) and Dedekind (1860) further simplified and generalized the theory and embedded it in a general theory of algebraic number fields.

1.2 Basic Concepts

As was already mentioned in §1.1, an (integral) *binary quadratic form* is a polynomial $f(x, y)$ of the form

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

We shall usually abbreviate this formula by writing

$$f = [a, b, c].$$

Definition. The form $f = [a, b, c]$ is said to *represent* an integer n if there exist $x, y \in \mathbb{Z}$ such that $f(x, y) = n$. If, in addition, x and y can be chosen such that $\gcd(x, y) = 1$, then we say that f *primitively represents* the integer n.

[3] This law was discovered by Euler in 1772 and was published in 1783 ([We], p. 187), and Legendre attempted to give a proof of it in 1785. Gauss (1801) gave the first correct proof and, in fact, gave 8 different proofs of it.

Example 1.1 (a) If $f = [a, b, c]$, then $a = f(1, 0)$, $c = f(0, 1)$ and $a \pm b + c = f(1, \pm 1)$ are primitively represented by f.

(b) If $n = f(x, y)$ is represented by f and if $g = \gcd(x, y)$, then $\frac{n}{g^2} = f(\frac{x}{g}, \frac{y}{g})$ is primitively represented by f. In particular, if $n = p$ is a prime number, then f represents p if and only if f represents p primitively.

From the discussion in §1.1 we see that a natural (but extremely difficult) question about binary quadratic forms is the following.

Problem 1.1 *For a given form $f = [a, b, c]$, determine (or describe) the set*

$$R(f) := \{f(x, y) : x, y \in \mathbb{Z}, \gcd(x, y) = 1\}$$

of integers which are primitively represented by f.

As was explained in §1.1, this problem does not have a satisfactory answer except in special cases. Two related but easier questions are the following.

Problem 1.2 *For a given form $f = [a, b, c]$ and integer n, determine the set $S(f, n) = \{(x, y) : f(x, y) = n\}$ of all integer solutions of the equation*

$$f(x, y) = n. \tag{1.3}$$

Alternately, determine the set $P(f, n) = \{(x, y) \in S(f, n) : \gcd(x, y) = 1\}$ of all primitive *solutions of this equation.*

Problem 1.3 *For a given form $f = [a, b, c]$, determine its* minimum

$$\min(f) := \min\{|f(x, y)| : x, y \in \mathbb{Z}, (x, y) \neq (0, 0)\} = \min\{|n| : n \in R(f)\}.$$

As we shall see, the nature (and method) of the solutions of these problems depends heavily on whether the form is *definite* or *indefinite*.

Definition. A form $f = [a, b, c]$ is called *positive definite* (notation: $f > 0$) if we have

$$f(x, y) > 0, \quad \text{for all } x, y \in \mathbb{R},\ (x, y) \neq (0, 0),$$

and is called *negative definite* if $-f$ is positive definite. It is called *indefinite* if f takes on both positive and negative values.

Remark. In view of their applications to part II of this course, we shall be mainly interested in positive definite binary quadratic forms. However, whenever convenient, we shall discuss both types of forms.

Whether or not $f = [a, b, c]$ is definite or indefinite can be determined by the sign of its *discriminant*

$$\Delta(f) = b^2 - 4ac, \tag{1.4}$$

as the following result shows:

Proposition 1.1 *If $f = [a, b, c]$, then we have*

$$4af(x, y) = (2ax + by)^2 - \Delta(f)y^2 \quad \textit{and} \quad 4cf(x, y) = (2ay + bx)^2 - \Delta(f)x^2. \tag{1.5}$$

Thus

$$f \textit{ is positive definite} \iff \Delta(f) < 0 \textit{ and } a > 0 \tag{1.6}$$

$$f \textit{ is indefinite} \iff \Delta(f) > 0. \tag{1.7}$$

Proof. The identities (1.5) are easily verified by expanding the right hand sides. From this, assertion (1.6) follows readily. Indeed, if $a > 0$ and $\Delta(f) < 0$, then (1.5) shows that $f > 0$. Conversely, if $f > 0$, then $a = f(1, 0) > 0$ and $-a^2\Delta(f) = af(b, -2a) > 0$, so $\Delta(f) < 0$.

Similarly, we can prove assertion (1.7). Suppose first that $\Delta(f) > 0$. If $a \neq 0$, then (1.5) shows that $f(1, 0)f(b, -2a) = -\Delta(f)a^2 < 0$, so f is indefinite. If $c \neq 0$, then $f(0, 1)f(-2c, b) = -\Delta(f)c^2 < 0$, so again f is indefinite. Finally, if $a = c = 0$, then $f(x, y) = bxy$ with $b \neq 0$ (because $\Delta(f) = b^2 \neq 0$), so f is clearly indefinite.

Conversely, suppose f is indefinite. If $a = 0$, then necessarily $b \neq 0$ for otherwise $f(x, y) = cy^2$ which isn't indefinite. Thus, $\Delta(f) = b^2 > 0$ in this case. Thus, we may assume that $a \neq 0$, and then (1.5) shows that $\Delta(f) \neq 0$ for otherwise f is not indefinite. Now if $a > 0$, then it follows from (1.6) that $\Delta(f) > 0$, and if $a < 0$, then the same argument applied to $-f$ shows that $\Delta(f) = \Delta(-f) > 0$.

Example 1.2 The form $f(x, y) = x^2 + Ny^2$ has discriminant $-4N$ and hence is positive definite if $N > 0$ and is indefinite if $N < 0$.

Corollary 1.2 *If $f = [a, b, c]$ is positive definite with discriminant $\Delta(f) = -D$, then*

$$f(x, y) = n \quad \Rightarrow \quad |x| \leq \sqrt{\frac{4cn}{D}},\ |y| \leq \sqrt{\frac{4an}{D}},$$

and so the equation $f(x, y) = n$ has at most finitely many integer solutions.

Proof. By (1.6) we know $a > 0, D > 0$ and hence also $c > 0$. By (1.5) we have $Dy^2 \leq (2ax + by)^2 + Dy^2 = 4an$, and so $|y| \leq \sqrt{4an/D}$, and the other bound is proved similarly.

Remark 1.1 (a) Note that this corollary gives an "algorithm" for solving Problem 2 when f is positive definite: for each of the finitely many pairs (x, y) satisfying the above bounds we test whether or not $f(x, y) = n$. However, the solution of the indefinite case is much harder since this equation may have infinitely many solutions.

(b) Since $\Delta(f) = b^2 - 4ac \equiv b^2 \pmod 4$, we see that $\Delta(f) \equiv 0$ or $1 \pmod 4$. Conversely, if $\Delta \equiv 0$ or $1 \pmod 4$, then there is a form $f = 1_\Delta$ of discriminant $D(f) = \Delta$:

$$1_\Delta = \begin{cases} [1, 0, -\frac{\Delta}{4}] & \text{if } \Delta \equiv 0 \pmod 4 \\ [1, 1, \frac{1-\Delta}{4}] & \text{if } \Delta \equiv 1 \pmod 4; \end{cases}$$

this form is called the *principal form* of discriminant Δ.

(c) If $\Delta(f) = 0$ or $\Delta(f) = d^2$ is a square, then one can show that f is a product of linear forms; cf. [BV], p. 16. We shall usually exclude this case from our study.

Definition. The *content* of a form $f = [a, b, c]$ is $\mathrm{cont}(f) = \gcd(a, b, c)$. Forms with content $\mathrm{cont}(f) = 1$ are called *primitive forms*.

Remark 1.2 (a) The content of a form can be defined more intrinsically by the formula

$$\mathrm{cont}(f) = \gcd(R(f)) := \gcd\{n : n \in R(f)\}.$$

Indeed, since $\mathrm{cont}(f) | f(x, y)$, for all $x, y \in \mathbb{Z}$, we see that $\mathrm{cont}(f) | \gcd(R(f))$. On the other hand, since $a, c, a + b + c \in R(f)$, we have $\gcd(R(f)) | \gcd(a, c, a + b + c) = \mathrm{cont}(f)$, and so equality holds.

(b) If $c = \mathrm{cont}(f)$, then f/c is a primitive form of discriminant $\Delta(f/c) = \Delta(f)/c^2$. Since $R(f) = cR(f/c)$, we can usually restrict attention to primitive forms. Note that if

$$\tilde{Q}_\Delta = \{[a, b, c] \in \mathbb{Z}^3 : b^2 - 4ac = \Delta, \gcd(a, b, c) = 1\}$$

denotes the set of primitive forms of discriminant Δ, then $n\tilde{Q}_{\Delta/n^2}$ is the set of forms of discriminant Δ and content n, and hence

$$Q^*_\Delta = \dot{\bigcup_{n^2|\Delta}} n\tilde{Q}_{\Delta/n^2}$$

is the set of all forms of discriminant Δ.

If $\Delta < 0$, then a similar result holds for the set positive definite forms (in place of all forms). Since in this case we shall be only interested in such forms, we put

$$Q_\Delta = \{f \in \tilde{Q}_\Delta : f > 0\}, \text{ if } \Delta < 0, \quad \text{and} \quad Q_\Delta = \tilde{Q}_\Delta, \text{ if } \Delta > 0.$$

1.3 Lagrange's Method: Equivalence and Reduction

We now turn to the method of Lagrange (1773) which is based on two key concepts: the equivalence and reduction of forms.

1.3.1 Equivalence

The following simple observation of Lagrange turns out to be an extremely powerful tool in the study of quadratic forms:

Observation 1.1 *If we make a (suitable) change of variables in $f(x, y)$, then the result is another binary quadratic form $f_1(x, y)$ which represents the same numbers as f, i.e. $R(f_1) = R(f)$.*

To study such changes of variables, it is useful to use the *matrix representation* of quadratic forms. For this, we view the elements of $\mathbb{Z}^2$ as column vectors $\vec{x} = \binom{x_1}{x_2} \in \mathbb{Z}^2$; then we can write the binary quadratic form $f = [a, b, c]$ in the form

$$f(\vec{x}) = f(x_1, x_2) = \tfrac{1}{2}\vec{x}^t A(f)\vec{x}, \quad \text{where } A(f) := \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}. \tag{1.8}$$

Conversely, if $A \in M_2(\mathbb{Z})$ is an integral symmetric 2×2 matrix with even diagonal entries, then the rule

$$f_A(\vec{x}) = \tfrac{1}{2}\vec{x}^t A\vec{x} \tag{1.9}$$

defines an (integral) binary quadratic form f_A such that $A(f_A) = A$. Thus, there is a complete dictionary between forms and matrices. [4] Note also that we have

$$\Delta(f) = -\det(A(f)). \tag{1.10}$$

Now if $T \in M_2(\mathbb{Z})$, then the *transform* fT of the form f by T is defined by $(fT)(\vec{x}) = f(T\vec{x})$. Since by (1.8)

$$f(T\vec{x}) = \tfrac{1}{2}(T\vec{x})^t A(f)(T\vec{x}) = \tfrac{1}{2}\vec{x}^t(T^t A(f)T)\vec{x} = f_{T^t A(f)T}(\vec{x}),$$

we see that fT is again an (integral) binary quadratic form with associated matrix

$$A(fT) = T^t A(f)T. \tag{1.11}$$

In particular, we see from this and (1.10) that its discriminant is

$$\Delta(fT) = \Delta(f)\det(T)^2. \tag{1.12}$$

For later use, let us write down fT more explicitly. Now if

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\vec{v}_1|\vec{v}_2),$$

where $\vec{v}_1 = T\binom{1}{0}$ and $\vec{v}_1 = T\binom{0}{1}$ represent the column vectors of T, then we have

$$\begin{aligned} (fT)(x,y) &= f\left(T\tbinom{x}{y}\right) = f(ax+by, cx+dy) \\ &= f(\vec{v}_1)x^2 + (\vec{v}_1^t A(f)\vec{v}_2)xy = f(\vec{v}_2)y^2, \end{aligned} \tag{1.13}$$

i.e. $fT = [f(\vec{v}_1), \vec{v}_1^t A(f)\vec{v}_2, f(\vec{v}_2)]$. (To see why the last formula is true, write $fT = [\alpha, \beta, \gamma]$ and $\vec{e}_1 = (1,0)^t$, $\vec{e}_2 = (0,1)^t$. Then

$$\alpha = \tfrac{1}{2}\vec{e}_1^t A(fT)\vec{e}_1 = \tfrac{1}{2}\vec{e}_1^t T^t A(f)T\vec{e}_1 = f(T\vec{e}_1) = f(\vec{v}_1),$$

and $\beta = \vec{e}_1^t A(fT)\vec{e}_2$ and $\gamma = \frac{1}{2}\vec{e}_2^t A(fT)\vec{e}_2$ are computed similarly.)

[4] In some books such as [Bu] or [BV] the matrix associated to f is defined as $\frac{1}{2}A(f)$.

Example 1.3 Let $f = [a, b, c]$. Then

$$f\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = [c, -b, a],\ f\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = [a, b{+}2at, at^2{+}bt{+}c],\ f\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = [a, -b, c].$$

We now restrict our attention to matrices $T \in \mathrm{GL}_2(\mathbb{Z}) = M_2(\mathbb{Z})^\times$, (i.e. to integral matrices $T \in M_2(\mathbb{Z})$ with $\det(T) = \pm 1$), and/or to matrices $T \in \mathrm{SL}_2(\mathbb{Z})$. To cover both these cases it is useful to introduce the following definition.

Definition. Let $G \leq \mathrm{GL}_2(\mathbb{Z})$ be a subgroup. We say that two forms f_1, f_2 are *G-equivalent* if we have $f_2 = f_1 T$, for some $T \in G$. If this the case, then we write $f_1 \sim_G f_2$.

If two forms f_1, f_2 are $\mathrm{SL}_2(\mathbb{Z})$-equivalent, then say that f_1 and f_2 are *properly equivalent* and write $f_1 \sim f_2$. Moreover, $\mathrm{GL}_2(\mathbb{Z})$-equivalence is denoted by $f_1 \approx f_2$.

Remark 1.3 (a) From (1.11) we see that we have

$$f(T_1T_2) = (fT_1)T_2, \quad \text{for all } T_1, T_2 \in M_2(\mathbb{Z}), \tag{1.14}$$

and so it follows that the rule $(f, T) \mapsto fT$ defines a *right* action of the group $G \leq \mathrm{GL}_2(\mathbb{Z})$ on the set of quadratic forms. In particular, the relation $\sim_G$ is an equivalence relation on this set.

(b) Since $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \cup \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$, we see that

$$f_1 \approx f_2 \ \Leftrightarrow\ f_1 \sim f_2 \text{ or } f_1 \sim f_2 \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right).$$

In other words, $f_1 \approx [a, b, c] \Leftrightarrow f_1 \sim [a, b, c]$ or $f_1 \sim [a, -b, c]$; cf. Example 1.3.

(c) The above definition of $\mathrm{GL}_2(\mathbb{Z})$-equivalence is the one that is found in all the literature starting from Gauss (see also Jones, Watson, O'Meara, etc.) except for [BV], p. 23, where a different definition is introduced for this concept.

The above equivalence relations preserve many of the properties of quadratic forms.

Proposition 1.3 *If $T \in \mathrm{GL}_2(\mathbb{Z})$, then for any form f and integer $n \in \mathbb{Z}$ we have*

$$T(S(fT, n)) = S(f, n) \quad \textit{and} \quad T(P(fT, n)) = P(f, n). \tag{1.15}$$

Thus, if $f_1 \approx f_2$, then

$$R(f_1) = R(f_2),\ \mathrm{cont}(f_1) = \mathrm{cont}(f_2),\ \min(f_1) = \min(f_2) \textit{ and } \Delta(f_1) = \Delta(f_2). \tag{1.16}$$

Moreover, f_1 is positive definite (respectively, indefinite) if and only if f_2 has this property.

Proof. Since T is a bijection of $\mathbb{Z}^2$, we have $\vec{x} \in T(S(fT,n)) \Leftrightarrow T^{-1}\vec{x} \in S(fT,n) \Leftrightarrow (fT)(T^{-1}\vec{x}) = n \Leftrightarrow f(TT^{-1}\vec{x}) = n \Leftrightarrow \vec{x} \in S(f,n)$, which proves the first equality of (1.15). From this, the second follows because we have

$$\vec{x} \text{ is primitive} \quad \Leftrightarrow \quad T\vec{x} \text{ is primitive.}$$

Next, if $f_1 \approx f_2$, then $f_2 = f_1 T$ for some $T \in \mathrm{GL}_2(\mathbb{Z})$. Thus, by (1.15) we have $\#P(f_1,n) = \#P(f_2,n)$, for all $n \in \mathbb{Z}$, and so $R(f_1) = R(f_2)$ because $R(f_i) = \{n \in \mathbb{Z} : P(f_i,n) \neq \emptyset\}$. This proves the first equality of (1.16), and from this the second and third follow in view of Remark 1.2(a) and the defining formula of $\min(f_i)$ (cf. Problem 1.3). Finally, the last equation follows from (1.12) because here $\det(T) = \pm 1$.

Remark 1.4 There are many other "invariants" that can be attached to forms, i.e. numbers attached to forms that are the same for every form in each GL_2-equivalence class. For example, since $T \in \mathrm{GL}_2(\mathbb{Z})$ permutes the $\mathbb{Z}$-bases of $\mathbb{Z}^2$, we see that

$$\min_b(f) = \min\{\max(|f(\vec{v}_1)|, |f(\vec{v}_2)|) : (\vec{v}_1, \vec{v}_2) \text{ is a } \mathbb{Z}\text{-basis of } \mathbb{Z}^2\}$$

is such an invariant, i.e. $f_1 \approx f_2 \Rightarrow \min_b(f_1) = \min_b(f_2)$.

Similarly, the orders of the groups

$$\mathrm{Aut}(f) = \{T \in \mathrm{GL}_2(\mathbb{Z}) : fT = f\} \quad \text{and} \quad \mathrm{Aut}^+(f) = \mathrm{Aut}(f) \cap \mathrm{SL}_2(\mathbb{Z})$$

are invariants because for any $T \in \mathrm{GL}_2(\mathbb{Z})$ we have

$$\mathrm{Aut}(fT) = T^{-1}\mathrm{Aut}(f)T \quad \text{and} \quad \mathrm{Aut}^+(fT) = T^{-1}\mathrm{Aut}^+(f)T. \tag{1.17}$$

(Indeed, if $T_1 \in \mathrm{GL}_2(\mathbb{Z})$, then $T_1 \in \mathrm{Aut}(fT) \Leftrightarrow fTT_1 = fT \Leftrightarrow fTT_1T^{-1} = f \Leftrightarrow TT_1T^{-1} \in \mathrm{Aut}(f) \Leftrightarrow T_1 \in T^{-1}\mathrm{Aut}(f)T$, which proves the first equality of (1.17). From this the second follows since $T^{-1}\mathrm{SL}_2(\mathbb{Z})T = \mathrm{SL}_2(\mathbb{Z})$.)

The elements of $\mathrm{Aut}(f)$ are called *automorphs*. Note that we have always have $\pm I \in \mathrm{Aut}^+(f)$. If f is positive-definite, then we shall see below that $\mathrm{Aut}^+(f) = \{\pm I\}$ for most f's. On the other hand, if f is indefinite, then $\mathrm{Aut}^+(f)$ is always an infinite group, but this is harder to see; cf. Fact 1.23 below.

Corollary 1.4 *The group* $\mathrm{Aut}^+(f)$ *acts fixed-point-free on the sets* $P(f,n)$ *and* $S(f,n)$ *(when* $n \neq 0$*). Thus* $\mathrm{Aut}^+(f)$ *is finite if* f *is positive definite. Moreover, if* $\mathrm{Aut}^+(f)$ *is infinite, then* $P(f,n)$ *and* $S(f,n)$ *are infinite whenever they are non-empty.*

Proof. By (1.15) we see that $\mathrm{Aut}^+(f)$ (and $\mathrm{Aut}(f)$) act on $P(f,n)$ and on $S(f,n)$. To show that $\mathrm{Aut}(f)$ acts fixed-point-free, assume the contrary. Thus, there exists $T \in \mathrm{Aut}^+(f)$, $T \neq I$ and $\vec{x} \neq \vec{0}$ such that $T\vec{x} = \vec{x}$. Then 1 is an eigenvalue of T and so its characteristic polynomial factors as $\mathrm{ch}_T(x) = (x-1)(x-\lambda)$. Since $1 = \det(T) = 1 \cdot \lambda$, we thus have $\mathrm{ch}_T(x) = (x-1)^2$. Now if T were diagonable, then $T = P^{-1}IP$ for some

$P \in \mathrm{GL}_2(\mathbb{Q})$, and then $T = I$, contradiction. Thus $T = P^{-1}\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)P$, so $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{Aut}(fP^{-1})$ by (1.17). Write $fP^{-1} = [a, b, c]$ with $a, b, c \in \mathbb{Q}$. Then by Example 1.3 we see that we have $b = b + 2a$ and $c = a + b + c$, so $a = b = 0$. This forces $\Delta(f) = 0$, which is not permissible. This proves that $\mathrm{Aut}^+(f)$ acts fixed-point-free.

Now if $f > 0$, then by Corollary 1.2 we know that $P(f, n)$ is finite and non-empty, if $n \in R(f)$, and so the $\mathrm{Aut}^+(f)$-orbit of each point is also finite. Since the stabilizer of $\mathrm{Aut}^+(f)$ is trivial, it follows that $\mathrm{Aut}^+(f)$ is finite. The last assertion is proven similarly.

Before going on, let us note in passing that the forms $f = [a, b, c]$ for which $\mathrm{Aut}(f) \neq \mathrm{Aut}^+(f)$ can be characterized by the property that $f \sim [a, -b, c]$; such forms are called (after Gauss) *ambiguous*.

Proposition 1.5 *We have* $\mathrm{Aut}(f) \neq \mathrm{Aut}^+(f)$ *if and only if* f *is ambiguous. If this is the case, then* $[\mathrm{Aut}(f) : \mathrm{Aut}^+(f)] = 2$*, and every* $f_1 \sim f$ *is ambiguous.*

Proof. We have $\mathrm{Aut}(f) \neq \mathrm{Aut}^+(f) \Leftrightarrow \exists T \in \mathrm{Aut}(f)$ with $\det(T) = -1 \Leftrightarrow \exists T_1 \in \mathrm{SL}_2(\mathbb{Z})$ such that $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)T_1 \in \mathrm{Aut}(f) \Leftrightarrow \exists T_1 \in \mathrm{SL}_2(\mathbb{Z})$ such that $f = f\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)T_1 \Leftrightarrow f \sim f\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. This proves the first statement because $[a, b, c]\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = [a, -b, c]$; cf. Example 1.3. The second follows immediately from the fact that $[\mathrm{GL}_2(\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z})] = 2$, and the last follows since the property $\mathrm{Aut}(f) \neq \mathrm{Aut}^+(f)$ is an invariant of the equivalence class of f; cf. equation (1.17).

As we shall see, the following simple observation is an extremely useful fact.

Proposition 1.6 *If* f *is a binary quadratic form and* $n \in \mathbb{Z}$*,* $n \neq 0$*, then*

$$n \in R(f) \quad \Leftrightarrow \quad f \sim [n, b, c], \quad \textit{for some } b, c \in \mathbb{Z}. \tag{1.18}$$

Proof. If $f \sim f' := [n, b, c]$, then $n = f'(1, 0) \in R(f')$ and so by (1.16) we have $n \in R(f) = R(f')$.

Conversely, suppose $n \in R(f)$., i.e. $n = f(x, y)$ for some $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$. By the extended Euclidean algorithm there exist $z, w \in \mathbb{Z}$ such that $xw - yz = 1$, and so $T = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $f \sim fT$, and by (1.13) we have $fT = [n, b, c]$ with $b, c \in \mathbb{Z}$.

Corollary 1.7 *If* $n \in R(f)$*,* $n \neq 0$*, then there is an integer* x *such that*

$$x^2 \equiv \Delta(f) \pmod{4n}. \tag{1.19}$$

Proof. By Proposition 1.6 we know that $f \sim f' = [n, b, c]$, for some $b, x \in \mathbb{Z}$. Then by (1.16) we have $\Delta(f) = D(f') = b^2 - 4nc \equiv b^2 \pmod{4n}$, so (1.19) holds with $x = b$.

As was mentioned above, Euler tried to prove the converse of this statement and later realized that the converse cannot hold in general. Lagrange, however, noticed that the following partial converse is true:

Proposition 1.8 *Suppose that n and Δ are non-zero integers such that the congruence*

$$x^2 \equiv \Delta \pmod{4n}. \tag{1.20}$$

has an integer solution. Then there is a form f with

$$\Delta(f) = \Delta \quad \textit{and} \quad n \in R(f). \tag{1.21}$$

Moreover, if $\gcd(n, \Delta) = 1$, then f can be chosen to be primitive.

Proof. By hypothesis, $x^2 - \Delta = 4nk$ for some $k \in \mathbb{Z}$, and so $f = [n, x, k]$ satisfies (1.21). Note that if $\gcd(n, \Delta) = 1$ then f is primitive because $\mathrm{cont}(f) | \gcd(n, \Delta(f))$.

Corollary 1.9 *If n and Δ are non-zero integers, then the following conditions are equivalent:*

(i) $n \in \bigcup_{\Delta(f)=\Delta} R(f)$

(ii) $x^2 \equiv \Delta \pmod{4n}$ *has a integer solution* $x \in \mathbb{Z}$.

Proof. Combine Corollary 1.7 with Proposition 1.8.

Note that this corollary constitutes a major step towards Theorem 1.2. What is still missing, however, is the fact that we only have to consider finitely many forms in Corollary 1.9(i) and that these can be computed explicitly. This will be done next.

1.3.2 Reduction

Lagrange's second observation, which is much more subtle than the first, is the following:

Observation 1.2 *Each proper equivalence class of forms contains a unique "simplest" representative. Moreover, there are only finitely many proper equivalence classes of forms of given discriminant Δ.*

These "simplest representatives" are the forms which satisfy certain inequalities on their coefficients; such forms are called *reduced*. Since the definition of such forms is different for positive definite and for indefinite forms, we consider these two cases separately. We begin with the positive-definite case.

Definition. A positive-definite form $f = [a, b, c] > 0$ is called *semi-reduced* if

$$|b| \leq a \leq c. \tag{1.22}$$

Moreover, f is called *reduced* if it semi-reduced and if we have in addition that

$$b \neq -a \quad \text{and} \quad b \geq 0 \text{ when } a = c. \tag{1.23}$$

Example 1.4 The principal form $1_\Delta = [1, \varepsilon, \frac{\varepsilon-\Delta}{4}]$ of discriminant $\Delta < 0$ is reduced. Here $\varepsilon = 0$ or 1 and $\varepsilon \equiv \Delta \pmod 4$.

Proposition 1.10 *If $f = [a, b, c] > 0$ is a semi-reduced form of discriminant $\Delta(f) = -D < 0$, then*

$$|b| \le a \le \sqrt{\frac{D}{3}} \quad \text{and} \quad c \le \frac{D}{3a} \le \frac{D}{3}. \tag{1.24}$$

In particular, there are only finitely many reduced forms of fixed discriminant $\Delta < 0$.

Proof. The first inequality is clear by (1.22). For the second we observe that by (1.22) we have $D = 4ac - b^2 \ge 4a^2 - b^2 \ge 4a^2 - a^2 = 3a^2$, so $3a^2 \le D/3$ or $a \le \sqrt{D/3}$. Finally, since $4ac = D + b^2 \le D + a^2 \le D + \frac{D}{3} = \frac{4}{3}D$, we have $c \le \frac{D}{3a} \le \frac{D}{3}$, as claimed.

Notation. For $\Delta < 0$ let

$$h(\Delta) = \#\{\text{reduced primitive forms } f \text{ with } \Delta(f) = \Delta\}.$$

Corollary 1.11 *If $0 < D \le 12$, then $h(-D) = 1$.*

Proof. Let $f = [a, b, c]$ be reduced and primitive with $\Delta(f) = -D$. Then by (1.24) we have $a \le \sqrt{D/3} \le \sqrt{\frac{12}{3}} = 2$. Assume first that $D \le 11$. Then $a < 2$, so $a = 1$. Thus $|b| \le 1$. Note that $b \equiv D \pmod 2$. Thus, if $\Delta \equiv 0(4)$, then $b = 0$ and so $f = [1, 0, \frac{D}{4}] = 1_{-D}$, and if $\Delta \equiv 1(4)$, then $b = 1$ (because $b = -1 = -a$ is forbidden by (1.23)), and so $f = [1, 1, \frac{1+D}{4}] = 1_{-D}$. Thus, $f = 1_{-D}$ in both cases, and hence $h(-D) = 1$ when $D \le 11$.

Now suppose that $D = 12$, so $a \le 2$. If $a = 1$, then one concludes as before that $f = 1_{-D}$, so assume $a = 2$. Then $|b| \le a = 2$, so $b = 0$ or 2 (because $b = -2 = -a$ is forbidden by (1.23)). But if $b = 0$, then $-12 = \Delta(f) = 0^2 - 4(2)c$, which is impossible. Thus, $b = 2$, and then $c = (b^2 + D)/(4a) = 2$. But then $f = [2, 2, 2]$, which is not primitive. Thus $f = 1_{-12} = [1, 0, 3]$ is the only reduced primitive form of discriminant -12, and so $h(-12) = 1$.

Example 1.5 For the next discriminant $D = -15$ we have $h(-15) = 2$.
Indeed, if $f = [a, b, c]$ is reduced and primitive of discriminant -15, then $a \le \sqrt{15/3} < 3$, so $a = 2$. If $a = 1$, then as in the above proof we have $f = 1_{-15} = [1, 1, 4]$. Thus, assume $a = 2$. Then $b = \pm 1$, and hence $c = (b^2 + D)/(4a) = 2$. But $[2, -1, 2]$ is not reduced, so $[1, 1, 4]$ and $[2, 1, 2]$ are the only reduced forms with $\Delta(f) = -15$, and hence $h(-15) = 2$.

Remark 1.5 It is clear that the inequalities (1.22) and (1.23) (together with (1.24)) yield an explicit algorithm for finding all reduced (primitive) forms of a given discriminant, and hence for computing $h(-D)$, as we saw in Corollary 1.11 and Example 1.5.

By using the following variant, we can speed up this (naive) algorithm as follows (provided we have an efficient factoring algorithm):

1) For $b = 0, 1, \ldots, \left[\sqrt{D/3}\right]$ with $b \equiv D \pmod 2$, find all factorizations of $(b^2+D)/4 = ac$ with $b \le a \le c$.

2) For each such tuple as above, $[a, \pm b, c]$ is a semi-reduced form of discriminant $-D$. By discarding forms which are not reduced or not primitive, we obtain the desired list of all reduced primitive forms of discriminant $-D$.

We now come to the main result about reduced positive definite forms:

Theorem 1.3 (Lagrange) *Each form $f > 0$ is properly equivalent to a unique reduced form, and hence*

$$h(\Delta) \;=\; \#(Q_\Delta/\mathrm{SL}_2(\mathbb{Z})) \tag{1.25}$$

is the number of proper equivalence classes of primitive, positive definite forms of discriminant Δ.

Before proving this theorem, let us observe that Theorem 1.2 (for $N > 0$) is an immediate consequence of it (together with what we have proved so far).

Proof of Theorem 1.2 *when* $N > 0$: Let $f_1 = [1, 0, N], f_2, \ldots, f_H$ be the reduced forms of discriminant $-4N$. Note that by (1.24) and/or Remark 1.5 we know that there are only finitely many such forms and that these can be computed explicitly (for a given $N > 0$). By Theorem 1.3 we know that for each $f > 0$ with $\Delta(f) = -4N$ there is a k with $1 \le k \le H$ such that $f \sim f_k$, and so by (1.16) we have

$$\bigcup_{\Delta(f)=-4N} R(f) \;=\; \bigcup_{k=1}^{H} R(f_k).$$

From this is clear that Theorem 1.2 follows from Corollary 1.9 (when $N > 0$).

We now turn to the proof of Theorem 1.3. This will be done in two parts. In the first part we give an algorithm which constructs for a given form f a reduced form $r(f) \sim f$, and in the second part we show that $r(f)$ is uniquely characterized by its properties.

To state the reduction algorithm in a convenient form, we first introduce the following notation.

Notation. If $f = [a, b, c] > 0$, then put

$$\nu(f) \;=\; f\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad \text{where } t = \left[\frac{a-b}{2a}\right], \tag{1.26}$$

$$\rho(f) \;=\; f\begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix}, \quad \text{where } s = \left[\frac{b+c}{2c}\right]. \tag{1.27}$$

Lemma 1.1 *If $f = [a, b, c]$ and $\nu(f) = [a', b', c']$, then*

$$a' = a \quad \textit{and} \quad -a' < b' \le a'. \tag{1.28}$$

Moreover, $\rho(f) = \nu([c, -b, a])$*. Thus, if we write* $\rho(f) = [a'', b'', c'']$*, then*

$$a'' = c \quad \textit{and} \quad -a'' < b'' \leq a''. \tag{1.29}$$

Proof. By Example 1.3 we have $\nu(f) = [a, b + 2at, *]$, so $a' = a$ and $b' = b + 2at$. Now for any $x \in \mathbb{R}$ we have (by definition of $[x]$) that $0 \leq x - [x] < 1$, and hence by replacing x by $x + \frac{1}{2}$ we obtain

$$-\tfrac{1}{2} \leq x - [x + \tfrac{1}{2}] < \tfrac{1}{2}.$$

Taking $x = \frac{-b}{2a}$ and noting that $t = \left[\frac{-b}{2a} + \frac{1}{2}\right]$, we obtain from this (after multiplying through by $-2a$) that $a' = a \leq b + 2at = b'$. Since $b' > -a = -a'$, this proves (1.28).

Now since $\left(\begin{smallmatrix} 0 & -1 \\ a & s \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & s \\ 0 & 1 \end{smallmatrix}\right)$, and since $f\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = [c, -b, a]$, we see that $\rho(f) = \nu([c, -b, a])$. Thus, by applying (1.28) to $[c, -b, a]$ in place of f, we see that (1.29) follows.

We are now ready to present the *reduction algorithm.*

Reduction Algorithm.

Given: A positive definite quadratic form $f = [a, b, c]$.

Result: A reduced form $r(f)$ with $r(f) \sim f$.

Steps: 1. Put $f_0 := \nu(f) = [a_0, b_0, c_0]$. If $a_0 \leq c_0$, go to step 4, otherwise to step 2.

2. If $a_{i-1} > c_{i-1}$, put $f_i := \rho(f_{i-1}) = [a_i, b_i, c_i]$.

3. Repeat step 3 until we obtain $a_k \leq c_k$, then go to step 4.

4. If $a_k \neq c_k$ or if $b_k \geq 0$, then put $r(f) = f_k$, otherwise put $r(f) = f_k\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Proposition 1.12 *The above reduction algorithm computes a reduced form* $r(f)$ *with* $r(f) \sim f$*.*

Proof. We first note that the algorithm stops after a finite number of steps. Indeed, since by (1.29) we have $a_i = c_{i-1} < a_{i-1}$, so we obtain a descending sequence

$$a_0 = a > a_1 > a_2 \ldots > a_k > \ldots \tag{1.30}$$

of positive integers which has to stop eventually (i.e. $k \leq a$).

Next we note that $r(f)$ is reduced. Indeed, in step 4 of the algorithm we have by Lemma 1.1 that $-a_k < b_k \leq a_k \leq c_k$, and so $r(f) = f_k$ is reduced except when $a_k = c_k$ and $b_k < 0$, and in this case and then $r(f) = f_k\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = [a_k, -b_k, a_k]$ is reduced.

Finally, since by construction $f_0 = fT_0$, $f_i = f_{i-1}T_i$ with $T_0, T_i \in \mathrm{SL}_2(\mathbb{Z})$, we see that $f \sim f_0 \sim \ldots f_i \sim f_k \sim r(f)$, and so $f \sim r(f)$.

Remark 1.6 (a) The above algorithm can be modified to find a matrix $T \in \mathrm{SL}_2(\mathbb{Z})$ such that $r(f) = fT$. Indeed, since the matrices $T_0, T_1, \ldots T_k$ mentioned in the above proof are

given explicitly, we can compute $T' = T_0 I_1 \cdots T_k$, and then $T = T'$ (or $T = T' \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, if $a_k = c_k$ and $b_k < 0$).

(b) For later applications it is useful to observe that this reduction algorithm also works for arbitrary *real* positive definite forms, i.e. for forms $f = [a, b, c]$ with $a, b, c \in \mathbb{R}$ (and $a > 0$, $\Delta(f) < 0$). In this case the reduction steps are exactly the same (because the greatest integer function $[x]$ is defined for arbitrary real numbers $x \in \mathbb{R}$). However, it is not clear from the above argument that the algorithm stops after a finite number of steps. Indeed, although we still have the descending sequence (1.30), the a_i's are now real numbers and so the above argument does not suffice. To see that there are only finitely many such a_i's we first observe that since $f_i \sim f$, we have by Proposition 1.3 (which also works in part for real forms) that

$$a_i = f_i(1, 0) \in R(f_i) = R(f) := \{f(x, y) : x, y \in \mathbb{Z}, \gcd(x, y) = 1\}.$$

Now Corollary 1.2 (applied to real positive definite forms) shows that $R(f)$ is a *discrete* set, i.e. $R(f) \cap [0, a]$ is finite for any $a > 0$, and so we see that the algorithm terminates after finitely many steps.

To conclude the proof of Theorem 1.3, we need to show that each proper equivalence class contains at most one reduced form. This, as we shall see, follows from the following fact which is interesting in itself and has many applications, as we shall see.

Proposition 1.13 *If $f = [a, b, c] > 0$ is a semi-reduced form, then*

$$f(x, y) \geq a - |b| + c \geq c, \quad \textit{for all } x, y \in \mathbb{Z} \textit{ with } xy \neq 0, \tag{1.31}$$

and hence we have

$$\min(f) = a \quad \textit{and} \quad \min_b(f) = c. \tag{1.32}$$

.

Proof. Suppose first that $|x| \geq |y| \geq 1$. Then

$$\begin{aligned} f(x, y) &= |x|(a|x| \pm |b||y|) + cy^2 \;\geq\; |x|(a|x| - |b||y|) + cy^2 \\ &\geq |x|(a|y| - |b||y|) + cy^2 \;=\; (a - |b|)|x||y| + cy^2 \;\geq\; a - |b| + c. \end{aligned}$$

Similarly, if $|y| \geq |x| \geq 1$, then

$$\begin{aligned} f(x, y) &= ax^2 + |y|(c|y| \pm |b||x|) \;\geq\; ax^2 + |y|(c|y| - |b||x|) \\ &\geq ax^2 + |y|(c|y| - |b||x|) \;=\; ax^2 + (c - |b|)|x||y| \;\geq\; a + c - |b|, \end{aligned}$$

which proves (1.31). Since we also have

$$f(x, 0) = ax^2 \geq a \quad \text{and} \quad f(0, y) = cy^2 \geq c, \quad \text{if } xy \neq 0, \tag{1.33}$$

it is clear that $\min(f) = a = f(1, 0)$. To prove the last equality, note first that since $\max(f(\pm 1, 0), f(0, \pm 1)) = \max(a, c) = c$, we have $\min_b(f) \leq c$. Now if $\vec{v}_1, \vec{v}_2$ is a basis of $\mathbb{Z}^2$ with (say) $\vec{v}_2 \notin \{(\pm 1, 0), (0, \pm 1)\}$, then $\vec{v}_2 = (x, y)$ with $xy \neq 0$. Thus $\max(f(\vec{v}_1), f(\vec{v}_2)) \geq a - |b| + c \geq c$, and so we have $\min_b(f) = c$.

Remark 1.7 We observe that this result, together with Proposition 1.12, gives a quick algorithm for solving Problem 1.3 (when $f > 0$). Given $f > 0$, apply the reduction algorithm (Proposition 1.12) to compute $r(f) \sim f$. Then $\min(f) = \min(r(f))$ by (1.16), and $\min(r(f))$ is given by (1.32).

Corollary 1.14 *If f is positive definite of discriminant $\Delta(f) = -D$, then*

$$\min(f) \leq \sqrt{\frac{D}{3}}. \tag{1.34}$$

Proof. By the reduction algorithm we have $f \sim r(f) =: [a, b, c]$. Then $\min(f) = \min(r(f)) = a \leq \sqrt{\frac{D}{3}}$, the latter by (1.32) and (1.24).

Corollary 1.15 *If $f = [a, b, c] > 0$ is semi-reduced, then*

$$S(f, a) = P(f, a) = \{(\pm 1, 0)\}, \quad \text{if } a < c, \tag{1.35}$$

$$P(f, c) = \{(0, \pm 1)\}, \quad \text{if } |b| < a < c, \tag{1.36}$$

$$P(f, a) = \{(\pm 1, 0), (0, \pm 1)\}, \quad \text{if } |b| < a = c. \tag{1.37}$$

Proof. From (1.31) and (1.33) we see that $S(f, a) = \{(\pm 1, 0)\}$, and so $S(f, a) = P(f, a)$. This proves (1.35).

Now if $|b| < a$, then $a - |b| + c > c$, and hence if $(x, y) \in P(f, c)$, then $xy = 0$ by (1.31). Thus $(x, y) = (\pm 1, 0)$ or $(0, \pm 1)$, and so (1.36) and (1.37) follow.

We are now ready to prove:

Proposition 1.16 *If f_1 and f_2 are two positive definite reduced forms which are properly equivalent, then $f_1 = f_2$.*

Proof. Write $f_i = [a_i, b_i, c_i]$. By (1.32) we have $a_i = \min(f_i)$ and $c_i = \min_b(f_i)$, so by (1.16) and Remark 1.4 we have $a_1 = a_2$ and $c_1 = c_2$. Moreover, since $\Delta(f_1) = \Delta(f_2)$, it follows that $b_1^2 = b_2^2$. Now if $|b_1| = a_1$, then $b_1 = a_1 = a_2 = b_2$ (cf. (1.23)), so $f_1 = f_2$. Similarly, if $a_1 = c_1$, then $b_i \geq 0$ by (1.23), and so $f_1 = f_2$ here as well.

Thus, assume that $|b_1| < a_1 < c_1$, and let $T = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ be such that $f_2 = f_1 T$. Then $a_1 = a_2 = f(x, y)$, so $(x, y) \in P(f_1, a_1)$, and hence $(x, y) = (\pm 1, 0)$ by (1.35). Similarly, $(z, w) = (0, \pm 1)$ by (1.36), so $T = \pm I$ because $\det(T) = 1$. But then $f_1 T = f_1$, and so $f_2 = f_1 T = f_1$, as claimed.

Proof of Theorem 1.3: Combine Propositions 1.12 and 1.16.

Remark 1.8 The above results show that $f_1 \sim f_2 \Leftrightarrow r(f_1) = r(f_2)$, and so the reduction algorithm can be used to decide whether or not $f_1 \sim f_2$. Moreover, if this is the case, then (the refined version of) the reduction algorithm (cf. Remark 1.6(a)) gives a matrix $T \in \mathrm{SL}_2(\mathbb{Z})$ such that $f_2 = f_1 T$, for we can take $T = T_1 T_2^{-1}$, where T_i is the matrix (computed by (refined) algorithm) such that $r(f_i) = f_i T_i$.

The last two propositions have many other applications. Here are two:

Proposition 1.17 *If $f > 0$ is primitive of discriminant $\Delta(f) \neq -3, -4$, then $\mathrm{Aut}^+(f) = \{\pm I\}$. On the other hand, if $\Delta(f) = -3$, then $|\mathrm{Aut}^+(f)| = 6$ and if $\Delta(f) = -4$, then $|\mathrm{Aut}^+(f)| = 4$.*

Proof. Since $\mathrm{Aut}^+(f)$ acts fixed-point free on $P(f, \min(f))$ by Corollary 1.4, we have

$$|\mathrm{Aut}^+(f)| \leq \#P(f, \min(f)). \tag{1.38}$$

Write $r(f) = [a, b, c]$. If $a \neq c$, then $\#P(f, \min(f)) = 2$ by (1.35), and so $\mathrm{Aut}^+(f) = \{\pm I\}$ because we always have $\pm I \in \mathrm{Aut}^+(f)$.

Thus, assume $a = c$. If $|b| < a$, then by (1.37) and the argument in the proof of Proposition 1.16 we see that $\mathrm{Aut}^+(r(f)) \subset \{\pm I, \pm s\}$, where $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. But if $b \neq 0$, then $r(f)s = [a, -b, a] \neq r(f)$, so $s \notin \mathrm{Aut}^+(r(f))$, and hence $\mathrm{Aut}^+(r(f)) = \{\pm I\} = \mathrm{Aut}^+(f)$ in this case. Thus, assume $b = 0$. Then, we have $r(f) = [1, 0, 1]$ because f is primitive, and so $\Delta(f) = \Delta(r(f)) = -4$. Note that in this case $s \in \mathrm{Aut}^+(r(f))$, so $|\mathrm{Aut}^+(f)| = 4$. Since every f' with $\Delta(f') = -4$ is properly equivalent to $[1, 0, 1]$ by Corollary 1.11 (and Theorem 1.3), the last assertion follows.

Finally, assume that $|b| = a = c$. Then $r(f) = [1, 1, 1]$ because f is primitive, and so $\Delta(f) = -3$. In this case $st = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{Aut}^+(r(f))$, so $|\mathrm{Aut}^+(f)| \geq |st| = 6$. But by (1.38) we have $|\mathrm{Aut}^+(f)| \leq 6$ since $P([1, 1, 1], 1) = \{\pm(1, 0), \pm(0, 1), \pm(1, -1)\}$. From this we deduce as before (using Corollary 1.11) that $|\mathrm{Aut}(f)| = 6$ when $\Delta(f) = -3$.

Proposition 1.18 $\mathrm{SL}_2(\mathbb{Z}) = \left\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle$.

Proof. Let $T \in \mathrm{SL}_2(\mathbb{Z})$ and put $f = f_0 T$, where $f_0 = [1, 0, 2]$ (say). By the reduction algorithm, there exists $T_1 \in \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$ such that $r(f) = fT_1$. Since $f_0 \sim f \sim r(f)$ and f_0 is reduced, we see that $f_0 = r(f)$ by Proposition 1.16. Thus $f_0 = r(f) = fT_1 = f_0 T T_1$, so $TT_1 \in \mathrm{Aut}^+(f_0) = \{\pm I\}$ by Proposition 1.17. Thus $T = \pm T_1^{-1} \in \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$ because $-I = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^2$.

Remark 1.9 Note that the above proof shows that the reduction algorithm can be used to express a given $T \in \mathrm{SL}_2(\mathbb{Z})$ as a *word* $T = s^{m_1} t^{n_1} \cdots s^{m_r} t^{n_r}$ in $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Connection with the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$

There is a close connection between the set

$$\mathcal{P} = \{[a, b, c] \in \mathbb{R}^3 : a > 0,\, b^2 - 4ac < 0\}$$

of all positive-definite *real* binary quadratic forms and the set of points in the upper half-plane

$$\mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\},$$

and this leads to new insight into the concept of reduced forms and/or into the reduction algorithm. This connection is given by the map $\tau : \mathcal{P} \to \mathfrak{H}$ which attaches to $f = [a, b, c] \in \mathcal{P}$ its *principal root*

$$\tau(f) = \frac{-b + \sqrt{\Delta(f)}}{2a} = \frac{-b + i\sqrt{|\Delta(f)|}}{2a}. \tag{1.39}$$

Note that $\tau(f)$ can be characterized by the property that it is the unique root of the polynomial $ax^2 + bx + c$ which lies in $\mathfrak{H}$. In particular, we see that for any $z \in \mathfrak{H}$ we have

$$\tau(f_z) = z, \quad \text{if } f_z := [1, -2\Re(z), |z|^2], \tag{1.40}$$

because $x^2 - 2\Re(z)x + |z|^2 = (x - z)(z - \overline{z})$. Since $\Delta(f_z) = -4\Im(z)^2$, we see that $f_z \in \mathcal{P}$, and so the map $\tau : \mathcal{P} \to \mathfrak{H}$ is surjective. It is not injective because we clearly have

$$\tau(rf) = \tau(f), \quad \text{for all } f \in \mathcal{P}, r > 0. \tag{1.41}$$

Nevertheless, τ induces a bijection $\mathcal{P}/\mathbb{R}_{>0} \xrightarrow{\sim} \mathfrak{H}$, as we shall see below.

Recall that the group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H}$ via *linear transformations*:

$$T(z) = \frac{az + b}{cz + d}, \quad \text{if } z \in \mathfrak{H},\ T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

As the notation indicates, this is a *left action* on $\mathfrak{H}$: we have $T_1(T_2(z)) = (T_1T_2)(z)$, for all $T_1, T_2 \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in fH$. We can convert this into a *right action* by defining

$$zT = T^{-1}(z), \quad \text{for all } z \in \mathfrak{H},\ T \in \mathrm{SL}_2(\mathbb{Z}).$$

(Indeed: $(zT_1)T_2 = T_2^{-1}(zT_1) = T_2^{-1}(T_1^{-1}(z)) = (T_2^{-1}T_1^{-1})(z) = (T_1T_2)^{-1}(z) = z(T_1T_2)$, so this gives a right action.)

We now relate this action to the (right) action of $\mathrm{SL}_2(\mathbb{Z})$ on quadratic forms:

Proposition 1.19 *We have*

$$\tau(fT) = \tau(f)T, \quad \textit{for all } f \in \mathcal{P},\ T \in \mathrm{SL}_2(\mathbb{Z}), \tag{1.42}$$

and so the map τ induces a bijection $\mathcal{P}/\mathbb{R}_{>0} \xrightarrow{\sim} \mathfrak{H}$ which is $\mathrm{SL}_2(\mathbb{Z})$-equivariant with respect to the right actions of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{P}$ and on $\mathfrak{H}$.

Proof. By (1.41) we see that τ induces a map $\mathcal{P}/\mathbb{R}_{>0} \to \mathfrak{H}$ which is surjective by (1.40). We now prove that this map is injective. For this, let $f_i \in \mathcal{P}$ be such that $\tau(f_1) = \tau(f_2)$, and let $r_2 > 0$ be such that $r_2^2 = \Delta(f_1)/\Delta(f_2)$, and put $r_1 = 1$, $f_i' = r_i f_i$. Then

$\Delta(f_1') = \Delta(f_2')$ and $\tau(f_i') = \tau(f_i)$. Write $f_i' = [a_i, b_i, c_i]$. Since $\tau(f_1') = \tau(f_2')$, we have $\Im(\tau(f_1')) = \Im(\tau(f_2'))$, so $a_1 = a_2$. Similarly, looking at the real parts yields $b_1 = b_2$, and hence $c_1 = c_2$. Thus $f_1 = rf_2$, which proves the desired injectivity.

To prove (1.42), consider the set

$$G = \{T \in \mathrm{SL}_2(\mathbb{Z}) : \tau(fT) = \tau(f)T, \quad \forall f \in \mathcal{P}\}.$$

It is easy to set that G is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. (Indeed, if $T_1, T_2 \in G$, then $T_1T_2^{-1} \in G$ because for $f \in \mathcal{P}$ we have $\tau(f)T_1 = \tau(fT_1) = \tau(fT_1T_2^{-1}T_2) = \tau(fT_1T_2^{-1})T_2$, and so $\tau(f)T_1T_2^{-1} = \tau(fT_1T_2^{-1})$, i.e. $T_1T_2^{-1} \in G$.) Since $G \leq \mathrm{SL}_2(\mathbb{Z})$, it is enough to show that $t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G$ and $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in G$ because $\mathrm{SL}_2(\mathbb{Z}) = \langle s, t\rangle$ by Proposition 1.18.

To see that $t \in G$, let $f = [a, b, c] \in \mathcal{P}$. Then $ft = [a, b + 2a, *]$ and $\Delta(ft) = \Delta(f)$. Thus

$$\tau(ft) = \frac{-(b + 2a) + \sqrt{\Delta(f)}}{2a} = \tau(f) - 1 = t^{-1}(\tau(f)) = \tau(f)t,$$

and so $t \in G$. To see that $s \in G$, let $f \in \mathcal{P}$. Then $f = rf_z$ for some $r > 0$ and $z = \tau(f)$ by what was shown above. Then $fs = r[1, -2\Re(z), |z|^2]s = r[|z|^2, 2\Re(z), 1] = (r/|z|^2)f_{-1/z}$, and so by (1.41)

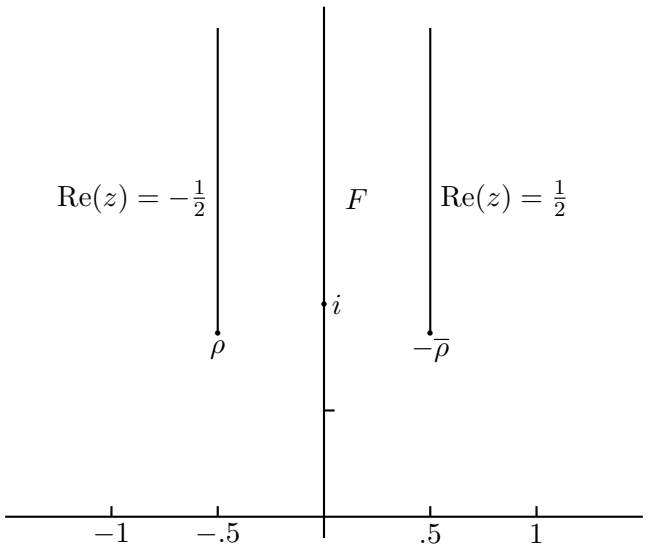
$$\tau(fs) = \tau(f_{-1/z}) = \frac{-1}{z} = s^{-1}(z) = zs = \tau(f)s,$$

and so $s \in G$, and hence $G = \mathrm{SL}_2(\mathbb{Z})$. Thus (1.42) holds for all $T \in \mathrm{SL}_2(\mathbb{Z})$, and so the map $\mathcal{P}/\mathbb{R}_{>0} \to \mathfrak{H}$ is $\mathrm{SL}_2(\mathbb{Z})$-equivariant.

Remark 1.10 By a direct (but tedious) computation one can verify that (1.42) holds for all $T \in \mathrm{SL}_2(\mathbb{R})$.

We can now give a geometric interpretation of reduction in terms of the sets

$$F = \{z \in \mathfrak{H} : |z| > 1, |\Re(z)| < \tfrac{1}{2}\} \quad \text{and} \quad \overline{F} = \{z \in \mathfrak{H} : |z| \geq 1, |\Re(z)| \leq \tfrac{1}{2}\}.$$



Proposition 1.20 *If $f = [a, b, c] > 0$, then*

$$\Re(\tau(f)) = -\frac{b}{2a} \quad \textit{and} \quad |\tau(f)|^2 = \frac{c}{a}. \tag{1.43}$$

Thus, f is semi-reduced if and only if $\tau(f) \in \overline{F}$.

Proof. The first equation of (1.43) is clear. To prove the second, put $\Delta(f) = -D$. Then

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

as claimed. From this the last assertion follows immediately.

Remark 1.11 It is clear from (1.43) and the definitions that f is reduced if and only if $f \in F_{red}$, where

$$F_{red} = F \cup \{z \in \overline{F} : \Re(z) = -\tfrac{1}{2}\} \cup \{z \in \overline{F} : |z| = 1, \Re(z) \leq 0\}.$$

Corollary 1.21 *For every $z \in \mathfrak{H}$, there is a unique $z_0 \in F_{red}$ such that $z_0 = T(z)$, for some $T \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. By Remark 1.6(b) there exists a $T \in \mathrm{SL}_2(\mathbb{Z})$ such that $f_0 = f_z T$ is reduced, and then $z_0 := \tau(f_0) \in F_{red}$ by Remark 1.11. Moreover, $z_0 = zT = T^{-1}(z)$ by (1.42). This proves the existence of z_0. The uniqueness follows by combining Propositions 1.16 and 1.19 (and Remark 1.11).

Remark 1.12 *Note that the above proof is constructive: given $z \in \mathfrak{H}$, the reduction algorithm gives us a quick method for finding a matrix $T \in \mathrm{SL}_2(\mathbb{Z})$ such that $z_0 = T(z) \in F_{red}$*

Definition. A point $z \in \mathfrak{H}$ is called a *complex multiplication point* (or CM-point) if $z = \tau(f)$ for some $f = [a, b, c] > 0$ with $a, b, c \in \mathbb{Z}$.

These points will play an important role in the second part of this course.

1.3.3 Reduction of indefinite forms (overview)

There is a close (but imperfect) connection between:

(i) the reduction of an indefinite form $f = [a, b, c]$ of discriminant $D > 0$ ($D \neq \square$);

(ii) the continued fraction expansion of $\tau(f) := \frac{-b+\sqrt{D}}{2a} \in \mathbb{R}$;

(iii) "good" rational approximations of $\tau(f)$, i.e. rational numbers $\frac{x}{y}$ satisfying

$$\left|\frac{x}{y} - \tau(f)\right| < \frac{1}{2y^2}. \tag{1.44}$$

Moreover, all three are related to solving the so-called *Pell equation*

$$x^2 - dy^2 = 1. \tag{1.45}$$

As a result, the history of this problem is somewhat convoluted, particularly since it was only later that the connection between these problems was made precise. Some highlights are:[5]

- Archimedes (ca. 300BC) and other Greeks found *good* approximations to $\sqrt{3}$ and to $\sqrt{2}$; these satisfy Pell-type equations. ([We], p. 15, 230).
- In India, Baskara (12^{th}C) used the *crakvala* (or cyclic) method to solve (1.45) in many cases.
- In the 17^{th} century, the above method was rediscovered by Brouncker and Wallis and probably also by Fermat (who called it "infinite descent"); cf. [We], p. 23, 92. This method is essentially the method of continued fractions.
- Euler (1730) named equation (1.45) "Pell's equation" (and the method of Brouncker and Wallis the "Pellian method"), but it seems that Pell never considered this equation; cf. [We], p. 230. Euler notes that solutions of (1.45) give good rational approximations of $\sqrt{d}$ and proved that if (1.45) has one solution, then it has infinitely many; cf. [We], p. 230.
- In 1768 Lagrange was the first to prove that (1.45) always has a solution; cf. [We], p. 314. Later (1775) he used these ideas to define the reduction theory of indefinite (and of definite) forms.

Continued fractions

Let $x \in \mathbb{R}$, $x > 0$. Put $a_0 = [x]$, $x_0 = x - a_0$ and for $i \geq 1$:

$$a_i = \left[\frac{1}{x_{i-1}}\right], \quad x_i = \frac{1}{x_{i-1}} - a_i, \quad \text{provided that } x_{i-1} \neq 0. \tag{1.46}$$

(If $x_{i-1} = 0$, then we stop the iteration.) Then we have after n iterations:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots \cfrac{1}{a_n + x_n}}}.$$

Denote the right hand side by the symbol $[a_0; a_1, \ldots, a_n + x_n]$. Since the a_i's are integers, the number

$$c_n = [a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}$$

[5] See [Di], vol. II, ch. XII, for a thorough discussion of the history of this problem.

is a rational number which is called the n-th *convergent* of x because we have

$$x = \lim_{n\to\infty} c_n;$$

indeed, one can show more precisely (cf. [Bu], p. 38) that if $x \notin \mathbb{Q}$, then

$$c_{2k} < c_{2k+2} < \ldots < x < \ldots < c_{2k+3} < c_{2k+1}, \quad \text{for all } k \geq 0. \tag{1.47}$$

We are thus justified in writing x as an infinite continued fraction $x = [a_0; a_1, \ldots, a_n, \ldots]$.

Remark. 1) It is easy to see that $x_i = 0$ for some i if and only $x \in \mathbb{Q}$. In this case we have only a finite expansion, and the a_i's correspond to the successive quotients appearing in the steps of the Euclidean algorithm applied to (r, s), where $x = \frac{r}{s}$; cf. [HW], p. 136.

2) For every convergent $c_n = \frac{p_n}{q_n}$ we have that

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2},$$

([HW], p. 140) and that for any two consecutive convergents, at least one satisfies the stronger inequality

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2};$$

cf. [HW], p. 152. Conversely, if $c = \frac{p}{q}$ satisfies this stronger inequality, then it is a convergent of x, i.e. $c = c_n$ for some n ([HW], p. 153). Thus we see that conditions (ii) and (iii) on p. 22 are closely related.

Example 1.6 The continued fraction expansion (cfe) of $\sqrt{3}$ is $\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, \ldots] = [1; \overline{1, 2}]$, so the expansion is periodic with period of length 2. The first few convergents are

$$c_0 = 1,\ c_1 = 2,\ c_2 = \frac{5}{3},\ c_3 = \frac{7}{4},\ c_4 = \frac{19}{11}, c_5 = \frac{26}{15}, \ldots$$

Archimedes found and used (cf. [Di], II, p. 342) the following approximations of $\sqrt{3}$:

$$c_8 = \frac{265}{153} < \sqrt{3} < \frac{13}{153} = c_{11}.$$

Note that $\sqrt{3}$ has a periodic cfe. This is a general property of quadratic irrationals, as was first observed by Euler and Lagrange (cf. [La1], p. 57 or [Bu], p. 39):

Fact 1.22 (Euler/Lagrange) *x has a periodic continued fraction expansion if and only if x is a quadratic irrational, i.e. $x \notin \mathbb{Q}$ and $ax^2 + bx + c = 0$, for some $a, b, c \in \mathbb{Z}$.*

Indefinite forms

Definition. A form $f = [a, b, c]$ of discriminant $\Delta(f) = D > 0$ is called *reduced* if we have

$$0 < b < \sqrt{D}, \quad \sqrt{D} - b < 2|a| < \sqrt{D} + b, \tag{1.48}$$

or, equivalently, if $|\sqrt{D} - 2|a|| < b < \sqrt{D}$. If $a > 0$, then this is also equivalent to the condition

$$\tau(f) > 1 \quad \text{and} \quad \frac{-1}{\tau'(f)} > 1; \tag{1.49}$$

cf. Lang[La1], p. 55. Here $\tau'(f) = \frac{-b-\sqrt{D}}{2a}$ and, as before, $\tau(f) = \frac{-b+\sqrt{D}}{2a}$. In addition, this condition is equivalent to the property that $\tau(f)$ has a purely periodic cfe; cf. Lang[La1], p. 57.

Example 1.7 The principal form $1_D = [1, \varepsilon, \frac{\varepsilon - D}{4}]$ of discriminant $D > 0$ is only reduced for $D = 5$. However, if $a_0 = [\tau(1_D)] = [(\sqrt{D} - \varepsilon)/2]$, then $1_D^* = [1, \varepsilon + 2a_0, *]$ is a reduced form which is properly equivalent to 1_D, i.e. $1_D^* \sim 1_D$.

Fact 1.23 1) *There exist only finitely many reduced forms of discriminant $D > 0$.* [This is clear because b is bounded and since $(b^2 - D)/4 = ac$ has only finitely many factorizations into integers a, b.]

2) *For each $f = [a, b, c]$ there is an $r(f) \sim f$ which is reduced.* More precisely, let the *reduction operator* ρ be defined by

$$\rho(f) = fT, \quad \text{where } T = \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix} \text{ with } s = \operatorname{sign}(c) \left[\frac{\sqrt{D} + b}{2|c|} \right].$$

If we put $f_0 = f$ and $f_k = \rho(f_{k-1})$ for $k \geq 1$, then there is an integer $n \geq 0$ such that f_n is reduced; cf. [Bu], p. 22. We put $r(f) := f_n \sim f$.

3) From 1) and 2) it follows that the number of classes (*class number*) is *finite*:

$$h(D) := \#Cl(D) = \#(Q_D/\mathrm{SL}_2(\mathbb{Z})) < \infty. \tag{1.50}$$

4) Each (proper) equivalence class $cl(f) := \{f_1 : f_1 \sim f\}$ contains (by 1)) finitely many reduced forms, but in general more than one. The set $cyc(f) = \{f_1 \in cl(f) : f_1 \text{ is reduced}\}$ of reduced forms in $cl(f)$ in called the *cycle* of f. It turns out that the reduction operator acts *transitive* on $cyc(f)$, i.e. for any $f_1 \in cyc(f)$ we have

$$cyc(f) = \{\rho^k(f_1) : 1 \leq k \leq n\} \quad \text{and } \rho^n(f_1) = f_1;$$

where $n = \#cyc(f)$; [BV], p. 126. This number n is called the *period* of f and is closely related (but not necessarily equal) to the period of the continued fraction $\tau(f)$.

5) We have $\mathrm{Aut}^+(f) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. An explicit generator T of $\mathrm{Aut}^+(f)/\{\pm I\}$ can be constructed by taking a suitable product of the matrices $T_i \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, where the T_i are

defined by the relations $f_{i+1} = f_i T_i$ for $cyc(f) = \{f_1, \ldots, f_n\}$ and $f_1 = fT_0$; cf. [BV], p. 133 (and pp. 127-9) for the precise recipe of T.

6) There is a natural bijection

$$\mathrm{Aut}^+(f) \xrightarrow{\sim} S(1_{4D}, 4)$$

which described explicitly in [BV], p. 28, and/or in [Bu], p. 31. Thus, there is a close relation between $\mathrm{Aut}^+(f)$ and the set of solutions $S(1_{4D}, 4)$ of the Pell-type equation

$$x^2 - Dy^2 = 4. \tag{1.51}$$

Moreover, if (x_1, y_1) is the solution of (1.51) corresponding via this bijection to the generator T of 5), then the set of positive solutions of (1.51) (i.e. those solutions (x, y) with $x > 0, y > 0$) is $\{(x_n, y_n) : n \geq 1\}$, where x_n, y_n are given by the formula

$$\frac{x_n + y_n\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n;$$

cf. [Bu], p. 33. In particular, (x_1, y_n) is the smallest positive solution of (1.51) in the sense that $x_n + y_n\sqrt{D} > x_1 + y_1\sqrt{D}$, for all $n > 1$.

7) The minimum of f is

$$\min(f) = \{|f_i(1, 0)| : f_i \in cyc(f)\};$$

cf. [BV], p. 139. Note that this solves Problem 3.

Remark. In Shanks[Sh], p. 178, there is a nice algorithm for solving the original Pell equation (1.45).

1.3.4 Applications to representation numbers

Let us now return to Lagrange's treatment of the Fermat/Euler results. By combining Propositions 1.6 and 1.8 we obtain as a special case the following result.

Proposition 1.24 *Let f be a primitive form of discriminant Δ. If $h(\Delta) = 1$, then for all n with $(n, \Delta) = 1$ we have:*

$$n \in R(f) \quad \Leftrightarrow \quad \#\mathrm{Sqrt}(\Delta, 4n) > 0, \tag{1.52}$$

where $\mathrm{Sqrt}(\Delta, m) = \{x \pmod m : x^2 \equiv \Delta \pmod m\}$ denotes the set of square roots of Δ mod m.

Proof. ($\Rightarrow$) Corollary 1.7.

($\Leftarrow$) If $b \in \mathrm{Sqrt}(\Delta, 4n)$, then (cf. Proposition 1.8) $\exists c$ such that $f_0 := [n, b, c]$ has $\Delta(f_0) = \Delta$. Since $(n, \Delta) = 1$, we see that f_0 is primitive, and so $f_0 \sim f$ because $h(\Delta) = 1$. Thus $n \in R(f_0) = R(f)$.

We thus need to study $\#\mathrm{Sqrt}(\Delta, 4n)$ in more detail. More precisely, we need to answer:

Question. *For which n's is $\#\mathrm{Sqrt}(\Delta, 4n) > 0$?*

Note that for a fixed n, it is "easy" to find the finite list of conditions on $\Delta \pmod{4n}$ which characterize the property "$\#\mathrm{Sqrt}(\Delta, 4n) > 0$". In the above question, however, Δ is fixed and n varies, so this is a much harder question.

To solve this question, we first observe that we can reduce it to the case of prime numbers $n = p$:

Proposition 1.25 *If $(n, \Delta) = 1$, then*

$$\#\mathrm{Sqrt}(\Delta, 4n) > 0 \quad \Leftrightarrow \quad \#\mathrm{Sqrt}(\Delta, 4p) > 0, \text{ for all primes } p|n. \tag{1.53}$$

Proof. ($\Rightarrow$) Trivial.

($\Leftarrow$) (Sketch)[6] If $\#\mathrm{Sqrt}(\Delta, 4p) > 0$, then there exists $x_1 \in \mathbb{Z}$ such that $x_1^2 \equiv \Delta \pmod{p}$, if $p > 0$. (For $p = 2$ we have that $\exists x_1$ such that $x_1^2 \equiv \Delta \pmod 8$.) Then by the method of Newton/Hensel we can lift successively x_k to a solution x_{k+1} of $x^2 \equiv \Delta \pmod{p^{k+1}}$ (resp. of $x^2 \equiv \Delta \pmod{4 \cdot 2^{k+1}}$) for $k = 1, 2, \ldots$. By using the Chinese Remainder Theorem (with some care), we obtain a solution $x \in \mathrm{Sqrt}(\Delta, 4n)$.

In studying the above question for $n = p$, it is useful to use the *Legendre symbol* $\left(\frac{a}{p}\right)$ which Legendre introduced in 1798; cf. [We], p. 323. This is defined for an odd prime $p > 2$ by the rule

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution } x \not\equiv 0 \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

Following Kronecker (who was perhaps inspired by a notation used by Dirichlet[7]), it is useful to extend this symbol to the prime $p = 2$ as follows:

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod 2 \\ (-1)^{\frac{a^2-1}{8}} & \text{if } x \equiv 1 \pmod 2 \end{cases}$$

In other words, $\left(\frac{a}{2}\right) = 1 \Leftrightarrow a \equiv \pm 1 \pmod 8$ and $\left(\frac{a}{2}\right) = -1 \Leftrightarrow a \equiv \pm 3 \pmod 8$.

[6] For details, see Hua[Hu], p. 306.

[7] [Di], II, p. 370 (footnote).

Remark 1.13 (a) It is easy to verify that if p is a prime with $p \nmid \Delta$, then

$$\#\mathrm{Sqrt}(\Delta, 4p) > 0 \quad \Leftrightarrow \quad \left(\frac{\Delta}{p}\right) = 1. \tag{1.54}$$

Thus, we see from Corollary 1.7 that

$$n \in R(f),\ (n, \Delta(f)) = 1 \quad \Rightarrow \quad \left(\frac{\Delta(f)}{p}\right) = 1,\ \forall p | n. \tag{1.55}$$

(b) Put $p^* = 8$ if $p = 2$ and $p^* = p$ if p is an odd prime. It is easy to see that

$$a \equiv b \pmod{p^*} \quad \Rightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \tag{1.56}$$

(c) It is harder to verify that the symbol $\left(\frac{\cdot}{p}\right)$ is multiplicative, i.e. that

$$\left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{ab}{p}\right). \tag{1.57}$$

For $p = 2$ this is a straightforward verification from the definition, but for $p > 2$ it is more difficult. For example, one can verify this by using *Euler's criterion*:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}, \quad \text{if } p \neq 2. \tag{1.58}$$

(This criterion can be proved by using the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group.)

(d) In particular, it follows from (1.58) that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod{p}, \quad \text{if } p \neq 2, \tag{1.59}$$

so if $p \neq 2$, then $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$.

We can now proceed to give a proof of Fermat's Theorem 1.1. Recall that this is the statement

$$p \in R(x^2 + y^2) \quad \Leftrightarrow \quad p \equiv 1 \pmod 4 \ \text{ or } \ p = 2.$$

Proof of Theorem 1.1. We apply Proposition 1.24 to $f(x, y) = x^2 + y^2$. Here $\Delta = -4$ so $h(\Delta) = 1$ by Corollary 1.11. Thus, for an odd prime p we have by Proposition 1.24 that

$$p \in R(f) \ \Leftrightarrow \ \left(\frac{-4}{p}\right) = 1 \ \Leftrightarrow \ \left(\frac{-1}{p}\right) = 1 \ \Leftrightarrow \ p \equiv 1 \pmod 4,$$

the latter by (1.59). This proves the assertion for odd primes and hence for all primes since $2 = f(1, 1)$.

Remark. Note that the above proof does not seem to use Fermat's "method of infinite descent". In actual fact, however, the infinite descent is hidden in the reduction algorithm.

To illustrate this, suppose we want to prove that $17 = x^2 + y^2$ has a solution by using the above method of proof. Since $4^2 \equiv -1 \pmod{17}$, we see that $8^2 \equiv -4 \pmod{4 \cdot 17}$, so $f_0 = [17, 8, 1]$ is a form with $\Delta(f_0) = -4$. By the reduction algorithm (and $h(\Delta) = 1$) we can find $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(Z)$ such that $f_0 T = [1, 0, 1] = f$, and so $f_0 = fT^{-1} = f\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, so $17 = d^2 + (-c)^2$. However, to find T, we apply the reduction operator repeatedly, and these applications correspond exactly to Fermat's method of descent.

To extend Lagrange's method to other discriminants (with $h(\Delta) = 1$), it is clear that we need to solve

Problem. Describe the set of primes p with $\left(\frac{\Delta}{p}\right) = 1$.

It turns out that the set of these primes can be described by congruence conditions (mod Δ). However, this fact is not at all obvious and is essentially the content of the *Law of Quadratic Reciprocity*. A preliminary version of this law was first discovered by Euler around 1742, and later in 1772 he formulated the complete version (which was published in 1783); cf. [We], p. 187, 208. This was then reformulated by Legendre in 1785 who gave an incorrect proof; cf. [We], p. 326, 328. Gauss rediscovered this law in 1796 (cf. [Cox], p. 64) and gave the first correct proof(s) which were published in [DA] in 1801.

Theorem 1.4 (Quadratic Reciprocity) *If p and q are odd primes, then*

$$\left(\frac{2}{p}\right) = \left(\frac{p}{2}\right) = (-1)^{\frac{p^2-1}{8}}, \tag{1.60}$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{1.61}$$

Proof. See Hua[Hu], p. 38.

By using this theorem, we can solve the Euler's problem in many more cases (but certainly not in all):

Example 1.8 We have:

$$p \in R(x^2 + 2y^2) \quad \Leftrightarrow \quad p \equiv 1, 3 \pmod{8} \text{ or } p = 2. \tag{1.62}$$

Indeed, here $f = x^2 + 2y^2$ has $\Delta(f) = -8$, so again $h(\Delta) = 1$ by Corollary 1.11. We can thus apply Proposition 1.24 to obtain that if p is an odd prime, then

$$p \in R(f) \Leftrightarrow \left(\frac{-8}{p}\right) = 1 \Leftrightarrow p \equiv 1, 3 \pmod{8},$$

the latter because $\left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$, and so $\left(\frac{-8}{p}\right) = 1 \Leftrightarrow \left(\frac{-1}{p}\right) = 1, \left(\frac{2}{p}\right) = 1$ or $\left(\frac{-1}{p}\right) = -1, \left(\frac{2}{p}\right) = -1 \Leftrightarrow p \equiv 1\,(4), p \equiv \pm 1\,(8)$ or $p \equiv 3\,(4), p \equiv \pm 3\,(8) \Leftrightarrow p \equiv 1\,(8)$ or $p \equiv 3\,(8)$. This proves (1.62) because for $p = 2$ we have $2 = f(0,1)$.

As the above example shows, we can describe the set of primes satisfying $\left(\frac{\Delta}{p}\right) = 1$ by congruence conditions mod Δ. This is not immediately obvious since the presence of the sign in the Quadratic Reciprocity formula seems to point to a congruence mod 4Δ. However, we have:

Proposition 1.26 *Let $\Delta \equiv 0, 1 \pmod 4$. Then there is a unique homomorphism*

$$\chi_\Delta : (\mathbb{Z}/\Delta\mathbb{Z})^\times \;\to\; \{\pm 1\}$$

such that $\chi_\Delta(p) = \left(\frac{\Delta}{p}\right)$, for all primes $p \not| \Delta$. In particular, the condition $\left(\frac{\Delta}{p}\right) = 1$ depends only on the congruence class of $p \pmod \Delta$. Thus, for a form $f \in Q_\Delta$ we have

$$\chi_\Delta(n) = 1, \quad \textit{for all } n \in R(f) \textit{ with } (n, \Delta) = 1. \tag{1.63}$$

Proof. If χ_Δ exists, then we can lift it to a homomorphism $\tilde{\chi}_\Delta : \mathbb{N} \to \{\pm 1\}$ by setting $\tilde{\chi}_\Delta(n) = 0$ if $(n, \Delta) > 1$. Thus $\tilde{\chi}_\Delta(p) = \left(\frac{\Delta}{p}\right)$, for all primes p, and so $\tilde{\chi}_\Delta$ is given by the *Kronecker-Jacobi symbol* $\left(\frac{\Delta}{n}\right)$, i.e.

$$\tilde{\chi}_\Delta(n) \;=\; \left(\frac{\Delta}{n}\right) \;:=\; \left(\frac{\Delta}{p_1}\right)^{e_1}\left(\frac{\Delta}{p_2}\right)^{e_2} \cdots \left(\frac{\Delta}{p_1}\right)^{e_r},$$

when $n = p_1^{e_1} \cdots p_r^{e_r}$ is a positive integer. Thus, $\tilde{\chi}_\Delta$ and hence χ_Δ is uniquely defined.

To prove existence, let $\tilde{\chi}_\Delta : \mathbb{N} \to \{\pm 1\}$ be defined by $\tilde{\chi}_\Delta(n) = \left(\frac{\Delta}{n}\right)$. By using the Quadratic Reciprocity Theorem 1.4 one easily sees that for $n > 0$ we have that

$$\tilde{\chi}_\Delta(n) \;=\; \begin{cases} \left(\dfrac{n}{|\Delta|}\right) & \text{if } \Delta \equiv 1 \pmod 4 \\ \left(\dfrac{2}{n}\right)^b \left(\dfrac{n}{|u|}\right) (-1)^{\frac{u-1}{2}\frac{n-1}{2}} & \text{if } \Delta = 2^b u, 2 \not| u \end{cases} \tag{1.64}$$

cf. [Hu], p. 305. From this one easily concludes that $\tilde{\chi}_\Delta(n_1) = \tilde{\chi}_\Delta(n_2)$ if $n_1 \equiv n_2 \pmod \Delta$, (and $n_i > 0$) and so $\tilde{\chi}_\Delta$ induces the desired homomorphism χ_Δ on $(\mathbb{Z}/\Delta\mathbb{Z})^\times$.

Finally, if $n \in R(f)$ and $(n, \Delta) = 1$, then by (1.55) we have $\left(\frac{\Delta}{p}\right) = 1$ for all $p|n$, and so $\chi_\Delta(n) = \left(\frac{\Delta}{n}\right) = 1$, which proves (1.63).

Remark 1.14 The above discussion and examples raise the natural question: *For which Δ's can the method of* Proposition 1.24 *be applied*? In other words:

Question. For which Δ's is $h(\Delta) = 1$?

This question was (indirectly) discussed by Gauss[DA] in Articles 303 and 304. From this discussion one can extract the following conjectures [8]:

1) If $\Delta < 0$, then $h(\Delta) = 1$ for precisely 13 values of Δ, i.e. the 6 with $-\Delta \leq 12$ and $-\Delta = 16, 19, 27, 28, 43, 67, 163$.

2) If $\Delta > 0$, then $h(\Delta) = 1$ for infinitely many Δ's.

Although the second conjecture is still open, the first has been settled. Heilbronn (1934) proved that $h(\Delta) \to \infty$ as $-\Delta \to \infty$, so in particular we see that there exist only finitely many Δ's with $\Delta < 0$ and $h(\Delta) = 1$. Heegner (1952) proved that the above conjecture is correct; for this he used the theory of modular forms and elliptic curves with CM. Later Baker (1966), Stark (1967) and Goldfeld/Gross/Zagier (1976/1986) gave other proofs.

1.3.5 Applications to the representation problem

We can refine the results of the previous subsection about the set $R(f)$ of numbers represented by f to yield precise information about the sets $P(f, n)$ of primitive representations. (Recall: $n \in R(f) \Leftrightarrow P(f, n) \neq \emptyset$.)

For this we observe that the key step of the proof of Proposition 1.6 can be reinterpreted as follows.

Proposition 1.27 *The group* $\mathrm{SL}_2(\mathbb{Z})$ *acts transitively on the set* $P(\mathbb{Z}^2) = \{\binom{x}{y} \in \mathbb{Z}^2 : \gcd(x, y) = 1\}$ *of primitive vectors. Thus, the map* $e_\infty : T \mapsto T\binom{1}{0}$ *induces a bijection*

$$\bar{e}_\infty : \mathrm{SL}_2(\mathbb{Z})/\Gamma_\infty \xrightarrow{\sim} P(\mathbb{Z}^2), \quad \textit{where } \Gamma_\infty = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}.$$

Proof. Let $\binom{x}{y} \in P(\mathbb{Z}^2)$. Then the proof of Proposition 1.6 shows that $\exists z, w \in \mathbb{Z}$ such that $T = \begin{pmatrix} x & z \\ y & w \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Thus $\binom{x}{y} = T\binom{1}{0}$ is in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of $\binom{1}{0}$, which means that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $P(\mathbb{Z}^2)$.

From this, the last assertion follows immediately once we have shown that the stabilizer of $\binom{1}{0}$ is Γ_∞, and this is clear because $T\binom{1}{0} = \binom{1}{0} \Leftrightarrow T = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \Leftrightarrow T = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in \Gamma_\infty$, the latter because $\det(T) = 1$.

Corollary 1.28 *If* f *is a quadratic form, then the rule* $fT \mapsto \mathrm{Aut}^+(f)e_\infty(T)$ *defines a surjection* $e_f : cl(f) := \{f_1 : f_1 \sim f\} \to \mathrm{Aut}^+(f)\backslash P(\mathbb{Z}^2)$ *which induces a bijection*

$$\bar{e}_f : cl(f)/\Gamma_\infty \xrightarrow{\sim} \mathrm{Aut}^+(f)\backslash P(\mathbb{Z}^2).$$

[8] Gauss only considered the case of even discriminants, but the extension to odd discriminants is straightforward.

Proof. First note that the map e_f is well-defined. Indeed, if $T_i \in \mathrm{SL}_2(\mathbb{Z})$ are such that $fT_1 = fT_2$, then $fT_1T_2^{-1} = f$, so $T_1T_2^{-1} \in \mathrm{Aut}^+(f)$ or $T_1 \in \mathrm{Aut}^+(f)T_2$. Thus $e_\infty(T_1) = T_1\binom{1}{0} \in \mathrm{Aut}^+(f)T_2\binom{1}{0} = \mathrm{Aut}^+(f)e_\infty(T_2)$, i.e. $e_\infty(T_1)$ is in the $\mathrm{Aut}^+(f)$-orbit of $e_\infty(T_2)$, and so the map is well-defined.

It is clear that e_f is surjective because $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $P(\mathbb{Z}^2)$. Moreover, $e_f(fT_1) = e_f(fT_2) \Leftrightarrow \mathrm{Aut}^+(f)T_1\binom{1}{0} = \mathrm{Aut}^+(f)T_2\binom{1}{0} \Leftrightarrow T_1\binom{1}{0} = AT_2\binom{1}{0}$, for some $A \in \mathrm{Aut}^+(f) \Leftrightarrow T_1\Gamma_\infty = AT_2\Gamma_\infty$, for some $A \in \mathrm{Aut}^+(f) \Leftrightarrow fT_1\Gamma_\infty = fT_2\Gamma_\infty$, and so e_f induces the bijection $\bar{e}_f$ by passing to the Γ_∞-orbits of $cl(f)$.

Corollary 1.29 *For every $f_1 \in cl(f)$ we have $f(e_f(f_1)) = f_1(1,0)$. Thus, if $n \in \mathbb{Z}$, and $cl(f)_n = \{f_1 \in cl(f) : f_1(1,0) = n\}$, then the map $\bar{e}_f$ restricts to a bijection*

$$\bar{e}_{f,n} : cl(f)_n/\Gamma_\infty \xrightarrow{\sim} \mathrm{Aut}^+(f)\backslash P(f,n). \tag{1.65}$$

Proof. First note that $f(e_f(f_1))$ is well-defined because if $v_1, v_2 \in e_f(f_1) = \mathrm{Aut}^+(f)v_1$ are two representatives, then $v_2 = Av_1$ with $A \in \mathrm{Aut}^+(f)$, and then $f(v_2) = f(Av_1) = f(v_1)$.

To prove the formula, let $f_1 \in cl(f)$; thus $f_1 = fT$ with $T \in \mathrm{SL}_2(\mathbb{Z})$. Then $f_1(1,0) = (fT)\binom{1}{0} = f(T\binom{1}{0}) = f(e_\infty(T)) = f(e_f(fT)) = f(e_f(f_1))$, as claimed.

Finally, since $cl(f)_n$ is the fibre above n of the map $f_1 \mapsto f_1(1,0)$ and $P(f,n)$ is the fibre above n of the map $v \mapsto f(v)$, the above rule shows that the image of $cl(f)_n/\Gamma_\infty$ is precisely $\mathrm{Aut}^+(f)\backslash P(f,n)$.

The above corollary can be viewed as a quantitative refinement of Proposition 1.6. In a similar vein we have the following quantitative refinement of Proposition 1.8.

Proposition 1.30 *Let $Q^*_{\Delta,n} = \{[n,b,c] \in \mathbb{Z}^3 : b^2 - 4nc = \Delta\}$. If $n \neq 0$, then the map $[n,b,c] \mapsto b \pmod{2n}$ induces a bijection*

$$\lambda_n : Q^*_{\Delta,n}/\Gamma_\infty \xrightarrow{\sim} \mathrm{Sqrt}'(\Delta,n) := \{x \pmod{2n} : x^2 \equiv \Delta \pmod{4n}\}.$$

Proof. Since $[n,b,c]\left(\begin{smallmatrix}1 & m\\ 0 & 1\end{smallmatrix}\right) = [n, b+2nm, *]$, it is clear that the given rule factors over the Γ_∞-action to define the map λ_n. The argument of Proposition 1.8 shows that λ_n is surjective: if $b \in \mathrm{Sqrt}'(\Delta,n)$, then $b^2 = \Delta - 4nc$, for some $c \in \mathbb{Z}$ and then $\lambda_n([n,b,c]) = b \pmod{2n}$.

To see that λ_n is injective, let $f_i = [n,b_i,c_i] \in \mathbb{Q}^*_{\Delta,n}$ be such that $\lambda_n(f_1) = \lambda_n(f_2)$. Then $b_2 = b_1 + 2nk$, for some k, and then $f_1\binom{1\ k}{0\ 1} = [n,b_2,c]$, for some $c \in \mathbb{Z}$. Since $\Delta([n,b_2,c]) = \Delta(f_1) = \Delta = \Delta(f_2)$, we see that $c = c_2$, and so $f_2\Gamma_\infty = f_1\Gamma_\infty$. Thus λ_n is injective and hence bijective.

Corollary 1.31 *For any quadratic form f of discriminant Δ and integer $n \neq 0$, the rule $\binom{x}{y} \mapsto \lambda_n(f\binom{x\ *}{y\ *}) = \lambda_n(e_{f,n}^{-1}\binom{x}{y})$ induces an injection*

$$\lambda_{f,n} : \mathrm{Aut}^+(f)\backslash P(f,n) \hookrightarrow \mathrm{Sqrt}'(\Delta,n).$$

In particular, $\mathrm{Aut}^+(f)\backslash P(f,n)$ is a finite set.

Proof. By definition, $cl(f)_n = cl(f) \cap Q^*_{\Delta,n} \subset Q^*_{\Delta,n}$, so $\lambda_{f,n} := \lambda_n \circ e^{-1}_{f,n}$ defines the desired injection, and hence $\mathrm{Aut}^+(f)\backslash P(f,n)$ is a finite set because $\#\mathrm{Sqrt}'(\Delta,n) \leq 2n$.

In view of the above results, it is of interest to determine $\#\mathrm{Sqrt}'(\Delta,n)$. For $(n,\Delta)=1$ this is given by the following formula which may be viewed as a refinement of Proposition 1.25:

Proposition 1.32 *Suppose* $(n,\Delta)=1$ *and* $\Delta \equiv 0,1 \pmod 4$. *Then*

$$\#\mathrm{Sqrt}'(\Delta,n) \;=\; \frac{1}{2}\#\mathrm{Sqrt}(\Delta,4n) \;=\; \prod_{p|n}\left(1+\left(\frac{\Delta}{p}\right)\right).$$

Proof. The first equality is clear, and the second is proved in [Hu], p. 304. (The method of proof is similar to the one that was sketched in the proof of Proposition 1.25.)

We can combine the above results to prove the following formula which may be viewed as quantitative refinement of Lagrange's Theorem 1.2:

Corollary 1.33 *Let* $f_1, f_2, \ldots, f_h$ *be a system of representatives of* $Cl(\Delta) = Q_\Delta/\!\sim$, *and let* $n>0$ *be an integer with* $(n,\Delta)=1$. *Then*

$$\sum_{i=1}^{h} \#(\mathrm{Aut}^+(f_i)\backslash P(f_i,n)) \;=\; \prod_{p|n}\left(1+\left(\frac{\Delta}{p}\right)\right). \tag{1.66}$$

Proof. Since $(n,\Delta)=1$, we have that $Q^*_{\Delta,n} = Q_{\Delta,n} = \dot\cup_{i=1}^h cl(f_i)_n$. Thus, by (1.65) and Proposition 1.30 we obtain $\sum_{i=1}^h \#(\mathrm{Aut}^+(f_i)\backslash P(f_i,n)) = \sum_{i=1}^h \#(cl(f_i)_n/\Gamma_\infty) = \#(Q^*_{\Delta,n}/\Gamma_\infty) = \#\mathrm{Sqrt}'(\Delta,n)$, and so (1.66) follows by using Proposition 1.32.

Another application of the above results is the following criterion for equivalence which (for n a prime) was noticed by Piehler (1960):

Proposition 1.34 *If* f_1 *and* f_2 *are two positive definite forms of discriminant* Δ *which both represent primitively a prime power* $n=p^r$ *with* $(n,\Delta)=1$, *then* $f_1 \approx f_2$.

Proof. By Corollary 1.29 we have $f_i \sim f_i' = [n,b_i,c_i]$, for some $b_i, c_i \in \mathbb{Z}$. If $f_1' \in f_2'\Gamma_\infty$, then $f_1 \sim f_2$, so assume $f_1' \notin f_2'\Gamma_\infty$. Then by Proposition 1.30 $b_1 \not\equiv b_2 \pmod{2n}$, and so $b_1 \equiv -b_2 \pmod{2n}$ because $\#\mathrm{Sqrt}'(\Delta,n)=2$ by Proposition 1.32 since $n=p^r$. Thus $f_1' \in [n,-b_2,c_2]\Gamma_\infty$, so $f_1 \sim [n,-b_2,c_2] \approx [n,b_2,c_2] = f_2' \sim f_2$, and hence $f_1 \approx f_2$.

A variant of the above result is the following observation which is in part due to Euler, who used it as a *primality criterion*, i.e. as a method for determining that a given number is composite (cf. Remark 1.18(b) below).

Corollary 1.35 *Let* f *be a positive definite form of discriminant* $\Delta < -4$, *and let* $n=p^r$ *be a prime power with* $(n,\Delta)=1$.

(a) *The equation $f(x,y) = n$ has at most two primitive solution (x,y) with $x > 0$, and at most one if f is not ambiguous.*

(b) *If $f = [a,0,c]$, then the equation $f(x,y) = n$ has at most one primitive solution (x,y) with $x > 0$ and $y > 0$.*

Proof. (a) Suppose first there are three distinct solutions $v_i = (x_i, y_i)^t \in P(f,n)$ with $x_i > 0$. Since $\#\mathrm{Sqrt}'(\Delta, n) \leq 2$ by Proposition 1.32, it follows from Corollary 1.31 that $v_i = Av_j$, for some $i \neq j$ and $A \in \mathrm{Aut}^+(f)$. But since $\mathrm{Aut}^+(f) = \{\pm I\}$ by Proposition 1.17, we have $v_i = -v_j$, which is impossible since $x_i > 0$. This proves the first statement.

Next, suppose that f is not ambiguous and that there are two $v_i \in P(f,n)$ with $v_1 \neq \pm v_2$. By Corollary 1.29 $\exists f_i = [n, b_i, c_i] \in cl(f)_n$ such that $e_{f,n}(f_i) = \mathrm{Aut}^+(f)v_i$. Since $v_1 \notin \mathrm{Aut}^+(f)v_2 = \{\pm v_2\}$, it follows that $f_1 \notin f_2\Gamma_\infty$. Thus, as in the proof of Proposition 1.34 we see that $b_2 \equiv -b_1 \pmod{2n}$ and that hence $f_2 \sim [n, -b_1, c_1]$. But $f_2 \sim f_1$, so $f_1 = [n, b_1, c_1] \sim [n, -b_1, c_2]$, and hence $f \sim f_1$ is ambiguous, contradiction.

(b) By part (a) we have at most two solutions $(x_i, y_i) \in P(f,n)$ with $x_i > 0$. But since also $(x_1, -y_1) \in P(f,n)$, we must have $(x_2, y_2) = (x_1, -y_1)$, and so at most one of these satisfies the condition $y_i > 0$.

As we shall now see, the above Corollary 1.31 can also be used to solve the Representation Problem (Problem 2):

Algorithm for determining $P(f,n)$:

Given: A quadratic form f and an integer $n \neq 0$.

Result: A finite set $S \subset P(\mathbb{Z}^2)$ of primitive vectors such that $P(f,n) = \bigcup_{f_i \in S} \mathrm{Aut}^+(f)f_i$.

Steps: 1. Determine the set $\mathrm{Sqrt}'(\Delta(f), n)$.

2. For each $b \in \mathrm{Sqrt}'(\Delta(f), n)$, determine whether or not $f_b := [n, b, (b^2 - \Delta)/4n]$ is equivalent to f (use the reduction algorithm).

3. If $f_b \not\sim f$, go to step 3. Otherwise, there is a matrix $T_b \in \mathrm{SL}_2(\mathbb{Z})$ (found by the reduction algorithm) such that $f_b = fT_b$. Add $v = T_b\binom{1}{0}$ to the set S.

4. Take the next b in the set $\mathrm{Sqrt}'(\Delta(f), n)$ and repeat steps 2 and 3. The algorithm terminates when the list $\mathrm{Sqrt}'(\Delta(f), n)$ has been exhausted.

Remarks. 1) To get a complete solution to Problem 2, we should also determine the group $\mathrm{Aut}^+(f)$. However, this was already done: for positive definite forms, see Proposition 1.17 and for indefinite forms, see Fact 1.23, 5).

2) In [BV], p. 48, is it pointed out that even for prime numbers $n = p$ no (deterministic) *polynomial time* algorithm is known for finding the square root mod p of an arbitrary number x. (Note that the usual square root algorithm (cf. Koblitz[Ko2], p. 48) is not deterministic since it requires the use of an explicit non-residue $\pmod p$.) However, *Schoof's algorithm* (using elliptic curves) does extract a square root of a *fixed* x for varying p's in polynomial time (explicitly, in time $O(\log^9 p)$), and this is what we need in step 1 of the above algorithm (if f is fixed but $n = p$ varies).

1.4 Gauss: The Theory of Genera and of Composition

1.4.1 Genera

In trying to describe the set of primes in $R(f)$ by congruence conditions, Gauss noticed that the condition $h(\Delta) = 1$ (which was required in Proposition 1.24) can be replaced by the weaker one "$h(\Delta) = g(\Delta)$", where $g(\Delta)$ denotes the *number of genera*. The definition of this new invariant $g(D)$ (which was discovered by Gauss) is based on the following "composition formula".

Proposition 1.36 *If $f = [a, b, c]$ has discriminant Δ, then*

$$4f(x,y)f(x',y') \;=\; A^2 - \Delta B^2, \quad \textit{for all } x, y, x', y' \in \mathbb{R}, \tag{1.67}$$

where

$$A = 2axx' + b(xy' + x'y) + 2cyy' \quad \textit{and} \quad B = xy' - x'y. \tag{1.68}$$

Proof. Exercise.

Remark. If we substitute $x' = 1$ and $y' = 0$ in (1.67), then we recover the basic identity (1.5). On the other hand, if we take $a = 1$, $b = 0$, $c = N$, then the identity (1.67) reduces to the formula

$$(x^2 + Ny^2)((x')^2 + N(y')^2) \;=\; (A/2)^2 + NB^2 \;=\; (xx' + Nyy')^2 + N(xy' - x'y)^2, \tag{1.69}$$

which is a (slight) generalization of the identity (1.2) of Diophantus/Fibonacci. Indeed, Euler observed in his textbook on Algebra (1770) that (1.69) can be deduced from (1.2) by replacing y by $-\sqrt{N}y$, z by x' and t by $\sqrt{N}y'$.

Corollary 1.37 *Let $p|\Delta$ be an odd prime. Then for all $m, n \in R(f)$ with $p \nmid mn$ we have*

$$\left(\frac{m}{p}\right) \;=\; \left(\frac{n}{p}\right). \tag{1.70}$$

Proof. By (1.67) we have $4mn \equiv A^2 \pmod{p}$, so $A \not\equiv 0 \pmod{p}$. Thus $1 = \left(\frac{A^2}{p}\right) = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$, and hence (1.70) follows.

If $2|\Delta$, then (in certain cases) a similar result is true. To be able to write this is a uniform way, it is useful to introduce the following terminology and notation.

Notation. If $p > 2$ is an odd prime, then put $p^* = (-1)^{\frac{p-1}{2}}p$. We call

$$\mathcal{P}^* = \{-4, 8, -8\} \;\cup\; \{p^* : p > 2 \text{ is an odd prime}\}$$

the set of *prime discriminants*. If $\Delta \equiv 0, 1 \pmod 4$ is any discriminant, then its set of *discriminental prime divisors* is

$$\mathcal{P}^*(\Delta) = \{d \in \mathcal{P}^* : d|\Delta \text{ and } \frac{\Delta}{d} \equiv 0, 1 \pmod 4\}.$$

Thus, if we put $\mathcal{P}_2^*(\Delta) = \mathcal{P}^*(\Delta) \cap \{-4, \pm 8\}$, then we have that

$$\mathcal{P}^*(\Delta) = \{p^* : p|\Delta, p > 2\} \cup \mathcal{P}_2^*(\Delta).$$

Moreover, it is easy to see that $\mathcal{P}_2^*(\Delta)$ is given explicitly by the following rules: if $\Delta \equiv 1 \pmod 4$, then $\mathcal{P}^*(\Delta) = \emptyset$, whereas if $\Delta \equiv 0 \pmod 4$, then

$$\mathcal{P}_2^*(\Delta) = \begin{cases} \emptyset & \text{if } \frac{\Delta}{4} \equiv 1, 5 \pmod 8 \\ \{8\} & \text{if } \frac{\Delta}{4} \equiv 2 \pmod 8 \\ \{-4\} & \text{if } \frac{\Delta}{4} \equiv 3, 4, 7 \pmod 8 \\ \{-8\} & \text{if } \frac{\Delta}{4} \equiv 6 \pmod 8 \\ \{4, \pm 8\} & \text{if } \frac{\Delta}{4} \equiv 0 \pmod 8 \end{cases} \tag{1.71}$$

If d is a discriminant and if $d|\Delta$, then we let

$$\chi_d^\Delta :\in (\mathbb{Z}/\Delta\mathbb{Z})^\times \to \{\pm 1\})$$

denote the lift of the homomorphism $\chi_d : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ of Proposition 1.26 via the canonical map $(\mathbb{Z}/\Delta\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$. (Recall from the proof of Proposition 1.26 that the lift of χ_d to $\mathbb{Z}$ is the Kronecker-Jacobi symbol.)

For later use, let us observe that for a prime discriminant $d \in \mathcal{P}^*$, and a positive integer $a > 0$ with $(a, d) = 1$, the character χ_d is determined explicitly by the following formulae (cf. Hua, p. 305, 44):

$$\chi_{-4}(a) = (-1)^{\frac{a-1}{2}} \tag{1.72}$$

$$\chi_8(a) = (-1)^{\frac{a^2-1}{8}} \tag{1.73}$$

$$\chi_{-8}(a) = \chi_{-4}(a)\chi_8(a), \tag{1.74}$$

$$\chi_{p^*}(a) = \left(\frac{a}{p}\right), \quad \text{if } p > 2, \tag{1.75}$$

where the last formula follows from the Quadratic Reciprocity laws (1.61) and (1.59).

Definition. Put $\mathcal{G}^*(\Delta) = \{\chi_d^\Delta : d \in \mathcal{P}^*(\Delta)\} \subset \mathrm{Hom}((\mathbb{Z}/\Delta)^\times, \{\pm 1\})$. Then the set of *generic characters* of Δ is

$$\mathcal{G}(\Delta) = \{\chi_d^\Delta : d \in \mathcal{P}(\Delta)\}, \quad \text{where } \mathcal{P}(\Delta) = \begin{cases} \mathcal{P}^*(\Delta) & \text{if } \Delta \not\equiv 0 \pmod{32} \\ \mathcal{P}^*(\Delta) \setminus \{-8\} & \text{if } \Delta \equiv 0 \pmod{32}. \end{cases}$$

Moreover, the group $\mathcal{G}_\Delta := \langle \mathcal{G}(\Delta) \rangle = \langle \mathcal{G}^*(\Delta) \rangle$ generated by $\mathcal{G}(\Delta)$ or by $\mathcal{G}^*(\Delta)$ (cf. (1.74)) is called the *group of genus characters* mod Δ.

Remark 1.15 (a) It is clear from the definitions and (1.71) that we have

$$\#\mathcal{G}(\Delta) \;=\; \#\mathcal{P}(\Delta) \;=\; \begin{cases} \omega(\Delta)-1 & \text{if } \Delta \equiv 4, 20 \pmod{32} \\ \omega(\Delta)+1 & \text{if } \Delta \equiv 0 \pmod{32} \\ \omega(\Delta) & \text{otherwise,} \end{cases} \tag{1.76}$$

where $\omega(\Delta) = \#\{p|\Delta\}$ denotes the number of distinct prime divisors of Δ.

(b) The subgroup $\mathcal{G}_\Delta \leq \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$ of genus characters is sometimes a *proper* subgroup; more precisely, we have that its index is

$$[\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\}) : \mathcal{G}_\Delta] \;=\; \begin{cases} 2 & \text{if } \Delta \equiv 4, 8, 16, 20, 24 \pmod{32} \\ 1 & \text{otherwise.} \end{cases} \tag{1.77}$$

To see this, note first that

$$|\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})| = \begin{cases} 2^{\omega(\Delta)+1} & \text{if } 8|\Delta \\ 2^{\omega(\Delta)} & \text{otherwise.} \end{cases} \tag{1.78}$$

To verify (1.78), we shall use the fact that for any finite abelian group A (written additively) we have that

$$|\mathrm{Hom}(A,\, \mathbb{Z}/2\mathbb{Z})| \;=\; |\mathrm{Hom}(A/2A,\, \mathbb{Z}/2\mathbb{Z})| \;=\; |A/2A|. \tag{1.79}$$

Indeed, the first equation of (1.79) is trivial and the second follows from the duality theory of $\mathbb{F}_2$-vector spaces (by viewing $V^* = \mathrm{Hom}(A/2A, \mathbb{Z}/2\mathbb{Z})$ as the dual space of the $\mathbb{F}_2$-vector space $V = A/2A$ and noting that $|V^*| = 2^{\dim V^*} = 2^{\dim V} = |V|$).

From this the assertion (1.78) follows by applying the Chinese Remainder Theorem to $A = (\mathbb{Z}/\Delta\mathbb{Z})^\times$ and observing that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic except when $8|p^r$ (in which case $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$).

We observe that the last argument (together with (1.74)) also shows that

$$\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\}) \;=\; \langle \chi_d^\Delta : d \in \mathcal{P}^*, d|\Delta \rangle \;=\; \langle \chi_d^\Delta : d \in \mathcal{P}^*, d|\Delta, d \neq -8 \rangle. \tag{1.80}$$

(Indeed, this is clear if $\Delta = \pm p^r$, where p is a prime, and so the general case follows by the Chinese Remainder Theorem.) Thus, if we view (as above) $\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$ as a (multiplicatively written) $\mathbb{F}_2$-vector space, then it follows from (1.80) and (1.79) that $\{\chi_d^\Delta : d \in \mathcal{P}^*, d|\Delta, d \neq -8\}$ is a basis of $\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$, and that hence $\mathcal{G}(\Delta)$ is a linearly independent set. Thus

$$|\mathcal{G}_\Delta| \;=\; 2^{\#\mathcal{G}(\Delta)}, \tag{1.81}$$

and so the assertion (1.77) follows by comparing (1.78) with (1.76).

We can now generalize Corollary 1.37 as follows.

Corollary 1.38 *If $\Delta(f) = \Delta$ and $d \in \mathcal{P}^*(\Delta)$, then*

$$\chi_d(m) \;=\; \chi_d(n), \quad \textit{for all } m, n \in R(f) \;\; \textit{with } (mn, d) = 1. \tag{1.82}$$

Proof. If $d = p^*$, where $p|\Delta$ is an odd prime, then (1.75) shows that this is just Corollary 1.37. Thus, assume that $d \in \mathcal{P}_2^*(\Delta)$, so $4|\Delta$. Then $f = [a, b, c]$ with $2|b$, so $2|A$ in (1.68), and hence we can write (1.67) in the form

$$mn = (A/2)^2 - \frac{\Delta}{4}B^2, \quad \text{for } m, n \in R(f).$$

If $d = -4$, then the hypothesis $d \in \mathcal{P}^*(\Delta)$ means that $-\frac{\Delta}{4} \equiv 0, 1 \pmod 4$, and so $mn \equiv (A/2)^2$ or $(A/2)^2 + B^2 \pmod 4$, and hence $mn \equiv 1 \pmod 4$ since $2 \nmid mn$. Thus $\chi_{-4}(mn) = 1$ and so (1.82) holds in this case.

Now suppose that $d = \pm 8$. Then $\frac{\Delta}{4}$ is even, so $\frac{A}{2}$ is odd. Thus, if B is even or if $\Delta \equiv 0 \pmod{32}$, then $mn \equiv (\frac{A}{2})^2 \equiv 1 \pmod 8$, and so $\chi_d(mn) = 1$. On the other hand, if B is odd and $\Delta \not\equiv 0 \pmod{32}$, then for $d = 8$ the hypothesis $d \in \mathcal{P}^*(\Delta)$ implies (cf. (1.71)) that $\frac{\Delta}{4} \equiv 2 \pmod 8$, and so $mn \equiv 1 - 2 \cdot 1 \equiv 7 \pmod 8$ and $\chi_8(mn) = 1$, whereas for $d = -8$ we have by (1.71) that $\frac{\Delta}{4} \equiv 6 \pmod 8$, and so $mn \equiv 1 - 6 \cdot 1 \equiv 3 \pmod 8$ and $\chi_{-8}(mn) = 1$. Thus $\chi_d(mn) = 1$ in all cases, and so (1.82) follows.

By the above corollary we see that the value $\chi_d(n) = \pm 1$ does not depend on the choice of $n \in R(f)$ with $(n, d) = 1$, and hence is an "invariant" of the form f. However, before we can define it as such, we need to guarantee that there is at least one $n \in R(f)$ with $(n, d) = 1$. To this end we prove more generally:

Proposition 1.39 *If f is primitive, then for any integer $d \geq 1$ there exists $n \in R(f)$ such that $(n, d) = 1$.*

Proof. Let $f = [a, b, c]$ and consider following sets of prime divisors of d:

$$\mathcal{P}_1 := \{p|(a, c, d)\},\ \mathcal{P}_2 := \{p|(a, d), p \nmid c\},\ \mathcal{P}_3 := \{p|(c, d), p \nmid d\},\ \mathcal{P}_4 := \{p|d, p \nmid a, p \nmid c\}.$$

Clearly $\{p|d\} = \mathcal{P}_1 \dot\cup \mathcal{P}_2 \dot\cup \mathcal{P}_3 \dot\cup \mathcal{P}_4$. Put $x_i = \prod_{p \in \mathcal{P}_i} p$. Then $n = f(x_2, x_3x_4) \in R(f)$ satisfies $(n, d) = 1$, as is straightforward (but somewhat tedious) to check.

Notation. If f is a primitive form of discriminant Δ and if $d \in \mathcal{P}^*(\Delta)$, then we write

$$\chi_d(f) = \chi_d(n), \quad \text{for any } n \in R(f) \text{ with } (n, d) = 1; \tag{1.83}$$

this value $\chi_d(f) = \pm 1$ exists by Proposition 1.39 and is independent of the choice of n by Corollary 1.38. We call $\chi_d(f)$ the *assigned value* of χ_d for f.

Remark 1.16 The set $\underline{\chi}(f) := \{(d, \chi_d(f)) : d \in \mathcal{P}(\Delta)\}$ is essentially the same as what Gauss[DA], Art. 231, called the "total character of the form" f. Note that we can view $\underline{\chi}(f)$ as the *graph* of the map $\chi_f : \mathcal{G}(\Delta) \to \{\pm 1\}$ defined by $\chi_f(d) = \chi_d(f)$. Moreover, since $\{\chi_d^\Delta : d \in \mathcal{G}(\Delta)\}$ is a basis of the group $\mathcal{G}_\Delta$ of genus characters (cf. Remark 1.15(b)), χ_f gives rise to a unique homomorphism (character) $\tilde\chi_f : \mathcal{G}_\Delta \to \{\pm 1\}$ such that $\tilde\chi_f(\chi_d^\Delta) = \chi_d(f)$. It is interesting to observe that the term "character" (which means a $\mathbb{C}$-valued homomorphism on a group) originated with this usage of Gauss.

Example 1.9 (a) The principal form $f = 1_\Delta$ represents 1, so its "total character" is $\underline{\chi}(1_\Delta) = \{(d, 1) : d \in \mathcal{P}(\Delta)\}$.

(b) For $\Delta = -15$ we have $\mathcal{P}(\Delta) = \{-3, 5\}$. The form $f = [2, 1, 2]$ has discriminant $\Delta(f) = -15$ and "total character" $\underline{\chi}(f) = \{(-3, -1), (5, -1)\}$ because $2 \in R(f)$ and so $\chi_{-3}(f) = \chi_{-3}(2) = \left(\frac{2}{3}\right) = -1$ and $\chi_5(f) = \chi_5(2) = \left(\frac{2}{5}\right) = -1$.

(c) For $\Delta = -20$ we have $\frac{\Delta}{4} = -5 \equiv 3 \pmod 8$, and so $\mathcal{P}(\Delta) = \{-4, 5\}$. The form $f = [2, 2, 3]$ has discriminant $\Delta(f) = -20$ and "total character" $\underline{\chi}(f) = \{(-4, -1), (5, -1)\}$ because $3 \in R(f)$ and hence $\chi_{-4}(f) = \chi_{-4}(3) = (-1)^{(3-1)/2} = -1$ and $\chi_5(f) = \left(\frac{3}{5}\right) = -1$.

(d) For $\Delta = 60$ we have $\mathcal{P}(\Delta) = \{-3, 5, 8\}$ because $\frac{\Delta}{4} = 15 \equiv 7 \pmod 8$. On the other hand, for $\Delta = -60$ we have $\mathcal{P}(\Delta) = \{-3, 5\}$ because $\frac{\Delta}{4} = -15 \equiv 1 \pmod 8$. Thus, for $f = [3, 0, 5]$ we have $\Delta(f) = -60$ and $\underline{\chi}(f) = \{(-3, -1), (5, -1)\}$ because $3, 5 \in R(f)$ and $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 = \left(\frac{3}{5}\right)$.

A key new concept which was introduced by Gauss is the following.

Definition. Two primitive forms f_1 and f_2 are said *to lie in the same genus* (or are *genus equivalent*) if we have

$$\Delta(f_1) \;=\; \Delta(f_2) \quad \text{and} \quad \underline{\chi}(f_1) = \underline{\chi}(f_2).$$

(If $\Delta(f_i) < 0$, then we also require that both are positive forms.) We write $f_1 \simeq f_2$ if f_1 and f_2 are genus equivalent and call the set $\text{gen}(f_1) := \{f_2 : f_2 \simeq f_1\}$ the *genus*[9] of f.

Remark 1.17 If $f_1 \approx f_2$, then $\Delta(f_1) = \Delta(f_2)$ and $R(f_1) = R(f_2)$ and hence $f_1 \simeq f_2$, if f_1 and f_2 are primitive. In other words:

$$f_1 \sim f_2 \quad \Rightarrow \quad f_1 \approx f_2 \quad \Rightarrow \quad f_1 \simeq f_2. \tag{1.84}$$

Thus, we see that $\text{gen}(f) = \bigcup_{f_1 \simeq f} cl(f_1)$ is a union of proper equivalence classes (of the same discriminant). Since the total number $h(\Delta(f))$ of such classes is finite, it follows that the genus of f has the form

$$\text{gen}(f) \;=\; cl(f_1) \,\dot\cup\, cl(f_2) \,\dot\cup\, \ldots \,\dot\cup\, cl(f_c)$$

for some (unique) integer $c = c(f) = \#\text{gen}(f)/\!\sim$, called the *class number* of the form f. Clearly, $c(f) \le h(\Delta)$.

Moreover, since $\simeq$ is an equivalence relation, we also have

$$Q_\Delta \;=\; \text{gen}(f_1') \,\dot\cup\, \text{gen}(f_2') \,\dot\cup\, \ldots \,\dot\cup\, \text{gen}(f_g')$$

for suitable forms $f_1', \ldots, f_g' \in Q_\Delta$. We call $g(\Delta) := g = \#Q_\Delta/\!\simeq$ the *number of genera* of discriminant Δ. Note that $g(\Delta) \le h(\Delta)$.

[9] Genus(lat.) = race, stock, kind. In English (cf. Oxford dictionary) it means a grouping of organisms having a common characteristic.

The following result explains Gauss's refinement of Lagrange's method.

Proposition 1.40 *Let $f \in Q_\Delta$ and let n be an integer with $(n, \Delta) = 1$.*

(a) *If $n \in R(f)$, then*

$$\left(\frac{\Delta}{p}\right) = 1, \quad \text{for all primes } p|n, \tag{1.85}$$

$$\chi_d(n) = \chi_d(f), \quad \text{for all } d \in \mathcal{P}(\Delta). \tag{1.86}$$

(b) *Conversely, if* (1.85) *and* (1.86) *hold (and if $n > 0$ when $\Delta < 0$), then there is a form $f' \in Q_\Delta$ which is genus-equivalent to f (i.e. $f' \simeq f$) such that $n \in R(f')$.*

Proof. (a) Equation (1.86) follows directly from the definition of the symbol $\chi_d(f)$. Moreover, by Corollary 1.7 we have $\#\mathrm{Sqrt}(\Delta, 4n) > 0$ and so $\#\mathrm{Sqrt}(\Delta, 4p) > 0, \forall p|n$. Thus, (1.85) holds; cf. (1.54).

(b) Using (1.54) and (1.53), we see that (1.85) implies that $\exists x \in \mathbb{Z}$ such that $x^2 \equiv \Delta \pmod{4n}$, and so there exists $f' = [n, x, c]$ such that $\Delta(f') = \Delta(f)$. Clearly $n \in R(f')$, so $\chi_d(f') = \chi_d(n)$, for all $d \in \mathcal{P}(\Delta)$. By (1.86) we have $\chi_d(f) = \chi_d(n) = \chi_d(f')$, for all $d \in \mathcal{P}(\Delta)$, and so $f' \simeq f$.

From this we obtain the following refinement of Corollary 1.33:

Corollary 1.41 *Let $f \in Q_\Delta$ and $n \in R(f)$ with $(n, \Delta) = 1$ and $n > 0$. Then*

$$\sum_{f_i \in \mathrm{gen}(f)/\sim} \#(\mathrm{Aut}^+(f_i) \backslash P(f_i, n)) = 2^{\omega(n)}. \tag{1.87}$$

Proof. Since $n \in R(f)$ and $(n, \Delta) = 1$ it follows from (1.55) that $\left(\frac{\Delta}{p}\right) = 1$, for all $p|n$, and so the right hand side of (1.66) equals $2^{\omega(n)}$. On the other hand, the sum on the left hand side of (1.66) need to be taken only over those f_i's such that $P(f_i, n) \neq \emptyset$, and for each such f_i we have (as in the proof of Proposition 1.40(b)) that $f_i \simeq f$.

Corollary 1.42 *If $c(f) = 1$, then the set of primes in $R(f)$ can be characterized by congruence conditions mod $\Delta(f)$.*

Proof. By an argument similar to that of Proposition 1.24, we see from Proposition 1.40 that for a prime $p \nmid \Delta(f)$ we have

$$p \in R(f) \Leftrightarrow \left(\frac{\Delta}{p}\right) = 1 \text{ and (1.86) holds for } n = p. \tag{1.88}$$

By Proposition 1.26, both conditions can be expressed in terms of congruence conditions mod Δ, and so the assertion follows.

The following example was studied by Euler, who discovered the result empirically but was unable to prove it; cf. [We], p. 214.

Example 1.10 (Euler) Let $f = x^2 + 5y^2$ and suppose p is a prime. Then

$$p \in R(f) \quad \Leftrightarrow \quad p = 5 \text{ or } p \equiv 1, 9 \pmod{20}.$$

Here $\Delta(f) = -20$. Since $\sqrt{\frac{20}{3}} < 3$, we see that the only reduced forms are $f = [1, 0, 5]$ and $f_2 = [2, 2, 3]$, and so $Q_{-20} = cl(f) \dot{\cup} cl(f_2)$. By Example 1.9 we know that $\mathcal{P}(-20) = \{-4, 5\}$ and that $\underline{\chi}(f) = \{(-4, 1), (5, 1)\}$ and $\underline{\chi}(f_2) = \{(-4, -1), (5, -1)\} \neq \underline{\chi}(f)$. Thus $\text{gen}(f) \neq \text{gen}(f_2)$ and hence (cf. Remark 1.17)

$$\text{gen}(f) = cl(f) \quad \text{and} \quad \text{gen}(f_2) = cl(f_2);$$

in particular, $c(f) = c(f_2) = 1$. We can thus apply Corollary 1.42 to obtain for $p \nmid 20$:

$$p \in R(f) \Leftrightarrow \left(\tfrac{-20}{p}\right) = 1,\ \chi_5(p) = 1, \chi_{-4}(p) = 1 \Leftrightarrow \left(\tfrac{-20}{p}\right) = 1,\ \left(\tfrac{p}{5}\right) = 1,\ (-1)^{\frac{p-1}{2}} = 1.$$

Now $\left(\frac{5}{p}\right) = 1$ and $(-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv \pm 1 \pmod 5$ and $p \equiv 1 \pmod 4 \Leftrightarrow p \equiv 1, 9 \pmod{20}$. If this is the case, then also $\left(\frac{-20}{p}\right) = 1$ because $\left(\frac{-20}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$, and so we see that all three conditions reduce to $p \equiv 1, 9 \pmod{20}$, and hence the above characterization of primes in $R(f)$ follows since $5 = 0^2 + 5 \cdot 1^2$ and $2 \notin R(f)$.

Remark 1.18 (a) In view of the above Corollary 1.42, it is natural to ask:

Question. For which forms f is $c(f) = 1$?

Since $c(f) \leq h(\Delta(f))$, this question is partially related to the class number 1 question discussed in Remark 1.14. In particular, it follows from Gauss's conjecture that there are infinitely many $\Delta > 0$ such that $c(f) = h(\Delta) = 1$.

If $\Delta < 0$, then the question is more delicate and is still not completely resolved (despite what Buell[Bu] claims on p. 81).

Gauss showed (as we shall see in Corollary 1.47 below) that $c(f) = h(\Delta)/g(\Delta)$; in particular, $c(f) = c(\Delta)$ depends only on $\Delta = \Delta(f)$. He also observed that if $\Delta = -4D$, then for $D \leq 3000$ there are precisely 65 values of D for which $c(-4D) = 1$: all D's up to 18 except for $D = 11, 14, 17$ and 40 others: $D = 21, 22, 24, 25, 28, 30, \ldots, 1320, 1365, 1848$. These were precisely the *idoneal numbers* (or *numeri idonei*) that were considered by Euler in another context; cf. Remark 1.18 (b) below. Gauss stated in Article 303 of [DA] the following conjecture:

Conjecture. $c(-4D) = 1,\ D > 0 \ \Leftrightarrow\ D$ is one of the 65 idoneal numbers of Euler.

This conjecture, together with its natural extension to odd discriminants, is *almost* proved. Chowla(1934), using a variant of Heilbronn's method (cf. Remark 1.14), showed that there are only finitely many Δ's with $c(\Delta) = 1$ (in fact, he proved that $c(\Delta) \to \infty$ as $\Delta \to -\infty$), and Weinberger (1973) showed that there is at most one more (fundamental)

discriminant. Moreover, he showed that the Generalized Riemann Hypothesis implies that Gauss's Conjecture is true.

(b) In 1776 Euler considered numbers $N > 0$ which have the following property:

If $m > 1$ is a number with $(m, 4N) = 1$ such that $m = x^2 + Ny^2$ has a unique solution with $x, y \geq 0$ and if that solution is proper, then m is prime.[10]

He called such numbers "idoneal" (= suitable, convenient) because he was able to use them in his *primality criterion* for finding large prime numbers. In addition, he used them his factorization method of numbers; cf. [We], p. 188, 223ff, [Di] I, p. 362 and [Bu], p. 191ff. One has the following result (cf. [Cox], p. 61):

$$N > 0 \text{ is idoneal} \quad \Leftrightarrow \quad c(1_{-4N}) = 1.$$

Indeed, one direction ($\Leftarrow$) follows easily from Corollary 1.41 (cf. also Corollary 1.35). However, the other direction is more difficult since it requires Dirichlet's Theorem (completed by Weber) that each $f \in Q_{-4N}$ represents infinitely many primes.

1.4.2 Composition

In the previous subsection we saw how the identity (1.67) gave us important information about quadratic forms. Here we shall generalize this idea by looking at *all* possible identities between quadratic forms. This naturally leads to Gauss's theory of composition of forms which in turn sheds new light on the previous theory of genera.

Definition. Two binary quadratic forms f_1 and f_2 are said to be *composable*[11] if there is a binary quadratic form f_3 and an integral 2×4 matrix P such that

$$f_1(x_1, y_1) f_2(x_2, y_2) \; = \; f_3(x, y), \tag{1.89}$$

where x, y are determined by the matrix equation

$$(x, y)^t \; = \; P(x_1x_2,\, y_1x_2,\, x_1y_2,\, y_1y_2)^t. \tag{1.90}$$

We let $C(f_1, f_2) = \{(f_3, P) : \text{ (1.89) and (1.90) hold}\}$ denote the set of pairs (f_3, P) which satisfy these equations.

Remark 1.19 (a) The identity (1.67) shows that if $f = [a, b, c]$ is any form, then $2f$ is composable with itself. Here $(f_3, P) \in C(2f, 2f)$ is given by

$$f_3 = x^2 - \Delta y^2 \quad \text{and} \quad P = \begin{pmatrix} 2a & b & b & 2c \\ 0 & 1 & -1 & 0 \end{pmatrix}.$$

(b) The above equation (1.89) can be re-written in matrix form by using the matrices $A(f_i)$ associated to f_i. For this, it is useful to observe that the vector $(x_1x_2, y_1x_2, x_1y_2, y_1y_2)^t$

[10] Note that the definition given in [Di] I, p. 361, is incorrect.

[11] Gauss[DA], Art. 235, uses here the terminology that f_3 is *transformable* into $f_1 f_2$.

on the right hand side of (1.90) can be written as a *Kronecker product* or *tensor product* of the 2×1 matrices (column vectors) $\vec{x}_i = (x_i, y_i)^t$:

$$(x_1x_2,\ y_1x_2,\ x_1y_2,\ y_1y_2)^t = \vec{x}_2 \otimes \vec{x}_1. \tag{1.91}$$

[Recall that if $A_k = (a_{ij}^{(k)})$ is an $m_k \times n_k$ matrix (where $k = 1, 2$), then the Kronecker/tensor product $A_1 \otimes A_2$ is the $(m_1m_2) \times (n_1n_2)$ matrix defined by $A_1 \otimes A_2 = (A_1 a_{ij}^{(2)})$; cf. [BA], ch. II, §10.10, p. 357.] Thus, since $f_i(\vec{x}_i) = \frac{1}{2}\vec{x}_i^t A(f_i)\vec{x}_i$, we see that (1.89) and (1.90) can be re-written as

$$\tfrac{1}{2}(\vec{x}_1^t A(f_1)\vec{x}_1)(\vec{x}_2^t A(f_2)\vec{x}_2) \ = \ (\vec{x}_2 \otimes \vec{x}_1)^t P^t A(f_3) P(\vec{x}_2 \otimes \vec{x}_1). \tag{1.92}$$

From this matrix equation we see immediately that if $T \in M_2(\mathbb{Z})$, then

$$(f_3, TP) \in C(f_1, f_2) \ \Rightarrow \ (f_3T, P) \in C(f_1, f_2) \tag{1.93}$$

because $A(f_3T) = T^t A(f_3)T$. In particular, if $T \in \mathrm{GL}_2(\mathbb{Z})$, then

$$(f_3, P) \in C(f_1, f_2) \ \Leftrightarrow \ (f_3T, T^{-1}P) \in C(f_1, f_2). \tag{1.94}$$

In addition, we see that if $f_i' = T_i f_i$, $T_i \in M_2(\mathbb{Z})$, for $i = 1, 2$, then

$$(f_3, P) \in C(f_1, f_2) \ \Rightarrow \ (f_3, P(T_2 \otimes T_1)) \in C(f_1', f_2'). \tag{1.95}$$

[Indeed, since $A(f_i') = T_i^t A(f_i) T_i$ and since $(T_2\vec{x}_2) \otimes (T_1\vec{x}_1) = (T_2 \otimes T_1)(\vec{x}_2 \otimes \vec{x}_1)$, the assertion follows easily by replacing $\vec{x}_i$ in (1.92) by $T_i\vec{x}_i$.]

We observe the following fundamental fact.

Proposition 1.43 *If $(f_3, P) \in C(f_1, f_2)$, then there are rational numbers $n_i \in \mathbb{Q}^\times$ such that*

$$\Delta(f_i) \ = \ n_i \Delta(f_3), \quad \textit{for } i = 1, 2. \tag{1.96}$$

Thus, if f_1 and f_2 are composable, then $\Delta(f_1)/\Delta(f_2) \in (\mathbb{Q}^\times)^2$.

Proof. Since the last assertion follows immediately from (1.96), it is enough to verify (1.96). For this, write $P = (P_1|P_2)$, where $P_i \in M_2(\mathbb{Z})$. If $\vec{x}_2 \in \mathbb{Z}^2$, then $P_{\vec{x}_2} := (P_1\vec{x}_2|P_2\vec{x}_2) \in M_2(\mathbb{Z})$ and we have the identity

$$P(\vec{x}_2 \otimes \vec{x}_1) = P_{\vec{x}_2}\vec{x}_1, \quad \text{for all } \vec{x}_1 \in \mathbb{Z}^2, \tag{1.97}$$

as is easy to verify. Thus, if we fix $\vec{x}_2$ and put $m_2 = f_2(\vec{x}_2)$, then we obtain from (1.89) that $m_2 f_1(\vec{x}_1) = f_3(P_{\vec{x}_2}\vec{x}_1)$, $\forall \vec{x}_1 \in \mathbb{Z}^2$. We therefore obtain

$$m_2 f_1 \ = \ f_3 P_{\vec{x}_2} \ \text{ and hence } \ m_2^2 \Delta(f_1) \ = \ \det(P_{\vec{x}_2})^2 \Delta(f_3), \quad \text{if } m_2 = f_2(\vec{x}_2). \tag{1.98}$$

In particular, choosing $\vec{x}_2$ such that $m_2 = f_2(\vec{x}_2) \neq 0$, we see that $\det(P_{\vec{x}_2}) \neq 0$ (because $\Delta(f_1) \neq 0$) and so (1.96) holds for $i = 1$ with $n_1 = \det(P_{\vec{x}_2})/m_2 \neq 0$.

In similar manner we can prove that (1.96) holds for $i = 2$. In this case, however, the identity (1.97) has to be replaced by the identity

$$P(\vec{x}_2 \otimes \vec{x}_1) = \tilde{P}_{\vec{x}_1}\vec{x}_2, \quad \text{for all } \vec{x}_2 \in \mathbb{Z}^2, \tag{1.99}$$

where $\tilde{P}_{\vec{x}_1} = (\tilde{P}_1\vec{x}_1, \tilde{P}_2\vec{x}_1)$ with $\tilde{P}_1 = (\vec{p}_1|\vec{p}_3)$ and $\tilde{P}_2 = (\vec{p}_2|\vec{p}_4)$ for $P = (\vec{p}_1|\vec{p}_2|\vec{p}_3|\vec{p}_4)$.

Remark. Gauss[DA] showed in Article 236 that the converse of the last statement of Proposition 1.43 holds: if $\Delta(f_1) = t^2\Delta(f_2)$, for some $t \in \mathbb{Q}^\times$, then f_1 and f_2 are composable; cf. Proposition 1.46 below. We shall give another proof of this fact in chapter 2; cf. Corollary 2.26.

In studying the set of solutions $C(f_1, f_2)$, we shall now restrict our attention to matrices P which are *primitive* in the following sense.

Definition. Let P be an $m \times n$ matrix with $m \leq n$. The *content* of P is

$$\mathrm{cont}(P) \;=\; \gcd(\det(P_I) : I \subset \{1, \ldots, n\}, \#I = m), \tag{1.100}$$

where $P_I = (\vec{p}_{i_1}| \ldots |\vec{p}_{i_m})$ denotes the $m \times m$ submatrix of $P = (\vec{p}_1| \ldots |\vec{p}_n)$ with columns indexed by $I = \{i_1, i_2, \ldots, i_m\}$. If $\mathrm{cont}(P) = 1$, then we call P *primitive*.

For what follows, it is useful the recall the following basic fact from linear algebra (cf. [BA], ch. VII, §4, Corollaries 1 and 2 of Proposition 5 or [La3], p. 153-5).

Theorem 1.5 (Invariant Factor Theorem) *Let A be an integral $m \times n$ matrix of rank r. Then:*

(a) *There are invertible matrices $T_1 \in \mathrm{GL}_m(\mathbb{Z})$ and $T_2 \in \mathrm{GL}_n(\mathbb{Z})$ such that*

$$T_1 A T_2 \;=\; \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \tag{1.101}$$

where $D = \mathrm{diag}(a_1, a_2, \ldots, a_r)$ is a diagonal integral $r \times r$ matrix whose entries are positive and satisfy the condition $a_1|a_2| \ldots |a_r$.

(b) *The above integers $a_1, \ldots a_r$, called the* invariant factors *of A, are uniquely determined by A because we have*

$$\delta_k \;:=\; a_1 \ldots a_k \;=\; \gcd(\{k \times k \text{ minors of } A\}), \quad \text{for } k = 1, \ldots, r. \tag{1.102}$$

(c) *If B is another integral $m \times n$ matrix, then $B = T_1 A T_2$ for some $T_1 \in \mathrm{GL}_m(\mathbb{Z})$ and $T_2 \in \mathrm{GL}_n(\mathbb{Z})$ (i.e. B is* equivalent *to A) if and only if A and B have the same list of invariant factors. In particular, the equivalence class of A is determined by the numbers δ_k.*

Remark 1.20 (a) The existence of T_1 and T_2 in part (a) is established by a (careful) row and column reduction procedure (using the Euclidean algorithm).

(b) According to Bourbaki[BA], p. VII.76, this theorem was first stated in 1868 by E. Schering, the editor of Gauss's collected works, and then in more abstract form by L. Kronecker in 1870.

(c) It follows from this theorem that if $f : \mathbb{Z}^n \to \mathbb{Z}^m$ is a linear map with associated matrix A of rank m, then $\mathrm{cont}(A) = [\mathbb{Z}^n : \mathrm{Im}(f)]$; cf. exercises. In particular, A is primitive if and only if f is surjective.

(d) We also observe that if A is an integral $m \times n$ matrix of rank m, then we can write $A = BP$, where P is primitive and $B \in M_m(\mathbb{Z})$ is a suitable $m \times m$ integral matrix with $|\det(B)| = \mathrm{cont}(A)$.
[Indeed, by Theorem 1.5(a) we have $A = T_1^{-1}(D|0)T_2^{-1} = T_1^{-1}D(I|0)T_2^{-1} = BP$, where $P = (I|0)T_2^{-1}$ is primitive and $B = T_1^{-1}D$ satisfies $\det(B) = \pm\det(D) = \pm\mathrm{cont}(A)$.]

Proposition 1.44 *If f_1 and f_2 are composable, then there exists $(f_3, P) \in C(f_1, f_2)$ such that P is primitive.*

Proof. By hypothesis, $\exists (f_3', P') \in C(f_1, f_2)$. By the above Remark 1.20(d) we have $P' = BP$ with P primitive. Put $f_3 = f_3'B$. Then by (1.93) we see that $(f_3, P) \in C(f_1, f_2)$.

Notation. (a) If $P = (\vec{p}_1|\vec{p}_2|\vec{p}_3|\vec{p}_4)$ is a 2×4 matrix, write $P_{ij} = \det(\vec{p}_i|\vec{p}_j)$. Thus

$$\mathrm{cont}(P) \;=\; \gcd(\{P_{ij} : 1 \le i < j \le 4\}) \;=\; \gcd(P_{12}, P_{13}, P_{14}, P_{23}, P_{24}, P_{34}).$$

(b) If f_1 and f_2 are binary forms, put $a_i = f_i(1, 0)$ and

$$f_1 \circ f_2 = \{f_3 : (f_3, P) \in C(f_1, f_2), \text{ where } P \text{ is primitive and } P_{12}a_1 > 0, P_{13}a_2 > 0\}.$$

Remark 1.21 From (1.94) we see easily that

$$f_3 \in f_1 \circ f_2 \quad \Rightarrow \quad f_2T \in f_1 \circ f_2, \quad \forall T \in \mathrm{SL}_2(\mathbb{Z}). \tag{1.103}$$

Thus $f_1 \circ f_2$ is a (possibly empty) union of proper equivalence classes of forms.

Similarly, from (1.95) we see (with some work) that

$$f_i' \sim f_i,\ i = 1, 2, \quad \Rightarrow \quad f_1' \circ f_2' \;=\; f_1 \circ f_2. \tag{1.104}$$

Proposition 1.45 *If $f_3 \in f_1 \circ f_2$, then $f_1 \circ f_2 = cl(f_3)$, provided that f_i is irreducible, i.e. $\Delta(f_i)$ is not a square. Moreover:*

$$\mathrm{cont}(f_3) = \mathrm{cont}(f_1)\mathrm{cont}(f_2). \tag{1.105}$$

Proof. (Sketch). Let P be the primitive matrix such that $(f_3, P) \in C(f_1, f_2)$, and put

$$\tilde{f}_1^P = [P_{12}, P_{14} - P_{23}, P_{34}] \quad \text{and} \quad \tilde{f}_2^P = [P_{13}, P_{14} + P_{23}, P_{24}]. \tag{1.106}$$

One then shows (cf. [Bu], p. 121-2) that

$$\tilde{f}_1^P = n_2 f_1 \quad \text{and} \quad \tilde{f}_2^P = n_1 f_2, \tag{1.107}$$

where $n_i \in \mathbb{Q}_i^\times$ satisfies (1.96). Note that the conditions $a_1 P_{12} > 0$ and $a_2 P_{13} > 0$ force that $n_i > 0$, for $i = 1, 2$.

Next one verifies (1.105) and that with $d_i = \Delta(f_i)$ and $g_i = \mathrm{cont}(f_i)$ we have

$$\Delta(f_3) \;=\; \gcd(d_1 g_2^2,\, d_2 g_1^2); \tag{1.108}$$

cf. [Bu], p. 125.

Now suppose that $f_3' \in f_1 \circ f_2$ is another element. Then by (1.108) we have $\Delta(f_3') = \Delta(f_3)$. Thus, if P' be the associated primitive matrix, then from (1.96) and (1.107) we see that

$$\tilde{f}_1^{P'} = n_2 f_1 \quad \text{and} \quad \tilde{f}_2^{P'} = n_1 f_2$$

for the *same* n_1 and n_2 as defined above (for P). We thus have $\tilde{f}_i^{P'} = \tilde{f}_i^P$, for $i = 1, 2$ and hence $P_{ij} = P'_{ij}$, for $i < j$. It thus follows from Lemma 1.2 below that $\exists T \in \mathrm{SL}_2(\mathbb{Z})$ such that $TP = P'$. Thus

$$f_3(P(\vec{x}_2 \otimes \vec{x}_1)) = f_1(\vec{x}_1) f_2(\vec{x}_2) = f_3'(P'(\vec{x}_2 \otimes \vec{x}_1)) = (f_3' T)(P(\vec{x}_2 \otimes \vec{x}_1)).$$

Since P is primitive, $P(\vec{x}_2 \otimes \vec{x}_1)$ runs through all vectors of $\mathbb{Z}^2$ (cf. Remark 1.20(c)), and so $f_3' T = f_3$, i.e. $f_3' \in cl(f_3)$. Thus $f_1 \circ f_2 = cl(f_3)$, as claimed.

Remark 1.22 The above proof also shows that if $f_3 \in f_1 \circ f_2$, then the associated primitive matrix P is uniquely determined by f_3 (and by f_1, f_2) up to multiplication by an arbitrary $T \in \mathrm{Aut}^+(f_3)$.

In the above proof of Proposition 1.45 we had used the following result which may be viewed as a partial refinement of Theorem 1.5.

Lemma 1.2 *If P and P' are two integral $2 \times n$ matrices such that P is primitive and $P_{ij} = P'_{ij}$, for all $1 \le i < j \le n$, then there is a matrix $T \in \mathrm{SL}_2(\mathbb{Z})$ such that $TP = P'$.*

Proof. Gauss[DA], Art. 234 or [Bu], pp. 125-7.

We now turn to the *existence* of $f_3 \in f_1 \circ f_2$. This was (essentially) proven by Gauss[DA], who did not, however, give an explicit form f_3. Although Dirichlet(1851) gave f_3 in (sufficiently many) special cases[12], it was Arndt(1859) (cf. [Di], III, p. 67) who gave the following general recipe for f_3.

[12] According to [We], p. 334, these cases had already been given by Legendre; see also [Di], III p. 60ff.

Proposition 1.46 (Gauss/Arndt) *Let $f_i = [a_i, b_i, c_i]$ be two quadratic forms of discriminant $\Delta_i = \Delta(f_i)$. Assume that Δ_1/Δ_2 is a square, so that we can write $\Delta_i = m_i^2\Delta$ with $\gcd(m_1, m_2) = 1$ and $m_i > 0$. Put $\beta := (b_1m_2 + b_2m_1)/2$, and let $t, u, v \in \mathbb{Z}$ be such that*

$$a_1m_2t + a_2m_1u + \beta v \;=\; n \;:=\; \gcd(a_1m_2, a_2m_1, \beta).$$

Put

$$a_3 = \frac{a_1a_2}{n^2}, \quad b_3 = \frac{a_1b_2t}{n} + \frac{a_2b_1u}{n} + \frac{(b_1b_2 + \Delta m_1m_2)v}{2n}, \quad c_3 = \frac{b_3^2 - \Delta}{4a_3}.$$

Then $f_3 = [a_3, b_3, c_3]$ is an integral form of discriminant Δ and $f_3 \in f_1 \circ f_2$. Furthermore, an associated primitive matrix P is

$$P = \begin{pmatrix} n & \frac{n(b_2 - b_3m_2)}{2a_2} & \frac{n(b_1 - b_3m_1)}{2a_1} & \frac{(b_1b_2 + \Delta m_1m_2 - 2b_3\beta)n}{4a_1a_2} \\ 0 & \frac{a_1m_2}{n} & \frac{a_2m_1}{n} & \frac{\beta}{n} \end{pmatrix}.$$

Proof. This is essentially Theorem 7.8 of [Bu], p. 129. Note that $P_{12}a_1 = a_1^2m_2 > 0$, $P_{13}a_2 = a_2^2m_1 > 0$, so that P satisfies the desired positivity conditions.

Gauss used his results on composition to make the set $Cl(\Delta) = Q_\Delta/\sim$ into what we now call an abelian group; cf. [DA], Article 249:

Theorem 1.6 (Gauss) *If Δ is not a square, then the rule $cl(f_1) \cdot cl(f_2) = f_1 \circ f_2$ makes $Cl(\Delta) = Q_\Delta/\sim$ into an abelian group with identity $cl(1_\Delta)$. Furthermore,*

$$cl([a, b, c])^{-1} = cl([a, -b, c]). \tag{1.109}$$

Proof. The fact that this rule defines a well-defined law of composition on $Cl(\Delta)$ follows from Propositions 1.45 and 1.46 (together with Remark 1.21). The rest of the properties are easily verified. Note that (1.109) follows by taking $f_1 = [a, b, c]$, $f_2 = [a, -b, c]$ in Arndt's algorithm. Indeed, since $\beta = 0$ and $n = |a|$, we can take $t = \mathrm{sign}(a)$, $u = v = 0$ and so $f_3 = [1, b, ac] \sim 1_\Delta$, which proves (1.109).

Remark 1.23 The product $cl(f_1)cl(f_2)$ of two classes $cl(f_i) \in Cl(\Delta)$ can be computed by using Arndt's composition law (Proposition 1.46). D. Shanks (1969) has proposed the following alternate method which is more convenient for computer computations.

Let $f_i = [a_i, b_i, c_i] \in Q_\Delta$, and put $\beta = \frac{b_1 + b_2}{2}$. Determine $x, y \in \mathbb{Z}$ such that

$$a_1x + \beta y \;=\; m \;:=\; \gcd(a_1, \beta),$$

and choose $z \in \mathbb{Z}$ such that

$$\frac{m}{n}z \;\equiv\; x\left(\frac{b_1 - b_2}{2}\right) - c_1y \;\left(\mathrm{mod}\; \frac{a_2}{n}\right),$$

where $n := \gcd(m, a_2) = \gcd(a_1, a_2, \beta)$. Put

$$a_3 = \frac{a_1 a_2}{n^2}, \quad b_3 = b_1 + \frac{2a_1 z}{n}, \quad c_3 = \frac{b_3^2 - \Delta}{4a_3}.$$

Then $f_3 = [a_3, b_3, c_3] \in Q_\Delta$ and $cl(f_1)cl(f_2) = cl(f_3)$, as is easy to deduce from Arndt's formula; cf. [Bu], p. 64.

As Gauss realized, the above theorem has important consequences for the number of a classes in a genus.

Corollary 1.47 *If $d \in \mathcal{P}^*(\Delta)$, then the map $f \mapsto \chi_d(f)$ defines a homomorphism*

$$\chi_d^* : Cl(\Delta) \ \to \ \{\pm 1\}.$$

Thus, the principal genus

$$PG(\Delta) \ := \ \mathrm{gen}(1_\Delta)/\sim \ = \ \bigcap_{d \in \mathcal{P}(\Delta)} \mathrm{Ker}(\chi_d^*) \tag{1.110}$$

is a subgroup of $Cl(\Delta)$ and we have

$$\mathrm{gen}(f)/\sim \ = \ cl(f)PG(\Delta), \quad \textit{for all } f \in Q_\Delta. \tag{1.111}$$

Thus, the set of genera can be identified with the quotient group $Cl(\Delta)/PG(\Delta)$ and hence $g(D) = [Cl(\Delta) : PG(\Delta)]$. In addition,

$$c(f) \ = \ |PG(\Delta)| \ = \ \frac{h(\Delta)}{g(\Delta)}, \quad \textit{for all } f \in Q_\Delta. \tag{1.112}$$

Proof. Since $\chi_d(f_1)$ has the same value for all $f_1 \in cl(f)$ by Remark 1.17, the given rule defines a map on $Cl(\Delta)$. We now verify that χ_d^* is a homomorphism. Clearly $\chi_d^*(cl(1_\Delta)) = \chi_d(1) = 1$. Moreover, we have

$$\chi_d(f_1 \circ f_2) \ = \ \chi_d(f_1)\chi_d(f_2), \quad \text{for all } f_1, f_2 \in Q_\Delta.$$

For this, let $f_3 \in f_1 \circ f_2$ and $n_i \in R(f_i)$ with $(n_i, d) = 1$. Then by (1.89) we have $n_1 n_2 = f_3(x, y)$, and so $\chi_d(f_1 \circ f_2) = \chi_d(n_1 n_2) = \chi_d(n_1)\chi_d(n_2) = \chi_d(f_1)\chi_d(f_2)$. We thus see that χ_d^* is a homomorphism.

The equation (1.110) is clear from the definitions. Since the χ_d^*'s are homomorphisms, it follows that $PG(\Delta)$ is a subgroup of $Cl(\Delta)$. Thus

$$\begin{aligned} cl(f_1) \in \mathrm{gen}(f)/\sim \ &\Leftrightarrow \ \chi_d(f_1) = \chi_d(f), \ \forall \chi_d \in \mathcal{G}(\Delta) \ \Leftrightarrow \ \chi_d(f_1 \circ f^{-1}) = 1, \ \forall \chi_d \in \mathcal{G}(\Delta) \\ &\Leftrightarrow \ cl(f_1 \circ f^{-1}) \in PG(\Delta) \ \Leftrightarrow cl(f_1) \in cl(f)PG(\Delta), \end{aligned}$$

and so (1.111) holds. The rest of the assertions follow from the fact that all cosets of a fixed subgroup have the same number of elements.

By the above corollary, the rule $\chi_d \mapsto \chi_d^*$ defines a map from certain characters on $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ to characters on $Cl(\Delta)$. We now examine this map in more detail.

Proposition 1.48 *If $f \in Q_\Delta$, then the set*

$$\bar{S}(f) := \{n \in (\mathbb{Z}/\Delta\mathbb{Z})^\times : n \equiv f(x,y) \pmod{\Delta}, \text{ for some } x, y \in \mathbb{Z}\}$$

is a coset with respect to the subgroup $\bar{S}(1_\Delta) \leq (\mathbb{Z}/\Delta\mathbb{Z})^\times$, and the map $f \mapsto \bar{S}(f)$ defines a homomorphism

$$\bar{S}_\Delta : Cl(\Delta) \ \to \ (\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta).$$

Moreover, for any $d \in \mathcal{P}^*(\Delta)$ we have that $\bar{S}(1_\Delta) \leq \mathrm{Ker}(\chi_d^\Delta)$ and that hence

$$\chi_d^*(f) \ = \ \bar{S}_\Delta^* \chi_d^\Delta(f) \ := \ \chi_d^\Delta(\bar{S}_\Delta(f)), \quad \text{for all } f \in Q_\Delta. \tag{1.113}$$

Proof. We first show that $\bar{S}(1_\Delta)$ is a subgroup of $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. If $\Delta \equiv 0 \pmod 4$, then the identity (1.69) shows that $\bar{S}(1_\Delta)$ is closed under multiplication and hence is a subgroup. If $\Delta \equiv 1 \pmod 4$, then

$$4(1_\Delta(x,y)) = 4\left(x^2 + xy + \frac{1-D}{4}y^2\right) \equiv (2x+y)^2 \pmod{\Delta},$$

and so we see that $\bar{S}(1_\Delta) = ((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2$ is the subgroup of squares $\pmod{\Delta}$.

Next, let $f \in Q_\Delta$ be arbitrary. Then by Proposition 1.39 we know that there exists $a = f(x_0, y_0)$ with $(n, \Delta) = 1$ (so $\bar{S}(f) \neq \emptyset$), and $f \sim f' = [a, b, c]$, for some $b, c \in \mathbb{Z}$. If $\Delta \equiv 0 \pmod 4$, then for any $x, y \in \mathbb{Z}$ we have by (1.5) that $af'(x,y) = (ax + \frac{b}{2}y)^2 - \frac{\Delta}{4}y^2 = 1_\Delta(ax + \frac{b}{2}y, y)$, so $\bar{S}(f) = \bar{S}(f') = a^{-1}\bar{S}(1_\Delta)$ is a coset of $\bar{S}(1_\Delta)$. Similarly, if $\Delta \equiv 1 \pmod 4$, then by (1.5) we have $4af'(x,y) = (2ax+by)^2 - \frac{\Delta}{y}^2 \equiv (2ax+by)^2 \in \bar{S}(1_\Delta)$, and so $\bar{S}(f) = \bar{S}(f') = (4a)^{-1}\bar{S}(1_\Delta) = a^{-1}\bar{S}(1_\Delta)$. This proves the first assertion.

We thus see that the rule $f \mapsto \bar{S}(f)$ defines a map $Q_\Delta \to (\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta)$. Since clearly $\bar{S}(f_1) = \bar{S}(f_2)$, when $f_1 \sim f_2$, it follows that this gives a map $\bar{S}_\Delta : Cl(\Delta) = Q_\Delta/\sim \ \to (\mathbb{Z}/\Delta\mathbb{Z})^\times/S(1_\Delta)$. To see that this is a homomorphism, let $f_1, f_2 \in Q_\Delta$ and let $f_3 \sim f_1 \circ f_2$. Then we have $\bar{S}(f_3) = \bar{S}(f_1)\bar{S}(f_2)$ because if $m_i \in \bar{S}(f_i)$ $(i = 1, 2)$, i.e. $m_i \equiv f_i(x_i, y_i) \pmod{\Delta}$, for some $x_i, y_i \in \mathbb{Z}$, then by (1.89) we have $m_1 m_2 \equiv f_1(x_1, y_1) f_2(x_2, y_2) \equiv f_3(x', y') \pmod{\Delta}$, for some $x', y' \in \mathbb{Z}$. Thus $m_1 m_2 \in \bar{S}(f_3)$ and so the cosets are equal. Thus $\bar{S}_\Delta$ is a homomorphism.

Now if $d \in \mathcal{P}^*(\Delta)$ and $f \in Q_\Delta$, then by definition and/or Corollary 1.38 we have $\chi_d(f) = \chi_d(m) = \chi_d^\Delta(m)$, for all $m \in \bar{S}(f)$ and so (1.113) holds. In particular, taking $f = 1_\Delta$ we see that $\chi_d(\bar{S}(1_\Delta)) = 1$, so $\bar{S}(1_\Delta) \leq \mathrm{Ker}(\chi_d^\Delta)$.

Remark 1.24 We see from (1.113) that the map $\chi_d \mapsto \chi_d^*$ is given by the homomorphism

$$\bar{S}_\Delta^* : \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta), \{\pm 1\}) \ \to \ \mathrm{Hom}(Cl(\Delta), \{\pm 1\})$$

which is defined by $\bar{S}_\Delta^*(\chi) = \chi \circ \bar{S}_\Delta$. Note that $\bar{S}_\Delta^*$ is never injective; in fact, we have

$$\chi_\Delta \in \mathrm{Ker}(\bar{S}_\Delta^*) \quad \text{because} \quad \bar{S}(f) \subset \mathrm{Ker}(\chi_\Delta), \ \forall f \in Cl(\Delta), \tag{1.114}$$

where (as before) χ_Δ is as in Proposition 1.26. Indeed, the inclusion $\bar{S}(f) \subset \mathrm{Ker}(\chi_\Delta)$ follows immediately from (1.63), and from this the first assertion follows.

Corollary 1.49 *We have*

$$\bar{S}(1_\Delta) \;=\; \bigcap_{\chi_d^\Delta \in \mathcal{G}(\Delta)} \mathrm{Ker}(\chi_d^\Delta) \;=\; \bigcap_{\chi \in \mathcal{G}_\Delta} \mathrm{Ker}(\chi), \tag{1.115}$$

and hence

$$[(\mathbb{Z}/\Delta\mathbb{Z})^\times : \bar{S}(1_\Delta)] \;=\; 2^{\#\mathcal{G}(\Delta)} \;=\; |\mathcal{G}_\Delta|. \tag{1.116}$$

In particular, the group $\mathcal{G}_\Delta$ of genus characters has the intrinsic interpretation

$$\mathcal{G}_\Delta \;=\; \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta), \pm 1). \tag{1.117}$$

The proof of this corollary uses the following general fact about the intersection of kernels of quadratic characters.

Lemma 1.3 *Let A be a finite abelian group and let $X \leq \mathrm{Hom}(A, \mathbb{Z}/2\mathbb{Z})$ be a subgroup. Then $X = \mathrm{Hom}(A/A_X, \mathbb{Z}/2\mathbb{Z})$, where $A_X = \cap_{f \in X} \mathrm{Ker}(f)$, and we have*

$$[A : A_X] \;=\; |X| \quad \textit{and} \quad [\mathrm{Hom}(A, \mathbb{Z}/2\mathbb{Z}) : X] \;=\; [A_X : 2A]. \tag{1.118}$$

Proof. We first verify (1.118). For this, consider the pairing $e_X : X \times A \to \mathbb{Z}/2\mathbb{Z}$ defined by $e_X(f, a) = f(a)$. Then the left kernel is $\{0\}$ and the right kernel is A_X. We thus have an isomorphism $A/A_X \xrightarrow{\sim} \mathrm{Hom}(X, \mathbb{Z}/2\mathbb{Z})$ (cf. [La3], p. 49), and hence $[A : A_X] = |\mathrm{Hom}(X, \mathbb{Z}/2\mathbb{Z})| = |X|$, the latter since X is a finite-dimensional $\mathbb{F}_2$-vector space. This proves the first equality of (1.118). The second follows from this and (1.79).

To verify the first assertion, note first that clearly $X \leq \mathrm{Hom}(A/A_X, \mathbb{Z}/2\mathbb{Z}) = \{\chi \in \mathrm{Hom}(A, \mathbb{Z}/2\mathbb{Z}) : \mathrm{Ker}(\chi) \geq A_X\}$. But by (1.118) we have that $|X| = [A/A_X| = |\mathrm{Hom}(A/A_X, \mathbb{Z}/2\mathbb{Z})|$, the latter because A/A_X is an $\mathbb{F}_2$-vector space, and so the desired equality holds.

Proof of Corollary 1.49. We first note that (1.116) and (1.117) follow immediately from (1.115) and Lemma 1.3 (together with (1.81)). Moreover, we observe that the second equality of (1.115) is trivial because $\mathcal{G}_\Delta = \langle \mathcal{G}(\Delta) \rangle$, and that $\bar{S}(1_\Delta) \leq H := \bigcap_{\chi \in \mathcal{G}_\Delta} \mathrm{Ker}(\chi)$ by Proposition 1.48. We now distinguish two cases.

Case 1: $\Delta \not\equiv 4, 8, 16, 20, 24 \pmod{32}$. In that case we know from (1.77) that $\mathcal{G}_\Delta = \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$ and that hence $H = ((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2$. Since it is clear that $((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2 \leq \bar{S}(1_\Delta)$, we see that $\bar{S}(1_\Delta) = H = ((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2$ in this case.

Case 2: $\Delta \equiv 4, 8, 16, 20, 24 \pmod{32}$, i.e. $\Delta = 4n$ with $n \equiv 1, 2, 4, 5, 6 \pmod 8$. Here we have by (1.118) and (1.77) that

$$[H : ((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2] \;=\; [\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\}) : \mathcal{G}_\Delta] \;=\; 2. \tag{1.119}$$

Thus, since $((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2 \leq \bar{S}(1_\Delta) \leq H$, and since $\bar{S}(1_\Delta) \neq ((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2$ (because $4 - n$ or $1 - n \in \bar{S}(1_\Delta) \setminus ((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2$), we see that (1.119) forces that $\bar{S}(1_\Delta) = H$. This proves (1.115) and hence Corollary 1.49.

Corollary 1.50 *The principal genus is the kernel of $\bar{S}_\Delta$, i.e. $PG(\Delta) = \mathrm{Ker}(\bar{S}_\Delta)$. Thus two forms $f_1, f_2 \in Q_\Delta$ are genus equivalent if and only if they represent the same values mod Δ, i.e.*

$$f_1 \simeq f_2 \quad \Leftrightarrow \quad \bar{S}(f_1) = \bar{S}(f_2). \tag{1.120}$$

Proof. If $f \in \mathrm{Ker}(\bar{S}_\Delta)$, then by (1.113) we have $\chi_d^*(f) = \chi_d(\bar{S}_\Delta(f)) = \chi_d(1) = 1$, $\forall \chi_d \in \mathcal{G}(\Delta)$, and so $\mathrm{Ker}(\bar{S}_\Delta) \leq \bigcap_{\chi_d \in \mathcal{G}(\Delta)} \mathrm{Ker}(\chi_d^*) = PG(\Delta)$. Conversely, let $f \in PG(\Delta)$, and let $m \in P(f)$ with $(m, \Delta) = 1$. Then $\chi_d(m) = 1$, $\forall \chi_d \in \mathcal{G}(\Delta)$, and so by (1.115) we have $m \pmod{\Delta} \in \bar{S}(1_\Delta)$. But this means that $\bar{S}_\Delta(f) = 1$, so $f \in \mathrm{Ker}(\bar{S}_\Delta)$, and hence $\mathrm{Ker}(S_\Delta) = PG(\Delta)$, as claimed. From this (together with Corollary 1.47), (1.120) follows immediately.

Remark 1.25 As Cox points out in his book, the idea of sorting quadratic forms according their values mod Δ is due to Lagrange (1775); cf. [Cox], p. 32 and p. 38. In view of the above Corollary 1.50, Lagrange therefore anticipated Gauss's genus theory. Unfortunately, Gauss himself did not explain the connection between his genus theory and that of Lagrange.

We next want to determine $g(\Delta)$. For this we first make the following observations.

Observation 1.3 If $f \in Q_\Delta$, then $\chi_d^*(f^2) = (\chi_d^*(f))^2 = 1$, and so $Cl(\Delta)^2 \leq \mathrm{Ker}(\chi_d^*)$, for all $d \in \mathcal{P}(\Delta)$. Thus

$$Cl(\Delta)^2 \leq PG(\Delta).$$

We therefore see that $Cl(\Delta)/PG(\Delta)$ is a quotient of $Cl(\Delta)/Cl(\Delta)^2$, and so it is an elementary abelian 2-group. We thus have

$$g(\Delta) = 2^t, \quad \text{with } t \leq r_2(\Delta), \tag{1.121}$$

where $r_2(\Delta)$ denotes the 2-*rank* of $Cl(\Delta)$ which is defined by $2^{r_2(\Delta)} = [Cl(\Delta) : Cl(\Delta)^2]$.

Before determining t, we first determine the 2-rank r_2 of $Cl(\Delta)$. For this we shall calculate instead the number of *ambiguous* or 2-torsion classes in $Cl(\Delta)$; these are the classes $cl(f) \in Cl(\Delta)$ such that $cl(f)^2 = 1$. This will give the 2-rank because of the following general fact.

Lemma 1.4 *If A is a finite abelian group (written additively) and $n \geq 1$ is an integer, then*

$$[A : nA] = |A[n]|, \quad \textit{where } A[n] = \{x \in A : nx = 0\}. \tag{1.122}$$

Proof. Let $[n] : A \to A$ denote the multiplication by n map. By definition, $A[n] = \mathrm{Ker}([n])$ and $nA = \mathrm{Im}([n])$, so by the (first) isomorphism theorem $|nA| = |A|/|A[n]|$ and hence $|A[n]| = |A|/|nA| = [A : nA]$, as claimed.

Proposition 1.51 *The number of ambiguous classes in $Cl(\Delta)$ is $2^{r_2(\Delta)}$, where $r_2(\Delta)$ denotes the 2-rank of $Cl(\Delta)$. Moreover,*

$$r_2(\Delta) \;=\; \#\mathcal{G}(\Delta) - 1. \tag{1.123}$$

Proof. The first assertion follows from Lemma 1.4 with $n = 2$. Note that by (1.109), a class $cl(f)$ is ambiguous if and only if f is ambiguous (in the sense of Proposition 1.5).

Assume first that $\Delta < 0$. Then by Theorem 1.3 each class contains a unique reduced form, and so $2^{r_2(\Delta)} = \#\{f \in Q_\Delta : f \text{ is a reduced, ambiguous form}\}$. Now if $f = [a, b, c]$ is reduced, then $\bar{f} := [a, -b, c]$ is semi-reduced, and so we see that f is reduced and ambiguous $\Leftrightarrow f = \bar{f}$ or $\bar{f}$ is not reduced. Thus by (1.23) we have

$$f \text{ is reduced and ambiguous } \Leftrightarrow\; f = [a, 0, c],\ [a, a, c] \text{ or } [a, b, a], \text{ where } 0 < b \le a \le c.$$

Suppose first that $\Delta \equiv 1(4)$. Then first case cannot happen. Moreover, the second case happens if and only if $c = \frac{a+a'}{4}$ where $aa' = -\Delta$ and $a' \ge 3a$, and the third case happens if and only if $b = \frac{a+a'}{2}$ and $3a > a' > a$. We thus see that

$$2^{r_2(\Delta)} = \#\{(a, a') : aa' = -\Delta, 1 \le a \le a', \gcd(a, a') = 1\} = 2^{\omega(\Delta)-1}.$$

Thus $r_2(\Delta) = \omega(\Delta) - 1 = \#\mathcal{G}(\Delta) - 1$ by (1.76).

If Δ is even then by considering the various cases separately, a similar analysis shows that $r_2(\Delta) = \#\mathcal{G}(\Delta) - 1$; cf. [Bu], p. 68.

Finally, if $\Delta > 0$, then each ambiguous class $cl(f)$ contains precisely two ambiguous forms ([Bu], p. 25) and hence precisely one ambiguous $f = [a, b, c]$ with $a > 0$. Then a similar analysis as for $\Delta < 0$ shows that (1.123) holds here as well; cf. [Bu], p. 68.

The value of $g(\Delta)$ is closely related to $r_2(\Delta)$, as the following result shows.

Theorem 1.7 (Gauss) *Every form in the principal genus is properly equivalent to a square; i.e.*

$$PG(\Delta) \;=\; Cl(\Delta)^2. \tag{1.124}$$

Thus

$$g(\Delta) \;= 2^{r_2(\Delta)} \;=\; 2^{\#\mathcal{G}(\Delta)-1} \;=\; \tfrac{1}{2}|\mathcal{G}_\Delta|. \tag{1.125}$$

This theorem is rather difficult to prove. Gauss himself first develops a *theory of ternary forms* in order to prove (1.124). In fact, Gauss proves more: he gives an explicit method for finding, for a given $f \in PG(\Delta)$, a form f_1 with $f_1 \circ f_2 \sim f$; cf. Gauss[DA], Art. 286.

Here we shall give a proof of Theorem 1.7 based on the following well-known result of Dirichlet (1837).[13]

[13]Legendre stated this theorem as a fact in 1785 and used it his work. He also gave an incorrect proof of it; cf. [We], p. 329.

Theorem 1.8 (Dirichlet) *If $(a,m) = 1$ and $m > 0$, then there are infinitely many primes $p \equiv a \pmod{m}$.*

Proof. Hua[Hu], p. 243.

As we shall see, Gauss's Theorem 1.7 follows immediately from the following refinement:

Proposition 1.52 *We have*

$$\text{(1.126)}\quad \mathrm{Im}(\bar{S}_\Delta) = \mathrm{Ker}(\chi_\Delta)/\bar{S}(1_\Delta), \quad \textit{and hence} \quad \mathrm{Ker}(\bar{S}_\Delta) = PG(\Delta) = Cl(\Delta)^2.$$

Proof. By (1.114) we know that $\mathrm{Im}(\bar{S}_\Delta) \subset \mathrm{Ker}(\chi_\Delta)/\bar{S}(1_\Delta)$. To prove the opposite inclusion, let $a \in \mathrm{Ker}(\chi_\Delta)$, with $(a,\Delta) = 1$ and $a > 0$. By Dirichlet's Theorem, there is a prime $p \equiv a \pmod{\Delta}$. Then $\chi_\Delta(p) = 1$, and so by Proposition 1.8 (together with (1.54)) there is a form $f \in Q_\Delta$ with $p \in R(f)$. Thus $\bar{S}_\Delta(f) = p\bar{S}(1_\Delta) = a\bar{S}(1_\Delta)$, and so $\mathrm{Ker}(\chi_\Delta)/\bar{S}(1_\Delta) \le \mathrm{Im}(\bar{S}_\Delta)$. This proves the first assertion of (1.126).

From this we thus have that $[Cl(\Delta) : \mathrm{Ker}(\bar{S}_\Delta)] = |\mathrm{Im}(\bar{S}_\Delta)| = [\mathrm{Ker}(\chi_\Delta) : \bar{S}(1_\Delta)]$. Moreover, since $\mathrm{Ker}(\chi_\Delta)$ has index 2 in $(\mathbb{Z}/\Delta\mathbb{Z})^\times$, it follows from (1.116) that $[\mathrm{Ker}(\chi_\Delta) : \bar{S}(1_\Delta)] = 2^{\#\mathcal{G}(\Delta)-1}$, and so we obtain that

$$[Cl(\Delta) : \mathrm{Ker}(\bar{S}_\Delta)] = |\mathrm{Im}(\bar{S}_\Delta)| = [\mathrm{Ker}(\chi_\Delta) : \bar{S}(1_\Delta)] = 2^{\#\mathcal{G}(\Delta)-1} = [Cl(\Delta) : Cl(\Delta)^2],$$

where the last equality follows from (1.123). Thus, since $Cl(\Delta)^2 \le PG(\Delta) = \mathrm{Ker}(\bar{S}_\Delta)$ by Observation 1.3 and (1.120), the second assertion of (1.126) follows.

Proof of Theorem 1.7. The assertion (1.124) is contained in (1.126) and (1.125) follows from this and (1.123).

Corollary 1.53 *The map $\bar{S}^*_\Delta : \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta), \{\pm 1\}) \to \mathrm{Hom}(Cl(\Delta), \{\pm 1\})$ is surjective and has kernel $\mathrm{Ker}(\bar{S}^*_\Delta) = \langle \chi_\Delta \rangle$, and so we obtain the exact sequence*

$$\text{(1.127)}\qquad 0 \to \langle \chi_\Delta \rangle \ \to\ \mathcal{G}_\Delta \ \stackrel{\bar{S}^*_\Delta}{\to}\ \mathrm{Hom}(Cl(\Delta), \{\pm 1\}) \ \to\ 0.$$

Proof. Let $p : (\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta) \to (\mathbb{Z}/\Delta\mathbb{Z})^\times/\mathrm{Ker}(\chi_\Delta)$ denote the canonical quotient map induced by the inclusion $\bar{S}(1_\Delta) \subset \mathrm{Ker}(\chi_\Delta)$. Then (1.126) shows that the sequence

$$0 \ \to\ Cl(\Delta)/Cl(\Delta)^2 \ \stackrel{\bar{S}_\Delta}{\to}\ (\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta) \ \stackrel{p}{\to}\ (\mathbb{Z}/\Delta\mathbb{Z})^\times/\mathrm{Ker}(\chi_\Delta) \ \to\ 0$$

is an exact sequence of finite-dimensional $\mathbb{F}_2$-vector spaces, and hence the induced dual sequence

$$0 \to ((\mathbb{Z}/\Delta\mathbb{Z})^\times/\mathrm{Ker}(\chi_\Delta))^* \ \stackrel{p^*}{\to}\ ((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta))^* \ \stackrel{\bar{S}^*_\Delta}{\to}\ (Cl(\Delta)/Cl(\Delta)^2)^* \ \to 0$$

is also exact. Thus, $\bar{S}^*_\Delta$ is surjective with kernel $\mathrm{Im}(p^*)$. But since p^* can be identified with the inclusion map $\langle \chi_\Delta \rangle \hookrightarrow ((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta))^* = \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar{S}(1_\Delta), \{\pm 1\})$, we see that $\mathrm{Ker}(\bar{S}^*_\Delta) = \langle \chi_\Delta \rangle$. This proves the first two assertions, and in view of (1.117) it is clear that the last assertion follows from the first two.

Remark 1.26 Note that the exact sequence (1.127) is a succint way of stating the main results (due to Gauss) on genus theory. In particular, Theorem 1.7 is an immediate consequence. Moreover, it implies the following result which is a variant of the discussion of Gauss[DA] in Articles 263, 264, and 287.

Corollary 1.54 *The "total character map"* $f \mapsto \tilde{\chi}_f$ *of* Remark 1.16 *induces an isomorphism*

$$X_\Delta : Cl(\Delta)/Cl(\Delta)^2 \ \tilde{\to}\ \mathrm{Hom}(\mathcal{G}_\Delta/\langle\chi_\Delta\rangle, \{\pm 1\}) = \{\tilde{\psi} \in (\mathcal{G}_\Delta)^* : \tilde{\psi}(\chi_\Delta) = 1\}. \tag{1.128}$$

Thus, if $\psi : \mathcal{G}(\Delta) \to \{\pm 1\}$ *is any map, then*

$$\psi = \chi_f, \text{ for some } f \in Q_\Delta \quad \Leftrightarrow \quad \prod_{d \in \mathcal{G}(\Delta)} \psi(d)^{e_d} = 1, \tag{1.129}$$

where χ_f *is as in* Remark 1.16 *and the* $e_d \in \mathbb{Z}/2\mathbb{Z}$ *are uniquely defined by the relation*

$$\chi_\Delta = \prod_{d \in \mathcal{G}(\Delta)} (\chi_d^\Delta)^{e_d}. \tag{1.130}$$

Proof. Write $C = Cl(\Delta)/Cl(\Delta)^2$. By (1.127) we have that $\bar{S}_\Delta^*$ induces an isomorphism $\overline{\mathcal{G}} := \mathcal{G}_\Delta/\langle\chi_\Delta\rangle \ \tilde{\to}\ C^*$, whose dual $\bar{S}_\Delta^{**}$ gives an isomorphism $C^{**} \ \tilde{\to}\ \overline{\mathcal{G}}^*$. Combining this with the canonical isomorphism $e_C : C \ \tilde{\to}\ C^{**}$ given by $e_C(f)(\chi) = \chi(f)$ yields an isomorphism $X'_\Delta : C \to \overline{\mathcal{G}}$.

To prove the first assertion, we still have to verify that $X'_\Delta(f) = \tilde{\chi}_f$, $\forall f \in Cl(\Delta)$; cf. Remark 1.16. Now by construction $X'_\Delta(f) = \bar{S}_\Delta^{**}(e_C(f)) = \bar{S}_\Delta^* \circ e_C(f)$, so for any $\chi \in \mathcal{G}$ we have $X'_D(f)(\chi) = \bar{S}^*(e_C(f))(\chi) = e_C(f)(\chi \circ \bar{S}_\Delta) = \chi(\bar{S}_\Delta(f))$. In particular, for $\chi = \chi_d^\Delta$ we have by (1.113) (and the definition of $\tilde{\chi}_f$) that $X'_\Delta(f)(\chi_d^\Delta) = \chi_d^\Delta(\bar{S}_\Delta(f)) = \chi_d(f) = \tilde{\chi}_f(\chi_d^\Delta)$, and so the assertion follows since $\{\chi_d^\Delta : d \in \mathcal{G}(\Delta)\}$ is a basis of $\mathcal{G}_\Delta$.

To prove (1.129), first note that there exist unique $e_d \in \mathbb{F}_2$ such that (1.130) holds because $\chi_\Delta \in \mathcal{G}_\Delta$ and $\{\chi_d^\Delta : d \in \mathcal{G}(\Delta)\}$ is an $\mathbb{F}_2$-basis of $\mathcal{G}_\Delta$. Now let $\tilde{\psi} \in \mathrm{Hom}(\mathcal{G}_\Delta, \{\pm 1\})$ be the unique homomorphism such that $\tilde{\psi}(\chi_d^\Delta) = \psi(d)$. Then $\psi = \chi_f$, for some $f \in Q_\Delta \Leftrightarrow \tilde{\psi} = \tilde{\chi}_f = X_\Delta(f)$, for some $f \in Q_\Delta \Leftrightarrow \tilde{\psi} \in \mathrm{Im}(X_\Delta) \Leftrightarrow \tilde{\psi}(\chi_\Delta) = 1$. Now by (1.130) we have $\tilde{\psi}(\chi_\Delta) = \prod_d \tilde{\psi}(\chi_d^\Delta)^{e_d} = \prod_d \psi(d)^{e_d}$, and so (1.129) follows.

Finally, we note that genus theory implies the the following useful fact.

Corollary 1.55 *If* $f \in Q_\Delta$*, then* f *lies in the principal genus if and only if* f *represents a square* n^2 *which is prime to* Δ*.*

Proof. Suppose first that $n^2 \in R(f)$ with $(n, \Delta) = 1$. Then $\chi_d(f) = \chi_d^\Delta(n^2) = 1$, for all $d \in \mathcal{G}(\Delta)$, and so $cl(f) \in PG(\Delta)$.

Conversely, suppose $f \in PG(\Delta)$. Then by (1.124) we have $f \sim f_1 \circ f_1$, for some $f_1 \in Q_\Delta$. By Proposition 1.39 there exists $n \in R(f_1)$ with $(n, \Delta) = 1$, and then $n^2 \in R(f)$ by (1.89) and (1.90).

Remark. Note that if f represents n^2 with $(n^2, \Delta) = 1$, then $n^2 = c^2 m^2$ with $m \in R(f)$ and $c \in \mathbb{Z}$. Thus $f \sim [m^2, b, c]$ for some b, c, and then $f \sim f_1 \circ f_1$ with $f_1 := [m, b, mc] \in Q_\Delta$. This gives a more constructive proof of (the one direction of) Corollary 1.55.

Chapter 2

Lattices and Quadratic Modules

2.1 Introduction

After Gauss, many mathematicians, particularly *L. Dirichlet*, simplified and extended Gauss's results on binary quadratic forms. In 1856/57, shortly before his death, Dirichlet gave a course on number theory in which binary quadratic forms played an important role, and the notes of this course were written up and published in 1863 by his student *R. Dedekind*, four years after Dirichlet's death.

In 1871 Dedekind added a number of *supplements* to the second edition of these lecture notes. In these, he introduced his notion of an "ideal" and showed how many concepts in number theory can be simplified and generalized with the help of this notion.

In particular, he showed how the theory of binary quadratic forms and specifically Gauss's (difficult) theory of composition have a very natural interpretation in terms of multiplication of (fractional) ideals. As a result, this made Gauss's theory much more transparent in many aspects.

Dedekind's theory also paved the way for a more geometric interpretation of binary quadratic forms. This geometric viewpoint was the approach pursued by Minkowski (ca. 1890; cf. [Di], III, p. 244) in studying quadratic forms in an arbitrary number variables and to his "geometry of numbers". In addition, his theory naturally leads to the concept of a *quadratic module* which is an abstract version of the notion of a quadratic form, as will be explained in §2.2

Roughly speaking, the idea behind Dedekind's construction is the following. Already in 1831 Gauss had observed that if

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

is a positive definite binary quadratic form, then its values are the squares of the distances (from $(0, 0)$) of the points lying on a "parallelogrammatic system" in the real plane; cf. [Di], III, p. 17. Such a system is now called *lattice* (in $\mathbb{R}^2$). Indeed, since by the Principal Axis Theorem we can always find a real matrix $B \in M_2(\mathbb{R})$ such that $B^t B = \frac{1}{2}A(f)$, we

have

$$f(\vec{x}) \;=\; \vec{x}^t(\tfrac{1}{2}A(f))\vec{x} \;=\; \vec{x}^tB^tB\vec{x} \;=\; (B\vec{x})^t(B\vec{x}) \;=\; ||B\vec{x}||^2, \quad \forall \vec{x} \in \mathbb{Z}^2,$$

and so the associated lattice is $L_B := \{B\vec{x} : \vec{x} \in \mathbb{Z}^2\}$. Note that if we want to consider several binary quadratic forms (as we did in the theory of Lagrange and Gauss), then we also have to look at several different lattices in $\mathbb{R}^2$.

Dedekind's theory is a variant of this, with two important differences.

1) In place of the simple Euclidean distance (squared) defined by $x^2 + y^2$, Dedekind also allowed the "dilated distance $x^2 + Ny^2$ where $N \in \mathbb{Z}$ and $-N \notin (\mathbb{Q}^\times)^2$.

2) Once N has been fixed, he restricts attention to those lattices L that are *commensurable* with $L_N = \mathbb{Z} + \sqrt{-N}\mathbb{Z}$, i.e. $L_N \cap L$ has finite index in L and in L_N. Thus all his lattices lie in the $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{-N}) = \mathbb{Q} + \mathbb{Q}\sqrt{-N}$, which is a quadratic field.

He then shows that these lattices are (fractional) ideals of suitable subrings (called *orders*) of $\mathbb{Q}(\sqrt{-N})$, and this allows him to give a complete dictionary between ideals/lattices and binary quadratic forms.

At a first glance, this dictionary may seem to be involved (and artificial). However, when we view it from the point of view of quadratic modules, this correspondence becomes much more transparent.

2.2 Quadratic Modules

Although we need only special cases of the following general definition, it is nevertheless useful to give it the most general form.

Definition. Let R be a commutative ring and let M be an R-module. A *quadratic form* on M is a map $f : M \to R$ such that

(i) f is homogeneous of degree 2, i.e. we have

$$f(rx) \;=\; r^2 f(x), \quad \text{for all } x \in M,\, r \in R. \tag{2.1}$$

(ii) the map $\beta_f : M \times M \to R$ defined by

$$\beta_f(x, y) = f(x + y) - f(x) - f(y) \tag{2.2}$$

is R-bilinear, i.e. R-linear in each variable.

If $f : M \to R$ is a quadratic form, then we call the pair (M, f) a *quadratic R-module* and the map β_f the *associated bilinear form*. Note that if follows from (2.2) and (2.1) that

$$\beta_f(x, x) = 2f(x), \quad \text{for all } x \in M. \tag{2.3}$$

Example 2.1 (a) Let $f = [a, b, c]$ be an integral binary quadratic form as in chapter 1, and view f as a map $f : \mathbb{Z}^2 \to \mathbb{Z}$ (as we did before). Then the pair $(\mathbb{Z}^2, f)$ is a quadratic $\mathbb{Z}$-module; the associated bilinear form is

$$\beta_f(\vec{x}, \vec{y}) = \vec{x}^tA(f)\vec{y}, \quad \text{for all } \vec{x}, \vec{y} \in \mathbb{Z}^2,$$

where, as in (1.8), $A(f)$ denotes the matrix associated to f.

(b) If (M, f) is a quadratic R-module and if $\varphi : M' \to M$ is an R-linear map of R-modules, then the pullback $\varphi^* f = f \circ \varphi : M' \to R$ is a quadratic form on M', and so $(M', \varphi^* f)$ is also a quadratic R-module.

In particular, if $M' \subset M$ is an R-submodule of M, then the *restriction* $f_{|M'} = j^* f$ of f to M' is a quadratic form on M'; here $j : M' \hookrightarrow M$ denotes the inclusion map.

(c) If $f = [a, b, c]$ is as in part (a) and $T \in M_2(\mathbb{Z})$, then the *transform* fT of f by T (as defined in subsection 1.3.1) is just the pullback of f with respect to the associated linear map $\varphi_T : \mathbb{Z}^2 \to \mathbb{Z}^2$ defined by $\varphi_T(\vec{x}) = T\vec{x}$. Indeed, $fT(\vec{x}) = f(T\vec{x}) = f(\varphi_T(\vec{x})) = \varphi_T^* f(\vec{x})$, so $fT = \varphi_T^* f$.

Definition. A *homomorphism* $\varphi : (M_1, f_2) \to (M_2, f_2)$ of quadratic R-modules is an R-linear map $\varphi : M_1 \to M_2$ such that $f_1 = \varphi^* f_2$. It is an *isomorphism* (or an *isometry*) if (in addition) $\varphi : M_1 \to M_2$ is an isomorphism. If an isomorphism exists, then we call (M_1, f_1) and (M_2, f_2) *isomorphic* and write $(M_1, f_1) \simeq (M_2, f_2)$.

Example 2.2 (a) If $f_1 = [a, b, c]$ is as in Example 2.1(a), and if $T \in \mathrm{GL}_2(\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}^2)$, then φ_T defines an isomorphism $\varphi_T : (\mathbb{Z}^2, f_1 T) \xrightarrow{\sim} (\mathbb{Z}^2, f_1)$ of quadratic modules (and conversely). Thus:

$$\begin{aligned} f_1 \;\approx\; f_2 \;&\overset{\text{def}}{\Leftrightarrow}\; \exists T \in \mathrm{GL}_2(\mathbb{Z}) \text{ such that } f_2 = f_1 T \\ &\Leftrightarrow\; (\mathbb{Z}^2, f_2) \simeq (\mathbb{Z}^2, f_1). \end{aligned}$$

Thus, a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of binary quadratic forms f (as in chapter 1) is the same thing as an isomorphism class of quadratic $\mathbb{Z}$-modules $(\mathbb{Z}^2, f)$.

(b) More generally, suppose that (M, f) is a *free* quadratic $\mathbb{Z}$ *of rank* 2, i.e. that (M, f) is a quadratic $\mathbb{Z}$-module and $M \simeq \mathbb{Z}^2$. Note that the choice of an isomorphism $\varphi : \mathbb{Z}^2 \xrightarrow{\sim} M$ is the same as choosing an (ordered) basis $\underline{x} = \{x_1, x_2\}$ of M (by the rule $\varphi(\vec{e}_i) = x_i$); we thus write $\varphi = \varphi_{\underline{x}}$. For any such choice,

$$f_{\underline{x}}(x, y) = f(\varphi_{\underline{x}}(x, y)) = f(xx_1 + yx_2)$$

is a binary quadratic form in the sense of chapter 1, and the set $\{f_{\underline{x}}\}_{\underline{x}}\}$ defines a unique $\mathrm{GL}_2(\mathbb{Z}$-equivalence class of forms. Thus: a free quadratic module (M, f) of rank 2 determines a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of binary quadratic forms (and conversely).

Definition. If (M, f) is a free quadratic R-module of rank n, then its *determinant* is

$$\det(M, f) \;=\; \det(\beta_f(x_i, x_j)) \in R/(R^\times)^2,$$

where $\{x_1, \ldots, x_n\}$ is any basis of M. This is well-defined because if $\{x_i'\}$ is another basis, then $x_i' = Tx_i$, for some $T \in \mathrm{GL}(M) = \mathrm{Aut}(M)$, (so $\det(T) \in R^\times$) and then $\det(\beta_f(x_i', x_j')) = \det(T)^2 \det(\beta_f(x_i, x_j))$.

Remark. If $R = \mathbb{Z}$, then $R^\times = \{\pm 1\}$ and $(R^\times)^2 = \{1\}$. Thus, for free quadratic $\mathbb{Z}$-modules we have $\det(M, f) \in \mathbb{Z}/(\mathbb{Z}^\times)^2 = \mathbb{Z}$. In particular, $\det(\mathbb{Z}^2, f) = \det(A(f)) = -\Delta(f)$.

2.3 Lattices and Orders

There are several (inequivalent) definitions of a lattice in mathematics[1]. The following definition covers all the cases that we shall consider.

Definition. Let V be an F-vector space of finite dimension n, where F is a field. A *lattice* of V is an additive subgroup $L \leq V$ such that $L \simeq \mathbb{Z}^n$ and L contains an F-basis of V.

Example 2.3 (a) Let $V = \mathbb{C}$, and view $\mathbb{C}$ as a 2-dimensional $\mathbb{R}$-vector space. Then $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice in $\mathbb{C}$ if and only if $\omega_2/\omega_1 \notin \mathbb{R} \Leftrightarrow \mathrm{Im}(\omega_2/\omega_1) \neq 0$. Such lattices will be considered in part II of the course. Note that not every subgroup $L \leq \mathbb{C}$ with $L \simeq \mathbb{Z}^2$ is a lattice in $\mathbb{C}$; for example $L = \mathbb{Z} + \mathbb{Z}\sqrt{2} \simeq \mathbb{Z}^2$ is not a lattice in $\mathbb{C}$.

(b) Let $V = \mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$, where $d \in \mathbb{Z}$. If d is not a square, then $K = \mathbb{Q}(\sqrt{d})$ is a 2-dimensional $\mathbb{Q}$-vector space (and a field). Moreover, if $\alpha \in K \setminus \mathbb{Q}$, then $L(\alpha) := \mathbb{Z} + \mathbb{Z}\alpha$ is a lattice in K.

(c) Let $V = K$, where K is a *number field*. Thus, K is a field containing $\mathbb{Q}$ which is a finite-dimensional $\mathbb{Q}$-vector space. We call $[K : \mathbb{Q}] := \dim_{\mathbb{Q}}(K)$ the *degree* of K.

If $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis of K, then

$$L(\alpha_1, \ldots, \alpha_n) := \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n = \langle \alpha_1, \ldots, \alpha_n \rangle$$

is a lattice in K. Conversely, every lattice L in K is of this form, for if $L \simeq \mathbb{Z}^n$, then $L = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$ for some $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of L. But then $\alpha_1, \ldots, \alpha_n$ are also $\mathbb{Q}$-linearly independent and hence a $\mathbb{Q}$-basis of K, so $L = L(\alpha_1, \ldots, \alpha_n)$ for a some $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$.

A key fact about lattices in number fields K is the following.

Proposition 2.1 *Let K be a number field of degree n, and let $L \leq K$ be an additive subgroup. Then the following conditions are equivalent:*

(i) *$L \simeq \mathbb{Z}^n$;*

(ii) *L is a lattice in K;*

(iii) *L is a finitely generated group and L contains a basis of K;*

(iv) *there exists a lattice L' in K with $L' \supset L$ and $[L' : L] < \infty$.*

Proof. (i) $\Rightarrow$ (ii): If $L \simeq \mathbb{Z}^n$, then $L = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$, for some $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of L. By the argument of Example 2.3(c) we see that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis of K, so L is a lattice.

(ii) $\Rightarrow$ (iii): Clear.

[1]For example, a lattice in Boolean algebras in not the same as a lattice in the theory of integral representations over a Dedekind domain.

(iii) $\Rightarrow$ (iv): By hypothesis, $L = \sum_{k=1}^{m} \mathbb{Z}\lambda_k$ and there is a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K such that $\alpha_i \in L$ for $1 \leq i \leq n$. Since L is a group, we have $L(\alpha_1, \ldots, \alpha_n) \leq L$, and since α_i is a basis of K, there exist $a_{ij} \in \mathbb{Q}$ such that $\lambda_j = \sum_i a_{ij}\alpha_i$. Then there exists $N \in \mathbb{Z}$, $N > 0$ such that $b_{ij} = Na_{ij} \in \mathbb{Z}$, for all i, j. Thus $\lambda_j = \sum b_{ij}\frac{\alpha_i}{N} \in L' := L(\frac{\alpha_1}{N}, \ldots, \frac{\alpha_n}{N})$, and so $L = \langle \lambda_j \rangle \leq L'$. Now $NL' = L(\alpha_1, \ldots, \alpha_n) \subset L \subset L'$, so $[L' : L] \leq [L' : NL'] = [\mathbb{Z}^n : N\mathbb{Z}^n] = N^n < \infty$. Thus L satisfies condition (iv).

(iv) $\Rightarrow$ (i): Since L' is free, so is $L \subset L'$ (cf. Lang[La3], p. 41). Thus $L \simeq \mathbb{Z}^k$ for some $k \leq n$, i.e. $L = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_k$, where the $\alpha_1, \ldots, \alpha_k$ are $\mathbb{Z}$-linearly and hence $\mathbb{Q}$-linearly independent. Put $m = [L' : L]$. Then $mL' \subset L$ and so $\mathbb{Q}(mL') \subset \mathbb{Q}L \subset \mathbb{Q}L' = K$. But $\mathbb{Q}(mL') = \mathbb{Q}L' = K$, so $\mathbb{Q}L = K$. Thus $\alpha_1, \ldots, \alpha_k$ generate K as a $\mathbb{Q}$-vector space and so $k \geq n$. Thus $n = k$ and $L \simeq \mathbb{Z}^n$, as desired.

Notation. The set of lattices of K is denoted by $\mathrm{Lat}_K = \{L \leq K : L \text{ is a lattice in } K\}$.

Corollary 2.2 *Let $L' \in \mathrm{Lat}_K$ and let $L \leq L'$ be a subgroup. Then:*

$$L \in \mathrm{Lat}_K \quad \Leftrightarrow \quad [L' : L] < \infty. \tag{2.4}$$

Proof. ($\Leftarrow$) This is the implication (iv) $\Rightarrow$ (ii) of Proposition 2.1.

($\Rightarrow$) By hypothesis, $L = L(\alpha_1, \ldots, \alpha_n)$; cf. Example 2.3(c). By the argument of the implication (iii) $\Rightarrow$ (iv), there exists $N > 0$ such that $L' \subset \frac{1}{N}L$ and so $[L' : L] \leq [\frac{1}{N}L : L] = N^n < \infty$.

The next result shows that the set Lat_K is closed under the operations of addition, multiplication, intersection and quotient of lattices:

Corollary 2.3 *Let $L, L_1, L_2 \in \mathrm{Lat}_K$. Then:*

(a) $\alpha L \in \mathrm{Lat}_K$, $\forall \alpha \in K^\times$;

(b) $L_1 + L_2 \in \mathrm{Lat}_K$

(c) $L_1 L_2 \in \mathrm{Lat}_K$;

(d) $L_1 \cap L_2 \in \mathrm{Lat}_K$;

(e) $(L_1 : L_2)_K := \{\alpha \in K : \alpha L_2 \subset L_1\} \in \mathrm{Lat}_K$.

Proof. (a) $\alpha L \simeq L \simeq \mathbb{Z}^n$, so αL satisfies condition (i) of Proposition 2.1.

(b) Since L_i is finitely generated, so is $L_1 + L_2$. Moreover, since L_1 contains a basis of K, so does $L_1 + L_2 \supset L_1$, so $L_1 + L_2$ satisfies condition (iii) of Proposition 2.1.

(c) By definition, $L_1 L_2 = \langle \alpha_1 \alpha_2 : \alpha_i \in L_i \rangle = \sum_i \beta_i L_2$, where $L_1 = \langle \beta_1, \ldots, \beta_n \rangle$. Thus $L_1 L_2 \in \mathrm{Lat}_K$ by (a) and (b).

(d) By part (b) and Corollary 2.2 we have $[L_1 + L_2 : L_1] < \infty$. Thus, by the isomorphism theorem $[L_2 : L_1 \cap L_2] = [L_1 + L_2 : L_1] < \infty$, and so $L_1 \cap L_2 \in \mathrm{Lat}_K$ by (2.4).

(e) Write $L_2 = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Then

$$(L_1 : L_2)_K = \bigcap_{i=1}^{m} \frac{1}{\alpha_i} L_1 \tag{2.5}$$

because $x \in (L_1 : L_2)_K \Leftrightarrow xL_2 \subset L_1 \Leftrightarrow x\alpha_i \in L_2, \forall i \Leftrightarrow x \in \alpha_i^{-1}L_1, \forall i \Leftrightarrow x \in \cap_i \alpha_i^{-1}L_1$. Now by (a) and (d) we see that the right hand side of (2.5) is a lattice, and hence $(L_1 : L_2)_K \in \mathrm{Lat}_K$.

We can now generalize Corollary 2.2 as follows:

Corollary 2.4 *Let $L_1 \in \mathrm{Lat}_K$, and let $L_2 \leq K$ be a subgroup. Then*

$$L_2 \in \mathrm{Lat}_K \quad \Leftrightarrow \quad [L_i : L_1 \cap L_2] < \infty, \quad \textit{for } i = 1, 2. \tag{2.6}$$

Thus, Lat_K consists of precisely those subgroups of K which are commensurable with L_1.

Proof. ($\Rightarrow$) Corollary 2.3(d) and (2.4).

($\Leftarrow$) Since $[L_1 : L_1 \cap L_2] < \infty$, it follows from (2.4) that $L_1 \cap L_2 \in \mathrm{Lat}_K$. In particular, $L_1 \cap L_2$ is finitely generated, and hence so L_2 because $[L_2 : L_1 \cap L_2] < \infty$. Moreover, L_2 contains a basis of K because $L_1 \cap L_2$ does, and so L_2 satisfies condition (iii) of Proposition 2.1. Thus $L_2 \in \mathrm{Lat}_K$.

We also observe the following fact about lattices.

Proposition 2.5 *The group $\mathrm{Aut}_{\mathbb{Q}}(K) \simeq \mathrm{GL}_n(\mathbb{Q})$ of $\mathbb{Q}$-linear automorphisms of K acts transitively on the set Lat_K, and the stabilizer of $L \in \mathrm{Lat}_K$ is $\mathrm{Aut}(L) \simeq GL_n(\mathbb{Z})$.*

Proof. Let $L \in \mathrm{Lat}_K$. Then by Example 2.3(c) we have $L = L(\alpha_1, \ldots \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis of K. If $T \in \mathrm{Aut}_{\mathbb{Q}}(K)$, then $T(L) = L(T(\alpha_1), \ldots, T(\alpha_n)) \in \mathrm{Lat}_K$ because $T(\alpha_1), \ldots, T(\alpha_n)$ is also a $\mathbb{Q}$-basis of K. Thus $\mathrm{Aut}_{\mathbb{Q}}(K)$ acts on Lat_K.

Moreover, if $L' = L(\alpha_1', \ldots, \alpha_n') \in \mathrm{Lat}_K$ is another lattice, then there is a (unique) $T \in \mathrm{Aut}_{\mathbb{Q}}(K)$ such that $T(\alpha_i) = \alpha_i'$, for $1 \leq i \leq n$, and then $T(L) = L'$. Thus, the action is transitive,

Suppose $T \in \mathrm{Stab}(L)$. Then $T(L) = L$, so $T_{|L} \in \mathrm{Aut}(L)$. Moreover, since L contains a $\mathbb{Q}$-basis of K, the restriction map $\mathrm{Stab}(L) \to \mathrm{Aut}(L)$ is injective. Finally, if $T \in \mathrm{Aut}(L)$, then T extends (uniquely) to a $\mathbb{Q}$-linear map $\tilde{T} \in \mathrm{Aut}_{\mathbb{Q}}(K)$, and clearly $\tilde{T}(L) = T(L) = L$, so $\tilde{T} \in \mathrm{Stab}(L)$, and hence the restriction map $\mathrm{Stab}(L) \to \mathrm{Aut}(L)$ is an isomorphism.

Remark 2.1 For later reference, it is useful to describe the above result more explicitly by fixing a basis $\mathcal{B} := \{\alpha_1, \ldots, \alpha_n\}$ of K. Then we have an isomorphism $t_{\mathcal{B}} : \mathrm{GL}_n(\mathbb{Q}) \xrightarrow{\sim} \mathrm{Aut}_{\mathbb{Q}}(K)$ given by $t_{\mathcal{B}}(g) = T_{g,\mathcal{B}}$, where $T_{g,\mathcal{B}} \in \mathrm{Aut}_{\mathbb{Q}}(K)$ is defined by the rule

$$T_{g,\mathcal{B}}(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i, \ 1 \leq j \leq n, \quad \text{for } g = (a_{ij}) \in \mathrm{GL}_n(\mathbb{Q}); \tag{2.7}$$

cf. Lang[La3], p. 510. Via this isomorphism, we obtain a transitive action of the group $\mathrm{GL}_n(\mathbb{Q})$ on Lat_K, and the stabilizer of $L(\mathcal{B}) := L(\alpha_1, \ldots, \alpha_n)$ is $\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{Q})}(L(\mathcal{B})) = \mathrm{GL}_n(\mathbb{Z})$. We thus have for $g_1, g_2 \in \mathrm{GL}_n(\mathbb{Q})$ that

$$(2.8)\ g_1(L(\mathcal{B})) = g_2(L(\mathcal{B})) \Leftrightarrow g_2^{-1}g_1 \in \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{Q})}(L(\mathcal{B})) = \mathrm{GL}_n(\mathbb{Z}) \Leftrightarrow g_1 \in g_2\mathrm{GL}_n(\mathbb{Z}).$$

We also note that (2.7) and the argument of the proof of Proposition 2.1 show that if $L \in \mathrm{Lat}_K$, then

$$(2.9) \qquad L \subset L(\mathcal{B}) \quad \Leftrightarrow \quad L = g(L(\mathcal{B})), \text{ for some } g \in \mathrm{GL}_n(\mathbb{Q}) \cap M_n(\mathbb{Z}),$$

where $M_n(\mathbb{Z})$ denotes the ring of integral $n \times n$ matrices.

Corollary 2.6 *Let $L_1, L_2 \in \mathrm{Lat}_K$. Then the positive rational number*

$$(2.10) \qquad [L_1 : L_2] := |\det(T)| \quad \textit{for } T \in \mathrm{Aut}_{\mathbb{Q}}(K) \textit{ with } T(L_1) = L_2$$

is independent of the choice of T. Furthermore, L_3 is another lattice, then we have

$$(2.11) \qquad [L_1 : L_2][L_2 : L_3] = [L_1 : L_3].$$

Proof. By Proposition 2.5 there exists $T \in \mathrm{Aut}_{\mathbb{Q}}(K)$ such that $T(L_1) = L_2$. Now if $T_1(L_1) = T_2(L_1) = L_2$, then $T_1^{-1}T_2 \in \mathrm{Stab}(L_1) = \mathrm{Aut}(L_1)$, and so $\det(T_1^{-1}T_2) \in \mathbb{Z}^\times = \{\pm 1\}$. Thus $\det(T_1) = \pm\det(T_2)$, and so $[L_1 : L_2] = |\det(T_i)|$ is independent of the choice of T_i.

To prove (2.11), let $T_i \in \mathrm{Aut}_{\mathbb{Q}}(K)$ be such that $T_1(L_1) = T_2$ and $T_2(L_2) = T_3$. Then $T_2T_1(L_1) = L_3$, so $[L_1 : L_3] = |\det(T_2T_1)| = |\det(T_1)||\det(T_2)| = [L_1 : L_2][L_2 : L_3]$.

Remark 2.2 If $L_1, L_2 \in \mathrm{Lat}_K$ and $L_2 \subset L_1$, then (2.9) shows that $[L_1 : L_2] \in \mathbb{Z}$ is a (positive) integer. In fact, in this case $[L_1 : L_2]$ is equal to *index* of L_2 in L_1, i.e.

$$(2.12) \qquad [L_1 : L_2] = |L_1/L_2|, \quad \text{if } L_2 \subset L_1.$$

To see this, note that the Invariant Factor Theorem 1.5 shows that we can choose a basis $\mathcal{B}$ of L_1 such that $L_2 = T_{g,\mathcal{B}}(L_1)$ where $g = \mathrm{diag}(a_1, a_2, \ldots, a_n)$ is a diagonal matrix (with $a_i \in \mathbb{Z}$, $a_i > 0$). Then $L_1/L_2 \simeq \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$ and so $|L_1/L_2| = a_1a_2\cdots a_n = |\det(T_{g,\mathcal{B}})| = [L_1 : L_2]$, as claimed.

When studying lattices, it is useful to partition them into classes which have the same *order* in the sense of following definition.

Definition. An *order* of a number field K is a lattice R of K which is also a subring of K; in particular, $1 \in R$. The *order* (or *multiplier ring*) of a lattice L is

$$\mathcal{O}(L) = (L : L)_K = \{\alpha \in K : \alpha L \subset L\}.$$

Moreover, we call $N(L) := [\mathcal{O}(L) : L] \in \mathbb{Q}$ the *norm* of L.

The above definition suggests that $\mathcal{O}(L)$ is subring and an order of K. This will be verified now.

Proposition 2.7 (a) *If $L \in \mathrm{Lat}_K$ is a lattice, then $\mathcal{O}(L)$ is an order of K.*

(b) *If R is an order of K, then $\mathcal{O}(R) = R$ and hence there is a lattice $L \in \mathrm{Lat}_K$ such that $\mathcal{O}(L) = R$.*

(c) *If R_1 and R_2 are two orders of K, then also $R_1 \cdot R_2$ and $R_1 \cap R_2$ are orders of K.*

Proof. (a) By Corollary 2.3(e) we know that $\mathcal{O}(L) \in \mathrm{Lat}_K$, so it is enough to show that $\mathcal{O}(L)$ is a subring of K. Clearly $1 \cdot L = L \subset L$, so $1 \in \mathcal{O}(L)$. Moreover, if $x, y \in \mathcal{O}(L)$, then $xL \subset L, yL \subset L$, and hence $xyL \subset xL \subset L$. Thus $xy \in \mathcal{O}(L)$, and so $\mathcal{O}(L)$ is a subring and hence an order of K.

(b) Since R is a lattice, the second assertion follows from the first by taking $L = R$. To prove the first, let $x \in R$. Since R is a ring, $xR \subset R$ so $x \in (R : R)_K$, and hence $R \subset (R : R)_K$. Conversely, since $1 \in R$, we see that if $x \in (R : R)_K$, then $xR \subset R$, so in particular $x = x \cdot 1 \in R$. Thus $(R : R)_K \subset R$, and we have $\mathcal{O}(R) = R$, as desired.

(c) By Corollary 2.3(c),(d) we know that R_1R_2, $R_1 \cap R_2 \in \mathrm{Lat}_K$, so it is enough to show that both are subrings of K. This is obvious for $R_1 \cap R_2$. Now $(R_1R_2)(R_1R_2) = (R_1R_1)(R_2R_2) = R_1R_2$ (because $R_iR_i = R_i$), so R_1R_2 is closed under multiplication. Moreover, since R_1R_2 is also closed under addition (because it is a lattice) and since $1 = 1 \cdot 1 \in R_1R_2$, we see that R_1R_2 is a subring of K.

Notation. If R is any order of K, let

$$\mathrm{Lat}(R) = \{L \in \mathrm{Lat}_K : \mathcal{O}(L) = R\}.$$

We thus obtain a partition of Lat_K as follows:

$$\mathrm{Lat}_K \;=\; \dot{\bigcup_R} \mathrm{Lat}(R),$$

where the union is over all orders R of K. It can be shown that each $\mathrm{Lat}(R)$ is an abelian group with respect to multiplication of lattices (with identity R). This will be verified in the special case when $n = 2$ in the next section.

It is useful to observe that each $L \in \mathrm{Lat}(R)$ is an R-module. More precisely, we have the following result.

Proposition 2.8 (a) *If $R \subset K$ is any subring, and if $L \in \mathrm{Lat}_K$, then*

$$L \text{ is an } R\text{-module} \quad \Leftrightarrow \quad R \subset \mathcal{O}(L). \tag{2.13}$$

In particular, each $L \in Lat_K$ is an $\mathcal{O}(L)$-module.

(b) *If R is an order of K, and if $L \leq K$ is a non-zero subgroup, then*

$$L \text{ is a finitely generated } R\text{-module} \quad \Leftrightarrow \quad L \in \mathrm{Lat}_K \text{ and } R \subset \mathcal{O}(L). \tag{2.14}$$

(c) *Let R be an order of K. If $M \subset K$ is an* invertible *R-module, i.e. if $MM' = R$, for some R-submodule $M' \subset K$, then $M \in \mathrm{Lat}(R)$.*

Proof. (a) Clearly, L is an R-module $\Leftrightarrow rL \subset L, \forall r \in R \Leftrightarrow r \in (L:L)_K = \mathcal{O}(L), \forall r \in R \Leftrightarrow R \subset \mathcal{O}(L)$.

(b) If $L \in \mathrm{Lat}_K$ and $R \subset \mathcal{O}(L)$, then L is an R-module by part (a). Moreover, since L is finitely generated as a $\mathbb{Z}$-module, it is also finitely generated as an R-module. Conversely, if L is a finitely generated R-module, then L is also a finitely generated $\mathbb{Z}$-module (because R is a finite $\mathbb{Z}$-module). Moreover, let $\alpha \in L$, $\alpha \neq 0$. Then $L \subset \alpha R$, and αR is a lattice of K. Thus $L \in \mathrm{Lat}_K$ by condition (iii) Proposition 2.1, and hence also $R \subset \mathcal{O}(L)$ by part (a).

(c) We first show that M is finitely generated. Since M is invertible, there is an R-module $M' \subset K$ such that $MM' = R$, and so there exist $x_1, \ldots x_k \in M$ and $x_1', \ldots, x_k' \in M'$ such that $x_1x_1' + \ldots + x_kx_k' = 1$. We claim that $M = \sum Rx_i$. Clearly, $M \supset \sum Rx_i$. Conversely, if $x \in M$, then $xx_i' \in MM' = R$, and so $x = (xx_1')x_1 + \ldots + (xx_k')x_k \in \sum Rx_i$.

Thus, M is a finitely generated R-module and hence by (2.14) we have that $M \in \mathrm{Lat}_K$ and $R \subset \mathcal{O}(M)$. Conversely, if $x \in \mathcal{O}(M) = (M:M)_K$, then $xM \subset M$ and hence $xR = xMM' \subset MM' = R$, so $x = x \cdot 1 \in R$. Thus $\mathcal{O}(M) = R$, and hence $M \in \mathrm{Lat}(R)$.

Example 2.4 (a) Let $\alpha \in K$ be an *integral element*, i.e. $f(\alpha) = 0$ for some monic polynomial $f \in \mathbb{Z}[x]$. For future reference, note that it follows from Corollary 1.6 of [La3], p. 337 that $\alpha \in K$ is integral if and only its *minimal polynomial* $m_\alpha \in \mathbb{Z}[x]$. (Recall that for any $\alpha \in K$, its minimal polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ is the unique monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ of smallest degree such that $m_\alpha(\alpha) = 0$.) Then

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}, \quad \text{where } d = \deg(m_\alpha)$$

is a subring of K which is a finite $\mathbb{Z}$-module. Thus, $\mathbb{Z}[\alpha]$ is an order of K if and only if $\mathbb{Z}[\alpha] \in \mathrm{Lat}_K \Leftrightarrow d = [K:\mathbb{Q}] \Leftrightarrow K = \mathbb{Q}(\alpha)$.

(b) Let $\mathcal{O}_K$ be the set of all integral elements of K, i.e.

$$(2.15)\ \mathcal{O}_K = \{\alpha \in K : f(\alpha) = 0, \text{ for some monic } f \in \mathbb{Z}[x]\} = \{\alpha \in K : m_\alpha(x) \in \mathbb{Z}[x]\}.$$

It is a standard (but non-trivial) fact that $\mathcal{O}_K$ is a ring; cf. [La3], p. 336. Moreover, $\mathcal{O}_K$ is a lattice of K and hence an order of K because if $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$, then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K \subset \frac{1}{\beta}\mathbb{Z}[\alpha]$ where $\beta = m_\alpha'(\alpha) \in K^\times$, and so $\mathcal{O}_K \in \mathrm{Lat}_K$ by (a) and Proposition 2.1(iv) (together with Corollary 2.2, 2.3(a)).

We also observe the following fact:

$$(2.16) \qquad R \text{ is an order of } K \quad \Rightarrow \quad R \subset \mathcal{O}_K.$$

Indeed, $\alpha \in R \Rightarrow \mathbb{Z}[\alpha] \subset R$ is a finite $\mathbb{Z}$-module $\Rightarrow \alpha$ is integral ([La3], p. 334) $\Rightarrow \alpha \in \mathcal{O}_K$. Thus, $\mathcal{O}_K$ is the unique *maximal order* of K: it is an order which contains all other orders of K.

2.4 Quadratic Orders and Lattices

2.4.1 Quadratic Fields

Let K be a *quadratic field*, i.e. K is a subfield of $\mathbb{C}$ with $[K:\mathbb{Q}]=2$. Then by basic field theory we know that there is a unique non-trivial field automorphism $\sigma=\sigma_K: K\to K$. Moreover, $\sigma_K^2=id_K$ and $\mathrm{Fix}(\sigma):=\{\alpha\in K:\sigma(\alpha)=\alpha\}=\mathbb{Q}$. We thus obtain two maps $tr=tr_K: K\to \mathrm{Fix}(\sigma_K)=\mathbb{Q}$ and $N=N_K: K\to \mathrm{Fix}(\sigma_K)=\mathbb{Q}$ defined by the rules:

$$tr_K(\alpha)=\alpha+\sigma_K(\alpha) \quad \text{and} \quad N_K(\alpha)=\alpha\sigma_K(\alpha), \text{ for } \alpha\in K.$$

Note that tr is a $\mathbb{Q}$-linear map and N_K a quadratic map (in the sense of §2.2), and that for every $\alpha\in K$ we have

$$f_\alpha(x) := (x-\alpha)(x-\sigma(\alpha)) = x^2-tr(\alpha)x+N(\alpha)\in\mathbb{Q}[x]. \tag{2.17}$$

In particular we have

$$\alpha^2=tr(\alpha)\alpha-N(\alpha) \tag{2.18}$$

because $f_\alpha(\alpha)=0$. Note that the minimal polynomial of $\alpha\in K$ is

$$m_\alpha(x)=\begin{cases} f_\alpha(x) & \text{if } \alpha\in K\setminus\mathbb{Q} \\ x-\alpha & \text{if } \alpha\in\mathbb{Q}\end{cases}, \tag{2.19}$$

and that the *discriminant* of f_α is

$$\Delta(\alpha) := \Delta(f_\alpha) = tr(\alpha)^2-4N(\alpha) = (\alpha-\sigma(\alpha))^2. \tag{2.20}$$

Proposition 2.9 *If $d_1,d_2\in\mathbb{Q}^\times$ are non-squares, then*

$$\mathbb{Q}(\sqrt{d_1})=\mathbb{Q}(\sqrt{d_2}) \quad\Leftrightarrow\quad d_1/d_2\in(\mathbb{Q}^\times)^2. \tag{2.21}$$

Thus, the map $d\mapsto\mathbb{Q}(\sqrt{d})$ defines a bijection between the set $Sqf(\mathbb{Z}):=\{d\in\mathbb{Z}: d \text{ is squarefree, } d\neq 1\}$ and the set of quadratic fields.

Proof. If $d_1=c^2d_2$ with $c\in\mathbb{Q}^\times$, then $\sqrt{d_1}=\pm c\sqrt{d_2}$ and so $\mathbb{Q}(\sqrt{d_1})=\mathbb{Q}(\sqrt{d_2})$. Conversely, suppose $\mathbb{Q}(\alpha_1)=\mathbb{Q}(\alpha_2)$, where $\alpha_i:=\sqrt{d_i}\notin\mathbb{Q}$. Then $\alpha_i^2=d_i$, so $m_{\alpha_i}(x)=x^2-d_i$. Thus, by (2.17) and (2.19) we see that $tr(\alpha_i)=0$, so $\sigma(\alpha_i)=-\alpha_i$. Put $c=\alpha_1/\alpha_2$. Then $\sigma(c)=\frac{\sigma(\alpha_1)}{\sigma(\alpha_2)}=\frac{-\alpha_1}{-\alpha_2}=c$, so $c\in\mathrm{Fix}(\sigma)=\mathbb{Q}$. Thus $\alpha_1=c\alpha_2$ and hence $d_1=\alpha_1^2=c^2\alpha_2^2=c^2d_2$, i.e. $d_1/d_2\in(\mathbb{Q}^\times)^2$. This proves (2.21).

Since $Sqf(\mathbb{Z})$ is a system of coset representatives of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2\setminus\{(\mathbb{Q}^\times)^2\}$, we see from (2.21) that the given map is injective. To see that it is surjective, let K be any quadratic field. Then $K\neq\mathbb{Q}$ and $K=\mathbb{Q}(\alpha)$ for any $\alpha\in K\setminus\mathbb{Q}$. By the quadratic formula and (2.17) we see that $\alpha=\frac{1}{2}(tr(\alpha)\pm\sqrt{\Delta(\alpha)})$, so $K=\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{\Delta(\alpha)})$. Since $\Delta(\alpha)=c^2d$ for some $d\in Sqf(\mathbb{Z})$ and $c\in\mathbb{Q}^\times$, we have $K=\mathbb{Q}(\sqrt{d})$, and so the map is surjective and hence bijective.

Remark 2.3 It follows from the above proof that if $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Q}^\times$ is a non-square, then $\sigma_K(\sqrt{d}) = -\sqrt{d}$, and so $\sigma_K(x + y\sqrt{d}) = x - y\sqrt{d}$, if $x, y \in \mathbb{Q}$. Thus

$$tr(\alpha) = 2x, \quad N(\alpha) = x^2 - dy^2, \quad \Delta(\alpha) = 4dy^2, \quad \text{if } \alpha = x + y\sqrt{d}. \tag{2.22}$$

In particular, we see that (K, N_K) is a quadratic space (in the sense of §2.2) with determinant

$$\det(K, N_K) = -4d(\mathbb{Q}^\times)^2 = -d(\mathbb{Q}^\times)^2 \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

By the above result we see that we can describe a quadratic field K uniquely by $d \in Sqf(\mathbb{Z})$ via the rule $K = \mathbb{Q}(\sqrt{d})$. Alternately, we can also describe K by its *fundamental discriminant* Δ_K which is defined as follows.

Definition. A (quadratic) *discriminant* is an integer $\Delta \in \mathbb{Z}$ which is not a square such that $\Delta \equiv 0, 1 \pmod 4$. A *fundamental discriminant* is a discriminant Δ such that either Δ is squarefree or $\frac{\Delta}{4}$ is squarefree and $\frac{\Delta}{4} \not\equiv 1 \pmod 4$.

Observation 2.1 For $d \in Sqf(\mathbb{Z})$, put

$$\Delta_d = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{otherwise.} \end{cases} \tag{2.23}$$

Then it is clear that the map $d \mapsto \Delta_d$ defines a bijection between the set $Sqf(\mathbb{Z})$ and the set $\{\Delta : \Delta \text{ is a fundamental discriminant}\}$ of fundamental discriminants. Note that the inverse of this map is given by $\Delta \mapsto sqf(\Delta)$, where $sqf(n)$ denotes the *square-free part* of an integer $n \neq 0$, i.e. the unique square-free integer n' such that $n = c^2 n'$.

We thus see from Proposition 2.9 that the map $\Delta \mapsto \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{sqf(\Delta)})$ defines a bijection between the set of fundamental discriminants and the set of quadratic fields. We write

$$\Delta_K = \Delta, \quad \text{if } K = \mathbb{Q}(\sqrt{\Delta}) \text{ and } \Delta \text{ is a fundamental discriminant.}$$

By abuse of language, Δ_K is often called the "discriminant of K".

Proposition 2.10 *For any discriminant Δ, there exists a unique fundamental discriminant Δ_{fun} such that $\Delta = c^2\Delta_{fun}$ for some $c \in \mathbb{Z}$.*

Proof. First note that if Δ_{fun} exists, then it is unique. Indeed, if $\Delta = c_i^2\Delta_i$, where $c_i \in \mathbb{Z}$ and Δ_i is a fundamental discriminant for $i = 1, 2$, then $sqf(\Delta_1) = sqf(\Delta) = sqf(\Delta_2)$ and so $\Delta_1 = \Delta_2$ by Observation 2.1.

To prove the existence of Δ_{fun}, write write $\Delta = t^2 d$, where $t \in \mathbb{Z}$ and $d = sqf(\Delta)$ is its squarefree part. Note that $d \neq 1$, so $d \in Sqf(\mathbb{Z})$ because Δ is not a square. Let Δ_d be as in (2.23). We shall prove $\Delta = c^2\Delta_d$, for some $c \in \mathbb{Z}$. Indeed, if $d \equiv 1 \pmod 4$, then $\Delta_d = d$ and so this holds with $c = t$. If $d \not\equiv 1 \pmod 4$, then $\Delta_d = 4d$ and $t^2 d \not\equiv 1 \pmod 4$, so $\Delta = t^2 d \equiv 0 \pmod 4$. Since $4 \not| d$, we must have $2|t^2$, and so $2|t$. Thus, we can take $c = \frac{t}{2} \in \mathbb{Z}$ because $\Delta = (\frac{t}{2})^2\Delta_d$.

Corollary 2.11 *If Δ is a discriminant and K is a quadratic field, then $\sqrt{\Delta} \in K \Leftrightarrow \Delta_{fun} = \Delta_K$.*

Proof. Since Δ is not a square, we have $\sqrt{\Delta} \in K \Leftrightarrow K = \mathbb{Q}(\sqrt{\Delta})$. Since $\Delta = c^2\Delta_{fun}$, with $c \in \mathbb{Q}$ we have $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta_{fun}})$. By Observation 2.1 we then have $\Delta_{fun} = \Delta_K$ for $K = \mathbb{Q}(\sqrt{\Delta})$.

Remark. It also follows from Proposition 2.10 that if Δ is a discriminant, then

$$\Delta \text{ is a fundamental discriminant} \quad \Leftrightarrow \quad \frac{\Delta}{c^2} \text{ is not a discriminant, for all } c^2|\Delta, c^2 \neq 1,$$

i.e. the above definition of "fundamental" agrees with that of Weber[Web], p. 321. Indeed, if $\Delta = \Delta_d$ is fundamental (in the above sense), then it is clearly "Weber-fundamental". Conversely, suppose that Δ is "Weber-fundamental". By Proposition 2.10 we have $\Delta = c^2\Delta_{fun}$ for some $c \in \mathbb{Z}$. But the hypothesis on Δ implies that $c^2 = 1$, so $\Delta = \Delta_{fun}$ is fundamental.

Note that each of the *prime discriminants* $d \in \mathcal{P}^* = \{-4, 8, -8\} \cup \{(-1)^{\frac{p-1}{2}}p : p > 2\}$ (cf. Subsection 1.4.1) is fundamental. In fact, we have (cf. Weber[Web], p. 322):

Proposition 2.12 *An integer Δ is a fundamental discriminant if and only if it is a product $\Delta = d_1 \cdots d_r$ of prime discriminants $d_i \in \mathcal{P}^*$ which are pairwise relatively prime. Moreover, the d_i's are uniquely determined by Δ.*

Proof. Clearly, every such product $\Delta = d_1 \cdots d_r$ has the form $\Delta = d$, $-4d$, $\pm 8d$ where $d \equiv 1 \pmod 4$ is squarefree (and $d \neq 1$, if Δ is odd), and so Δ is a fundamental discriminant.

Conversely, suppose that Δ is a fundamental discriminant, and assume first that $\Delta \equiv 1 \pmod 4$. Then $\Delta \neq 1$ is squarefree, and so $\Delta = (-1)^r p_1 \cdots p_r$, where $r = \#\{i : p_i \equiv 3 \pmod 4\}$. Thus, if we put (as in Subsection 1.4.1) $p_i^* = (-1)^{\frac{p_i-1}{2}}p_i$, then $\Delta = p_1^* \cdots p_r^*$ is a product of prime discriminants $p_i^* \in \mathcal{P}^*$ which are clearly relatively prime (and are uniquely determined by Δ).

Now suppose that $\Delta \equiv 0 \pmod 4$ is a fundamental discriminant. Then by definition we have $\Delta = 4d$, where d is squarefree and $d \not\equiv 1 \pmod 4$, i.e. $d \equiv 2, 3 \pmod 4$. If $d \equiv 3 \pmod 4$, then either $d = -1$ or $-d \equiv 1 \pmod 4$ is a fundamental discriminant. In the former case $\Delta = -4 \in \mathcal{P}^*$ is a prime discriminant, whereas in the latter case $-d = p_1^* \cdots p_r^*$ is a product of odd prime discriminants by what was just shown, and so $\Delta = (-4)p_1^* \cdots p_r^*$ is a product of prime discriminants which are pairwise relatively prime (and are clearly uniquely determined). Finally, if $d \equiv 2 \pmod 4$, then $d = 2\varepsilon d'$ where $d' \equiv 1 \pmod 4$ is squarefree and $\varepsilon \in \{\pm 1\}$. If $d' = 1$, then $\Delta = 8\varepsilon \in \mathcal{P}^*$, and if $d' \neq 1$, then d' is a fundamental discriminant which by the above has the form $d' = p_1^* \cdots p_r^*$, and so $\Delta = (8\varepsilon)p_1^* \cdots p_r^*$ is the desired factorization of Δ into prime discriminants which are pairwise relatively prime.

2.4.2 Quadratic Orders

A *quadratic order* is an order of some quadratic field. As we shall see, each quadratic order R can be characterized uniquely by its discriminant $\Delta(R)$ which will be defined below; cf. Remark 2.4.

Notation. If Δ is a discriminant, put $\omega_\Delta = \frac{\Delta+\sqrt{\Delta}}{2}$ and $\mathcal{O}_\Delta = \mathbb{Z} + \mathbb{Z}\omega_\Delta$.

Proposition 2.13 *Let Δ be a discriminant and K a quadratic field. Then $\omega_\Delta \in K \Leftrightarrow \Delta_{fun} = \Delta_K$. If this is the case, then $\mathcal{O}_\Delta$ is an order of K with $\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta_K}$.*

Proof. We have $\omega_\Delta \in K \Leftrightarrow \sqrt{\Delta} \in K \Leftrightarrow \Delta_{fun} = \Delta_K$, the latter by Corollary 2.11. This proves the first statement. Moreover, to prove that $\mathcal{O}_\Delta$ is order of K, it is enough to verify that $\mathcal{O}_\Delta$ is a subring because $\mathcal{O}_\Delta = L(1, \omega_\Delta)$ is clearly a lattice of K.

For this, we note that since $K = \mathbb{Q}(\sqrt{\Delta})$, it follows from (2.22) (with $x = \frac{\Delta}{2}, y = \frac{1}{2}$) that

$$tr(\omega_\Delta) = \Delta, \quad N(\omega_\Delta) = \frac{1}{4}(\Delta^2 - \Delta), \quad \Delta(\omega_\Delta) = \Delta. \tag{2.24}$$

We thus obtain from (2.18) that $\omega_\Delta^2 = \Delta\omega_\Delta - \frac{1}{4}(\Delta^2 - \Delta) \in \mathbb{Z} + \mathbb{Z}\omega_\Delta = \mathcal{O}_\Delta$ because $\Delta^2 \equiv \Delta\,(4)$, and so $\mathcal{O}_\Delta$ is a subring of K (because clearly $1^2, 1 \cdot \omega_\Delta \in \mathcal{O}_\Delta$).

To prove that $\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta_K}$, write $\Delta = c^2\Delta_{fun} = c^2\Delta_K$ with $c \in \mathbb{Z}$, $c > 0$; cf. Proposition 2.10. Then $\sqrt{\Delta} = c\sqrt{\Delta_K}$, so

$$\omega_\Delta \;=\; \frac{c(c-1)}{2}\Delta_K + c\omega_{\Delta_K} \tag{2.25}$$

because $\omega_\Delta = \frac{1}{2}(c^2\Delta_K + c\sqrt{\Delta_K}) = \frac{1}{2}(c^2\Delta_K - c\Delta_K) + \frac{1}{2}(c\Delta_K + c\sqrt{\Delta_K})$. Thus, $\omega_\Delta \in \mathbb{Z} + \mathbb{Z}\omega_{\Delta_K} = \mathcal{O}_{\Delta_K}$ and hence $\mathcal{O}_\Delta = \mathbb{Z} + \mathbb{Z}\omega_\Delta \subset \mathcal{O}_{\Delta_K}$, as claimed.

As in Example 2.4(b), let $\mathcal{O}_K$ denote the maximal order of K. Then $\mathcal{O}_K = \mathcal{O}_{\Delta_K}$, as we shall see presently. Moreover, we shall also see that every quadratic order R is of the form $R = \mathcal{O}_\Delta$ for a (unique) discriminant Δ.

Proposition 2.14 *Let K be a quadratic field.*

(a) *If $\alpha \in \mathcal{O}_K \setminus \mathbb{Q}$, then $\Delta(\alpha)$ is a discriminant and we have*

$$\mathcal{O}_{\Delta(\alpha)} \;=\; \mathbb{Z} + \mathbb{Z}\alpha. \tag{2.26}$$

(b) *The maximal order of K is $\mathcal{O}_K = \mathcal{O}_{\Delta_K}$, where Δ_K is the fundamental discriminant of K.*

(c) *For every $c \in \mathbb{N}$, there exists a unique order $R = R_{K,c}$ of K such that $[\mathcal{O}_K : R] = c$. Moreover, we have*

$$R_{K,c} \;=\; \mathcal{O}_{c^2\Delta_K} \;=\; \mathbb{Z} + \mathbb{Z}c\omega_{\Delta_K}. \tag{2.27}$$

Proof. (a) By hypothesis, $m_\alpha(x) \in \mathbb{Z}[x]$, and so by (2.19) and (2.17) we see that $tr(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$. Thus $\Delta(\alpha) = tr(\alpha)^2 - 4N(\alpha) \equiv tr(\alpha)^2 \equiv 0, 1 \pmod 4$, and so $\Delta(\alpha)$ is a discriminant. (Note that $\Delta(\alpha)$ cannot be a square in $\mathbb{Q}$ because $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\alpha) = K$).

Now by the quadratic formula and (2.17) we have

$$\alpha \;=\; \frac{1}{2}(tr(\alpha) \pm \sqrt{\Delta(\alpha)}) \;=\; s \pm \omega_{\Delta(\alpha)}, \quad \text{where } s \;=\; \frac{1}{2}(tr(\alpha) \mp \Delta(\alpha)). \tag{2.28}$$

Since $\Delta(\alpha) \equiv tr(\alpha)^2 \equiv tr(\alpha) \pmod 2$, we see that $s \in \mathbb{Z}$, and so $\mathbb{Z} + \mathbb{Z}\alpha = \mathbb{Z} + \mathbb{Z}\omega_{\Delta(\alpha)} = \mathcal{O}_{\Delta(\alpha)}$, as claimed.

(b) Since $\mathcal{O}_{\Delta_K}$ is an order of K by Proposition 2.13, we have $\mathcal{O}_{\Delta_K} \subset \mathcal{O}_K$; cf. (2.16). To prove the opposite inclusion, let $\alpha \in \mathcal{O}_K$. If $\alpha \in \mathbb{Q}$, then $m_\alpha(x) = x - \alpha \in \mathbb{Z}[x]$ (cf. (2.19)), so $\alpha \in \mathbb{Z} \subset \mathcal{O}_{\Delta_K}$. If $\alpha \notin \mathbb{Q}$, then by part (a) and Proposition 2.13 we have $\alpha \in \mathbb{Z} + \mathbb{Z}\alpha = \mathcal{O}_{\Delta(\alpha)} \subset \mathcal{O}_{\Delta_K}$. Thus $\alpha \in \mathcal{O}_{\Delta_K}$ in all cases and so $\mathcal{O}_K \subset \mathcal{O}_{\Delta_K}$. This proves $\mathcal{O}_K = \mathcal{O}_{\Delta_K}$, as claimed.

(c) Put $\Delta = c^2\Delta_K$. Then by (2.25) we have $\mathcal{O}_\Delta = \mathbb{Z} + c\omega_{\Delta_K}\mathbb{Z}$, so the second equality of (2.27) holds. Moreover, it follows from this (and part (b)) that for $\mathcal{B} = \{1, \omega_K\}$ and $g = \mathrm{diag}(1, c)$ we have (in the notation of Remark 2.1) that $T_{g,\mathcal{B}}(\mathcal{O}_K) = T_{g,\mathcal{B}}(L(\mathcal{B})) = \mathcal{O}_\Delta$, so $[\mathcal{O}_K : \mathcal{O}_D] = |\det(g)| = c$; cf. Remark 2.2. Thus, $R_{K,c} = \mathcal{O}_\Delta$ satisfies (2.27). Now suppose that R is any order with $[\mathcal{O}_K : R] = c$. Then $cx \in R$, $\forall x \in \mathcal{O}_K$, so in particular $c\omega_{\Delta_K} \in R$. Thus $\mathcal{O}_\Delta = \mathbb{Z} + c\omega_{\Delta_K}\mathbb{Z} \subset R$. But since $[\mathcal{O}_K : R] = c = [\mathcal{O}_K : \mathcal{O}_\Delta]$, it follows that $R = \mathcal{O}_\Delta = R_{K,c}$, i.e. the order R is uniquely determined by the condition $[\mathcal{O}_K : R] = c$.

Corollary 2.15 *The map $\Delta \mapsto \mathcal{O}_\Delta$ defines a bijection between the set of quadratic discriminants and the set of quadratic orders.*

Proof. If Δ is a discriminant, then $\mathcal{O}_\Delta$ is a quadratic order by Proposition 2.13. Conversely, let R be a quadratic order. Then $R \subset K$ for some quadratic field K which is uniquely determined by R since $K = \mathbb{Q}R$. Thus, $R \subset \mathcal{O}_K$; cf. (2.16). Put $c = [\mathcal{O}_K : R]$. Then $\Delta = c^2\Delta_K$ is uniquely determined by R and we have $R = \mathcal{O}_\Delta$ by Proposition 2.14(c), and so the map $\Delta \to \mathcal{O}_\Delta$ is a bijection.

Remark 2.4 In view of the above Corollary 2.15, each quadratic order R is of the form $R = \mathcal{O}_\Delta$, for a unique discriminant $\Delta = \Delta(R)$, called the *discriminant* of the order R. Note that the proof of the corollary shows that

$$\Delta(R) \;=\; c^2\Delta_K, \quad \text{where } K = \mathbb{Q}R \text{ and } c = [\mathcal{O}_K : R]. \tag{2.29}$$

Furthermore, the index $c = [\mathcal{O}_K : R]$ is called the *conductor* of R (in $\mathcal{O}_K$).

Example 2.5 1) $K = \mathbb{Q}(i)$. Here $d = -1 \not\equiv 1 \pmod 4$, so $\Delta_K = 4d = -4$. Thus $\omega_{\Delta_K} = \omega_{-4} = \frac{-4+\sqrt{-4}}{2} = -2 + i$, and so $\mathcal{O}_K = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$. Thus, every order in K has the form $R_{K,c} = \mathbb{Z}[ci] = \mathbb{Z} + \mathbb{Z}ci$.

2) $K = \mathbb{Q}(\sqrt{-3})$. Here $d = -3 \equiv 1 \pmod 4$, so $\Delta_K = d = -3$. Thus $\omega_{\Delta_K} = \omega_{-3} = \frac{-3+\sqrt{-3}}{2} = -2 + \frac{1+\sqrt{-3}}{2}$, and so $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Thus, every order in K has the form $R_{K,c} = \mathbb{Z}[c\frac{1+\sqrt{-3}}{2}]$. Note that if c is even, then we also have $R_{K,c} = \mathbb{Z}[\frac{c}{2}\sqrt{-3}]$.

2.4.3 Quadratic Lattices

A *quadratic lattice* is a lattice of some quadratic field. Some of these are given by the following construction.

Proposition 2.16 *Let $f = [a, b, c]$ be an integral binary quadratic form of discriminant $\Delta = \Delta(f)$, where Δ is not a square. Then*

$$L(f) \;:=\; \mathbb{Z}a + \mathbb{Z}\frac{-b+\sqrt{\Delta}}{2} \;=\; a(\mathbb{Z} + \mathbb{Z}\tau(f)) \;=\; aL(\tau(f))$$

is an $\mathcal{O}_\Delta$-ideal. Moreover, if f is primitive, then the order of $L(f)$ is

$$\mathcal{O}(L(f)) \;=\; \mathcal{O}_\Delta \tag{2.30}$$

and hence the norm of $L(f)$ is

$$N(L(f)) \stackrel{def}{=} [\mathcal{O}(L(f)) : L(f)] \;=\; |a| \;=\; \operatorname{sign}(a)a. \tag{2.31}$$

In addition, we have

$$L(f)\sigma_K(L(f)) = a\mathcal{O}_\Delta, \tag{2.32}$$

where $K = \mathbb{Q}(\sqrt{\Delta})$, and hence $L(f)$ is an invertible $\mathcal{O}_\Delta$-ideal.

Proof. Put $\beta_1 = \frac{-b+\sqrt{\Delta}}{2}$ and $\beta_2 = \frac{b+\sqrt{\Delta}}{2}$. Then by (2.22) we have $\Delta(\beta_i) = \Delta$ and so $\mathbb{Z} + \mathbb{Z}\beta_i = \mathcal{O}_\Delta$ by (2.26); in particular, $L(f) \subset \mathbb{Z} + \mathbb{Z}\beta_1 = \mathcal{O}_\Delta$. Thus, to show that $L(f)$ is an $\mathcal{O}_\Delta$-ideal, it is enough to show that $L(f)\beta_2 \subset L(f)$. This, however, is immediate because $a \cdot \beta_2 = a\frac{b+\sqrt{\Delta}}{2} = ab + a\frac{-b+\sqrt{\Delta}}{2} \in L(f)$ and $\beta_1 \cdot \beta_2 = \frac{-b^2+\Delta}{4} = \frac{4ac}{4} = ac \in L(f)$, and so $L(f)$ is an $\mathcal{O}_\Delta$-ideal.

Now suppose that f is primitive, i.e. $\gcd(a, b, c) = 1$. We first prove (2.32). Since $\beta_2 = -\sigma_K(\beta_1) = b + \beta_1$ and $\beta_1\beta_2 = ac$, we have

$$\begin{aligned} L(f)\sigma_K(L(f)) &= (\mathbb{Z}a + \mathbb{Z}\beta_1)(\mathbb{Z}a + \mathbb{Z}\beta_2) \;=\; \mathbb{Z}a^2 + \mathbb{Z}\beta_1 a + \mathbb{Z}a\beta_2 + \mathbb{Z}\beta_1\beta_2 \\ &= a(\mathbb{Z}a + \mathbb{Z}c + \mathbb{Z}\beta_2 + \mathbb{Z}\beta_1) \;=\; a(\mathbb{Z}a + \mathbb{Z}c + \mathbb{Z}b + \mathbb{Z}\beta_1) \\ &= a(\mathbb{Z} + \mathbb{Z}\beta_1) \;=\; a\mathcal{O}_\Delta. \end{aligned}$$

This proves (2.32), and so it follows that $L(f)$ is an invertible $\mathcal{O}_\Delta$-module. Thus, by Proposition 2.8(c) we have that $\mathcal{O}(L(f)) = \mathcal{O}_\Delta$, which proves (2.30).

Finally, to prove (2.31), we note that with $\mathcal{B} = \{1, \beta_1\}$ and $g = \left(\begin{smallmatrix} a & -b \\ 0 & 1 \end{smallmatrix}\right)$ we have $T_{g,\mathcal{B}}(\mathcal{O}_\Delta) = L(f)$ and so $[\mathcal{O}_\Delta : L(f)] = |\det(g)| = |a|$; cf. Remark 2.1. In view of (2.30), this proves (2.31).

Corollary 2.17 *Let $f = [a, b, c] \in Q_\Delta$ and put $\beta_f = a\tau(f) = \frac{-b+\sqrt{\Delta}}{2}$ and $K = \mathbb{Q}(\sqrt{\Delta})$. Then*

$$f(x, y) \;=\; \frac{1}{a}N_K(xa - y\beta_f) \;=\; \frac{\operatorname{sign}(a)}{N(L(f))}N_K(xa - y\beta_f), \quad \text{for all } x, y \in \mathbb{Z}. \tag{2.33}$$

Proof. By (2.31) we have $a = \text{sign}(a)N(L(f))$. Thus, by (2.22) we have

$$\begin{aligned} N_K(xa - y\beta_f) &= N_K((xa + \tfrac{b}{2}y) - \tfrac{y}{2}\sqrt{\Delta}) \;=\; (xa + \tfrac{b}{2}y)^2 - (\tfrac{-y}{2})^2\Delta \\ &= a^2x^2 + abxy + \tfrac{b^2y^2}{4} - \tfrac{y^2}{4}(b^2 - 4ac) \;=\; a(xa^2 + bxy + cy^2) \\ &= af(x,y) = \text{sign}(a)N(L(f))f(x,y). \end{aligned}$$

We can refine the previous proposition by characterizing precisely the lattices which are of the form $L(f)$. For this we require the following concept.

Definition. A sublattice $L \leq L'$ of a lattice L' is called *primitive in* L' if we have $L \not\subset nL'$, for all $n \in \mathbb{Z}$, $n > 1$. Moreover, an $\mathcal{O}_\Delta$-ideal L is called *primitive* if it is primitive in $\mathcal{O}_\Delta$ and if $\mathcal{O}(L) = \mathcal{O}_\Delta$. We denote the set of primitive $\mathcal{O}_\Delta$-ideals by $PrId(\mathcal{O}_\Delta)$. .

Proposition 2.18 *Let $L \in \text{Lat}_K$. Then $L = L(f)$, for some $f \in Q_\Delta$ if and only if L is a primitive $\mathcal{O}_\Delta$-ideal. Thus*

$$PrId(\mathcal{O}_\Delta) \;=\; \{L(f) : f \in Q_\Delta\}.$$

In the proof we shall use the following technical fact.

Lemma 2.1 (a) *Let $A \in M_2(\mathbb{Z})$. Then there exist matrices $B, C \in \text{SL}_2(\mathbb{Z})$ such that BA and AC are upper triangular matrices.*

(b) *Let $L = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ be a quadratic lattice, and let $L' \leq L$ be a sublattice. Then L' has a* Hermite basis *with respect to $\{\alpha_1, \alpha_2\}$, i.e. $L' = \mathbb{Z}a\alpha_1 + \mathbb{Z}(b\alpha_1 + d\alpha_2)$, for suitable $a, b, d \in \mathbb{Z}$.*

Proof. (a) Write $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$. If $c = 0$, then we can take $B = C = I$. If $c \neq 0$, choose $x, y \in \mathbb{Z}$ such that $ax + cy = \delta := \gcd(a, c)$ and also $x', y' \in \mathbb{Z}$ such that $cx' + dy' = \delta' := \gcd(c, d)$. Then $B := \left(\begin{smallmatrix} x & y \\ -c/\delta & a/\delta \end{smallmatrix}\right) \in \text{SL}_2(\mathbb{Z})$ and $BA = \left(\begin{smallmatrix} \delta & * \\ 0 & * \end{smallmatrix}\right)$, and similarly $C := \left(\begin{smallmatrix} d/\delta' & x' \\ -c/\delta' & y' \end{smallmatrix}\right) \in \text{SL}_2(\mathbb{Z})$ and $AC = \left(\begin{smallmatrix} * & * \\ 0 & \delta' \end{smallmatrix}\right)$.

(b) Let $\mathcal{B} = \{\alpha_1, \alpha_2\}$. Then by (2.9) $\exists A \in M_2(\mathbb{Z})$ such that $L' = T_{A,\mathcal{B}}(L)$. By part (a) $\exists C \in \text{SL}_2(\mathbb{Z})$ such that $AC = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, for some $a, b, d \in \mathbb{Z}$. By (2.8) we have $T_{AC,\mathcal{B}}(L) = T_{A,\mathcal{B}}(L) = L'$. But $T_{AC,\mathcal{B}}(\alpha_1) = a\alpha_1$ and $T_{AC,\mathcal{B}}(\alpha_2) = b\alpha_1 + d\alpha_2$ (cf. (2.7)), so $L' = \mathbb{Z}a\alpha_1 + \mathbb{Z}(b\alpha_1 + d\alpha_2)$, as desired.

Proof of Proposition 2.18. If $L = L(f)$ with $f \in \mathcal{O}_\Delta$, then by Proposition 2.16 we have that L is an $\mathcal{O}_\Delta$-ideal with $\mathcal{O}(L) = \mathcal{O}_\Delta$. Moreover, L is primitive in $\mathcal{O}_\Delta$ because $L(f) = \mathbb{Z}a + \mathbb{Z}\alpha_f$ and $\{1, \alpha_f\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_\Delta$. Thus $L \in PrId(\mathcal{O}_\Delta)$.

Conversely, if $L \in PrId(\mathcal{O}_\Delta)$ is a primitive $\mathcal{O}_\Delta$-ideal, then by Lemma 2.1(b) (applied to $\alpha_1 = 1$, $\alpha_2 = \omega_\Delta$) there exist $a, B, C \in \mathbb{Z}$ such that $L = \mathbb{Z}a + \mathbb{Z}(B + C\omega_\Delta)$. Note that by replacing $B + C\omega_\Delta$ by $-B - C\omega_\Delta$ (if necessary), we may assume that $C \geq 1$. Now since L is an $\mathcal{O}_\Delta$-ideal we have that $a\omega_\Delta \in L$, so

$$a\omega_\Delta = xa + y(B + C\omega_\Delta), \quad \text{for some } x, y \in \mathbb{Z} \text{ with } y \neq 0.$$

Comparing coefficients (with respect to the basis $\{1, \omega_\Delta\}$ of K) yields $a = yC$ and $xa + yB = 0$, so $B = -xC$. Thus $C|a$ and $C|B$ and so $L \subset C\mathcal{O}_\Delta$. Since L is primitive, it follows that $C = 1$, so $L = \mathbb{Z}a + \mathbb{Z}(B + \omega_\Delta) = \mathbb{Z}a + \mathbb{Z}(\frac{-b+\sqrt{\Delta}}{2})$, where $-b = 2B + \Delta$. Then $\frac{b+\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta$ and so, since L is an $\mathcal{O}_\Delta$-ideal, we have $\frac{\Delta-b^2}{4} = (\frac{-b+\sqrt{\Delta}}{2})(\frac{b+\sqrt{\Delta}}{2}) \in L$, which means that $\frac{\Delta-b^2}{4} = -ca$, for some $c \in \mathbb{Z}$. Thus $\Delta = B^2 - 4ac$, so $f = [a, b, c]$ has discriminant $\Delta(f)$ and hence $L(f) = \mathbb{Z}a + \mathbb{Z}(\frac{-b+\sqrt{\Delta}}{2}) = L$.

It remains to show that f is primitive. For this, put $g = \gcd(a, b, c)$. Then $f = gf'$ where $f' = [a', b', c']$ is primitive with $\Delta(f') = \Delta/g^2 =: \Delta'$, and so we have $L(f) = \mathbb{Z}a + \mathbb{Z}(\frac{-b+\sqrt{\Delta}}{2}) = g(\mathbb{Z}a' + \mathbb{Z}(\frac{-b'+\sqrt{\Delta'}}{2})) = gL(f')$. By (2.30) we know that $\mathcal{O}(L(f')) = \mathcal{O}_{\Delta'}$. But we also have $\mathcal{O}(L(f')) = \mathcal{O}(gL(f')) = \mathcal{O}(L(f)) = \mathcal{O}_\Delta$, so it follows from Corollary 2.15 that $\Delta' = \Delta$ and $g = 1$. Thus f is primitive, i.e. $f \in Q_\Delta$.

Corollary 2.19 *Let $L \in \mathrm{Lat}_K$ with $\mathcal{O}(L) = \mathcal{O}_\Delta$. Then there exist $f \in Q_\Delta$ and $r \in \mathbb{Q}^\times$ such that $L = rL(f)$. Moreover, if $L \subset \mathcal{O}_\Delta$, then $r \in \mathbb{Z}$.*

Proof. By the argument of Proposition 2.1, $\exists n \in \mathbb{N}$ such that $L_0 := nL \subset R := \mathcal{O}_\Delta$. Let $\mathcal{S} = \{t \in \mathbb{N} : L_0 \subset tR\}$. Then $L_0 \subset \cap_{t\in\mathcal{S}} tR = sR$, where $s = \mathrm{lcm}\{t \in \mathcal{S}\}$, and $\frac{1}{s}L_0 \subset R$ is primitive in R. (Indeed, if $\frac{1}{s}L_0 \subset tR$, for some integer $t > 1$, then $L_0 \subset stR$, so $st \in \mathcal{S}$ and then $st|\mathrm{lcm}(\mathcal{S}) = s$, contradiction.) Since $\mathcal{O}(\frac{1}{s}L_0) = \mathcal{O}(L) = \mathcal{O}_\Delta$, Proposition 2.18 shows that $\exists f \in Q_\Delta$ such that $\frac{1}{s}L_0 = L(f)$, and so $L = \frac{1}{n}L_0 = \frac{s}{n}L(f)$. This proves the first assertion and also the second because if $L \subset \mathcal{O}_\Delta$, then we can take $n = 1$.

Corollary 2.20 *Let $L \in \mathrm{Lat}_K$. Then for any $\lambda \in L$ we have $\frac{N_K(\lambda)}{N(L)} \in \mathbb{Z}$ and*

$$\gcd\left(\tfrac{N_K(\lambda)}{N(L)} : \lambda \in L\right) \;=\; 1. \tag{2.34}$$

In particular, if $L \subset \mathcal{O}_K$, then

$$\gcd\left(N_K(\lambda) : \lambda \in L\right) \;=\; N(L). \tag{2.35}$$

Proof. We first observe that

$$N(rL) \;=\; r^2 N(L), \quad \text{for all } L \in \mathrm{Lat}_K,\ r \in \mathbb{Q}^\times. \tag{2.36}$$

Indeed, since $\mathcal{O}(rL) = \mathcal{O}(L)$ and since $[L : rL] = r^2$ (because $T_{g,\mathcal{B}}(L) = rL$ if $g = \mathrm{diag}(r, r)$ and $\mathcal{B}$ is a basis of L), we obtain by using (2.11) that $N(rL) = [\mathcal{O}(L) : rL] = [\mathcal{O}(L) : L][L : rL] = N(L)r^2$.

To prove (2.34), write $\mathcal{O}(L) = \mathcal{O}_\Delta$. Then by Corollary 2.19 there exist $f = [a, b, c] \in Q_\Delta$ and $r \in \mathbb{Q}^\times$ such that $L = rL(f)$. By combining (2.36) with (2.31) we see that $N(L) = r^2 N(L(f)) = r^2|a|$, and so by (2.33) we obtain

$$\frac{N_K(xra - yr\beta_f)}{N(L)} \;=\; \frac{N_K(xa - y\beta_f)}{|a|} \;=\; \mathrm{sign}(a) f(x, y), \quad \text{for all } x, y \in \mathbb{Z}. \tag{2.37}$$

Since $\{ra, r\beta_f\}$ is a basis of $L = rL(f)$, this shows that

$$\left\{ \tfrac{N_K(\lambda)}{N(L)} : \lambda \in L \right\} \;=\; \{\mathrm{sign}(a) f(x,y) : x, y \in \mathbb{Z}\} \;\subset\; \mathbb{Z},$$

which proves the first assertion. From this (2.34) follows because f is primitive. Moreover, if $L \subset \mathcal{O}_K$, then $N_K(\lambda) \in \mathbb{Z}$, for all $\lambda \in L$, and so (2.35) follows directly from (2.34).

Corollary 2.21 *For any $L \in \mathrm{Lat}_K$ we have*

$$L\sigma_K(L) \;=\; N(L)\mathcal{O}(L). \tag{2.38}$$

In particular, for any order R of K we have

$$N(\alpha R) \;= |N_K(\alpha)|, \quad \textit{for all } \alpha \in K. \tag{2.39}$$

Proof. As in the previous proof, $L = rL(f)$ for some $r \in \mathbb{Q}^\times$ and $f \in Q_\Delta$, where $\mathcal{O}(L) = \mathcal{O}_\Delta$. Then by (2.32), (2.31) and (2.36) we have $L\sigma(L) = r^2 L(f)\sigma(L(f)) = r^2 N(L(f))\mathcal{O}_\Delta = N(rL(f))\mathcal{O}_\Delta = N(L)\mathcal{O}(L)$, which proves (2.38).

To deduce (2.39) from this, take $L = \alpha R$. Since $\mathcal{O}(\alpha R) = \mathcal{O}(R) = R$, we obtain from (2.38) that $N(L)R = \alpha R \sigma_K(\alpha R) = \alpha\sigma_K(\alpha)R = |N_K(\alpha)|R$, i.e. $(N(L)/|N_K(\alpha)|)R = R$. From this (2.39) follows because $N(L) > 0$ and because we have (for any lattice L) that

$$rL \subset L,\ r \in \mathbb{Q}^\times \;\Rightarrow\; r \in \mathbb{Z} \quad \text{and} \quad rL = L,\ r \in \mathbb{Q}^\times \;\Rightarrow\; r = \pm 1. \tag{2.40}$$

Indeed, if $rL \subset L = L(\omega_1, \omega_2)$, then $r\omega_1 \in L$ and hence $r\omega_1 = x\omega_1 + y\omega_2$ with $x, y \in \mathbb{Z}$ so $r = x \in \mathbb{Z}$. This proves the first assertion of (2.40), and the second follows from this by observing that $rL = L \Rightarrow rL \subset L$ and $r^{-1}L \subset L$, and so $r \in \mathbb{Z}^\times = \{\pm 1\}$.

The above corollary allows us to deduce the following important result about the set $\mathrm{Lat}(R) = \{L \in \mathrm{Lat}_K : \mathcal{O}(L) = R\}$.

Proposition 2.22 *If R is an order of K, then $L \in \mathrm{Lat}(R)$ if and only if L is an invertible R-submodule of K. Thus*

$$\mathrm{Lat}(R) \;=\; I(R) \;:=\; \{L : L \textit{ is an invertible } R\textit{-submodule of } K\}$$

is an abelian group under multiplication of lattices with identity R. Moreover, the inverse of $L \in \mathrm{Lat}(R)$ is

$$L^{-1} \;=\; (R : L)_K \;=\; \frac{1}{N(L)}\sigma_K(L). \tag{2.41}$$

Proof. If L is an invertible R-submodule of K, then $L \in \mathrm{Lat}(R)$ by Proposition 2.8(c). Conversely, if $L \in \mathrm{Lat}(R)$, then $\mathcal{O}(L) = R$, so L is an R-module (cf. (2.13)) and equation (2.38) shows that L is invertible. (Note that $L' = \frac{1}{N(L)}\sigma(L) \in \mathrm{Lat}(R)$ because $\mathcal{O}(L') =$

$\mathcal{O}(\sigma(L)) = (\sigma(L) : \sigma(L))_K = \sigma((L : L)_K) = \sigma(\mathcal{O}(L)) = \mathcal{O}(L) = R$.) This proves that $\mathrm{Lat}(R) = I(R)$.

Since it is immediate from the definition that the set $I(R)$ is an abelian group under multiplication, the same is true for $\mathrm{Lat}(R)$. Moreover, the fact that $L^{-1} = \frac{1}{N(L)}\sigma_K(L)$ is just a restatement of (2.38). Finally, the first equality of (2.41) is a standard fact: if $LL' = R$, then clearly $L' \subset (R : L)_K = (R : L)_K R = (R : L)_K LL' \subset RL' = L'$, and so $(R : L)_K = L' = L^{-1}$.

Corollary 2.23 *The maximal order $\mathcal{O}_K$ is a* Dedekind domain*, i.e. every non-zero ideal of $\mathcal{O}_K$ is invertible.*

Proof. Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero $\mathcal{O}_K$-ideal. Then $\mathfrak{a} \in \mathrm{Lat}_K$ and $\mathcal{O}_K \subset \mathcal{O}(\mathfrak{a})$; cf. Proposition 2.8. But since $\mathcal{O}(\mathfrak{a})$ is an order, we have $\mathcal{O}(\mathfrak{a}) \subset \mathcal{O}_K$ (cf. (2.16)) and so $\mathcal{O}(\mathfrak{a}) = \mathcal{O}_K$. Thus $\mathfrak{a} \in \mathrm{Lat}(\mathcal{O}_K)$, and hence $\mathfrak{a}$ is invertible by Proposition 2.22.

Remark 2.5 The converse of Corollary 2.23 is also true, i.e. if R is an order of K, then

$$R \text{ is a Dedekind domain} \quad \Leftrightarrow \quad R = \mathcal{O}_K. \tag{2.42}$$

Indeed, $\Leftarrow$ was shown in Corollary 2.23. Conversely, suppose that $R \neq \mathcal{O}_K$, i.e. that $c := [\mathcal{O}_K : R] > 1$. Consider the ideal $\mathfrak{a} = c\mathcal{O}_K$. Then $\mathfrak{a} = \mathbb{Z}c + \mathbb{Z}c\omega_{\Delta_K} \subset \mathbb{Z} + \mathbb{Z}c\omega_{\Delta_K} = R$ (cf. (2.27)), so $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal which is contained in R. Thus $\mathfrak{a}$ is also an R-ideal and $\mathcal{O}(\mathfrak{a}) = \mathcal{O}_K \neq R$, so by Proposition 2.22, $\mathfrak{a}$ is not invertible as an R-ideal. Thus, R is not a Dedekind domain.

Proposition 2.24 *For any two lattices $L_1, L_2 \in \mathrm{Lat}_K$ we have*

$$\mathcal{O}(L_1L_2) = \mathcal{O}(L_1)\mathcal{O}(L_2), \tag{2.43}$$

$$N(L_1L_2) = N(L_1)N(L_2). \tag{2.44}$$

Proof. We first observe that it follows from (2.38) that

$$N(L_1L_2)\mathcal{O}(L_1L_2) = N(L_1)N(L_1)\mathcal{O}(L_1)\mathcal{O}(L_2) \tag{2.45}$$

because $N(L_1L_2)\mathcal{O}(L_1L_2) = (L_1L_2)\sigma(L_1L_2) = L_1L_2\sigma(L_1)\sigma(L_2) = L_1\sigma(L_1)L_2\sigma(L_2) = N(L_1)\mathcal{O}(L_1)N(L_2)\mathcal{O}(L_2)$. Taking $\mathcal{O}(\cdot)$ of both sides of (2.45) and noting that $\mathcal{O}(L_1L_2)$ and $\mathcal{O}(L_1)\mathcal{O}(L_2)$ are both orders (cf. Proposition 2.7), we obtain $\mathcal{O}(L_1L_2) = \mathcal{O}(\mathcal{O}(L_1L_2)) = \mathcal{O}(N(L_1L_2)\mathcal{O}(L_1L_2)) = \mathcal{O}(N(L_1)N(L_1)\mathcal{O}(L_1)\mathcal{O}(L_2)) = \mathcal{O}(\mathcal{O}(L_1)\mathcal{O}(L_2)) = \mathcal{O}(L_1)\mathcal{O}(L_2)$. This proves (2.43). From this and (2.45) it follows that $N(L_1L_2)\mathcal{O}(L_1L_2) = N(L_1)N(L_1)\cdot \mathcal{O}(L_1L_2)$ and so (2.44) follows by using (2.40).

We can apply the above results to prove the following interesting result which connects the composition of forms (cf. subsection 1.4.2) to the product of lattices.

Proposition 2.25 *If $f_i = [a_i, b_i, c_i] \in Q_{\Delta_i}$, for $i = 1, 2$, where $\Delta_i = m_i^2 \Delta_3$ with $(m_1, m_2) = 1$, then this is an integer $n > 0$ and a form $f_3 = [a_3, b_3, c_3] \in Q_{\Delta_3}$ such that*

$$L(f_1)L(f_2) = nL(f_3) \quad \text{and} \quad \text{sign}(a_1)\text{sign}(a_2) = \text{sign}(a_3). \tag{2.46}$$

Moreover, if $\beta_i = \beta_{f_i} = \frac{-b_i + \sqrt{\Delta_i}}{2}$, for $i = 1, 2, 3$, then there is an integral 2×4 matrix P such that for all $\vec{x}_1 = (x_1, y_1)^t, \vec{x}_2 = (x_2, y_2)^t \in \mathbb{Z}^2$ we have

$$(x_1 a_1 - y_1 \beta_1)(x_2 a_2 - y_2 \beta_2) = (x a_3 - y \beta_3) \quad \text{where } (x, y)^t = P(\vec{x}_2 \otimes \vec{x}_1). \tag{2.47}$$

In particular, $(f_3, P) \in C(f_1, f_2)$, i.e. f_3 is a composition of f_1 and f_2 via the matrix P.

Proof. By Proposition 2.16 we have $L(f_i) \subset \mathcal{O}_{\Delta_i} = \mathcal{O}(L(f_i))$ for $i = 1, 2$, and so $L := L(f_1)L(f_2) \subset \mathcal{O}_{\Delta_1}\mathcal{O}_{\Delta_2} = \mathcal{O}(L)$, the latter by (2.43). Moreover, since $(m_1, m_2) = 1$, we see easily that $\mathcal{O}_{\Delta_1}\mathcal{O}_{\Delta_2} = \mathcal{O}_{\Delta_3}$, and so by Corollary 2.19 there exist $f_3 = [a_3, b_3, c_3] \in Q_{\Delta_3}$ and $n \in \mathbb{N}$ such that the first equality of (2.46) holds. Moreover, by replacing f_3 by $f_3' = [-a_3, b_3, -c_3]$ if necessary, we can ensure that the second equation of (2.46) also holds. (Note that $\Delta(f_3') = \Delta(f_3)$ and $L(f_3') = L(f_3)$.)

Since $a_1a_2, a_1\beta_2, \beta_1 a_2, \beta_1\beta_2 \in L(f_1)L(f_2) = nL(f_3) = \mathbb{Z}na_3 + \mathbb{Z}n\beta_3$, it follows that there exist $p_{ij} \in \mathbb{Z}$ such that

$$\begin{aligned} a_1a_2 &= p_{11}na_3 - p_{21}n\beta_3 \\ a_1\beta_2 &= -p_{12}na_3 + p_{22}n\beta_3 \\ \beta_1 a_2 &= -p_{13}na_3 + p_{23}n\beta_3 \\ \beta_1\beta_2 &= p_{14}na_3 - p_{24}n\beta_3, \end{aligned}$$

and then we have

$$\begin{aligned} (x_1a_1 - y_1\beta_1)(x_2a_2 - y_2\beta_2) &= x_1x_2a_1a_2 - x_2y_1\beta_1a_2 - x_1y_2a_1\beta_2 + y_1y_2\beta_1\beta_2 \\ &= x_1x_2(p_{11}na_3 - p_{21}n\beta_3) - x_1y_2(-p_{12}na_3 + p_{22}n\beta_3) \\ &\quad -x_2y_1(-p_{13}na_3 + p_{23}n\beta_3) + y_1y_2(p_{14}na_3 - p_{24}n\beta_3) \\ &= (p_{11}x_1x_2 + p_{12}x_1y_2 + p_{13}y_1x_2 + p_{14}y_1y_2)na_3 \\ &\quad -(p_{21}x_1x_2 + p_{22}x_1y_2 + p_{23}y_1x_2 + p_{24}y_1y_2)n\beta_3 \\ &= xna_3 - yn\beta_3. \end{aligned}$$

This proves (2.47). Moreover, by (2.31), (2.44), (2.46) and (2.36) we have

$$a_1a_2 = n^2a_3 \tag{2.48}$$

because $a_1a_2 = \text{sign}(a_1)N(L(f_1))\text{sign}(a_2)N(L(f_2)) = \text{sign}(a_3)N(nL(f_3)) = \text{sign}(a_3)n^2 \cdot N(L(f_3)) = n^2a_3$. Now by (2.33) and (2.47) we have

$$\begin{aligned} a_1a_2f_1(x_1, y_1)f_2(x_2, y_2) &= N_K(x_1a_1 - y_1\beta_1)N_K(x_2a_2 - y_2\beta_2) \\ &= N_K((x_1a_1 - y_1\beta_1)(x_2a_2 - y_2\beta_2)) \\ &\overset{(2.47)}{=} N_K(xna_3 - yn\beta_3) = n^2N_K(xa_3 - y\beta_3) \\ &= n^2a_3f_3(x, y), \end{aligned}$$

and so by (2.48) (and (2.46)) we obtain

$$f_1(x_1,y_1)f_2(x_2,y_2) \;=\; f_3(x,y), \quad \text{where } (x,y)^t = P(\vec{x}_2 \otimes \vec{x}_1),$$

which means that $(f_3, P) \in C(f_1, f_2)$.

Remark 2.6 A closer look at the proof of Proposition 2.25 shows that P has the form

$$P \;=\; \begin{pmatrix} n & * & * & * \\ 0 & \frac{a_1 m_2}{n} & \frac{a_2 m_1}{n} & \frac{B}{n}, \end{pmatrix} \quad \text{where } B = \frac{b_1 m_2 + b_2 m_1}{2}. \tag{2.49}$$

Indeed, it follows from the definition of the p_{ij}'s and (2.48) that $p_{11} = n$ and $p_{21} = 0$, and the other entries follow similarly by observing that $\beta_i = m_i\beta_3 + \frac{m_i b_3 - b_i}{2}$, for $i = 1, 2$. Note that the displayed entries of P are the same as those of the matrix of Arndt's composition algorithm (Proposition 1.46). In particular, one can show by the same method that $\gcd(a_1 m_2, a_2, n_1, B) = n$ (cf. [Bu], p. 152), and from this we see that P is primitive (in the sense of subsection 1.4.2).

As was promised in subsection 1.4.2, this proposition leads to a second proof of Gauss's composition result. More precisely:

Corollary 2.26 *Let $f_i \in Q_{\Delta_i}$. Then f_1 and f_2 are composable if and only if Δ_1/Δ_2 is a square in $\mathbb{Q}$.*

Proof. If f_1 and f_2 are composable, then $\Delta_1/\Delta_2 \in (\mathbb{Q}^\times)^2$ by Proposition 1.43. Conversely, if $\Delta_1/\Delta_2 \in (\mathbb{Q}^\times)^2$, then $K := \mathbb{Q}(\sqrt{\Delta_1}) = \mathbb{Q}(\sqrt{\Delta_2})$ and so $\Delta_i = c_i\Delta_K$, for some $c_i \in \mathbb{N}$. Put $g = (c_1, c_2)$ and $\Delta_3 = g^2\Delta_K$. Then $\Delta_i = m_i^2\Delta_3$ with $m_i = \frac{c_i}{g}$ and $(m_1, m_2) = 1$, so we can apply Proposition 2.25 to conclude that f_1 and f_2 are composable.

2.4.4 Dedekind's Main Result

As was mentioned in the introduction, Dedekind showed that the theory of binary quadratic forms can be re-interpreted in terms of quadratic lattices, and Propositions 2.16 and 2.25 constituted the first steps in this direction. Next we need to re-interpret the equivalence of quadratic forms in terms of an equivalence relation on lattices. Towards this end we introduce the following concept.

Definition. If R is an integral domain with quotient field K, then its *Picard group* is the quotient group

$$\mathrm{Pic}(R) \;=\; I(R)/P(R),$$

where $P(R) = \{\alpha R : \alpha \in K^\times\}$ is the group of *principal* R-submodules of K and, as in Proposition 2.22, $I(R) = \mathrm{Lat}(R)$ denotes the group of invertible R-submodules of K. We let

$$\pi_R : I(R) \;\to\; \mathrm{Pic}(R) \;=\; I(R)/P(R)$$

denote the quotient map, i.e. $\pi_R(L) = P(R)L = \{\alpha L : \alpha \in K^\times\}$, and say that two invertible R-modules $L_1, L_2 \in I(R)$ are *equivalent* (notation: $L_1 \sim L_2$) if $\pi_R(L_1) = \pi_R(L_2) \Leftrightarrow L_1 = \alpha L_2$, for some $\alpha \in K^\times$.

Proposition 2.27 *If Δ is s discriminant, then the map $f \mapsto \pi_{\mathcal{O}_\Delta}(L(f))$ defines a surjection $\tilde{\lambda}_\Delta : Q_\Delta \to \mathrm{Pic}(\mathcal{O}_\Delta)$ which induces a surjective homomorphism*

$$\lambda_\Delta : Cl(\Delta) \ \to \ \mathrm{Pic}(\mathcal{O}_\Delta).$$

In particular, $\mathrm{Pic}(\mathcal{O}_\Delta)$ *is a finite group.*

In order to prove this, we require the following technical result which shows that equivalent quadratic forms give rise to equivalent lattices (in the sense of the above definition).

Lemma 2.2 *Let Δ be a discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$.*

(a) *If $T \in \mathrm{GL}_2(\mathbb{Z})$ and $\alpha \in K \setminus \mathbb{Q}$, then*

$$L(T(\alpha)) \ = \ \beta L(\alpha), \quad \text{for some } \beta = \beta_{T,\alpha} \in K^\times. \tag{2.50}$$

(b) *If $T \in \mathrm{SL}_2(\mathbb{Z})$ and $f \in Q_\Delta$, then*

$$L(fT) \ = \ \beta L(f), \quad \text{for some } \beta = \beta_{T,f} \in K^\times \text{ with } N_K(\beta) = \frac{fT(1,0)}{f(1,0)}. \tag{2.51}$$

Proof. (a) Write $T = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$. Since $L(\alpha) = \mathbb{Z} + \mathbb{Z}\alpha$ (cf. Example 2.3(b)), we have

$$L(T(\alpha)) = \mathbb{Z} + \mathbb{Z}\frac{x\alpha + y}{z\alpha + w} = \frac{1}{z\alpha + w}(\mathbb{Z}(z\alpha + w) + \mathbb{Z}(x\alpha + y)) = \frac{1}{z\alpha + w}(\mathbb{Z} + \mathbb{Z}\alpha)$$

so (2.50) holds with $\beta_{T,\alpha} = (z\alpha + w)^{-1}$. (Note that $z\alpha + w \neq 0$ for else $\alpha \in \mathbb{Q}$.)

(b) Write $a = f(1,0)$ and $a' = fT(1,0) = f(x,z)$. Using the transformation law[2] (1.42) and (2.50), we obtain $L(fT) = a'L(\tau(fT)) = a'L(T^{-1}(\tau(f))) = a'\beta L(\tau(f)) = \frac{a'\beta}{a}L(f)$, and so the first equation of (2.51) holds with $\beta_{T,f} = \frac{a'\beta}{a} = \frac{a'}{a}\beta_{T^{-1},\tau(f)} = \frac{a'}{a(x - z\tau(f))}$. Since $aN(x - z\tau(f)) = aN(x - z\frac{\beta_f}{a}) = f(x,z) = a'$ by (2.33), assertion (2.51) follows.

Proof of Proposition 2.27. By Propositions 2.16 and 2.22 we know that $L(f) \in \mathrm{Lat}(R) = I(R)$, so the map $\tilde{\lambda}_\Delta$ is well-defined. Moreover, Corollary 2.19 shows that $\tilde{\lambda}_\Delta$ is surjective.

By Lemma 2.2(b) we see that $\tilde{\lambda}_\Delta$ is constant on proper equivalence classes of forms, and hence defines a map $\lambda_\Delta : Q_\Delta/\sim \ = Cl(\Delta) \to \mathrm{Pic}(\mathcal{O}_\Delta)$. Clearly, the surjectivity of $\tilde{\lambda}_\Delta$ implies that λ_Δ is surjective. Finally, Proposition 2.25 shows that λ_Δ is a homomorphism, and so $\mathrm{Pic}(\mathcal{O}_\Delta)$ is a quotient of the finite group $Cl(\Delta)$; in particular, $\mathrm{Pic}(\mathcal{O}_\Delta)$ is finite.

For positive definite forms, Dedekind's main result is the following.

Theorem 2.1 (Dedekind) *If $\Delta < 0$, then*

$$\lambda_\Delta : Cl(\Delta) \ \xrightarrow{\sim} \ \mathrm{Pic}(\mathcal{O}_\Delta)$$

is an isomorphism of groups. In particular,

$$|\mathrm{Pic}(\mathcal{O}_\Delta)| \ = \ h(\Delta), \quad \text{if } \Delta < 0. \tag{2.52}$$

[2]Although this law was only stated in the case that $\tau \in \mathfrak{H}$, it is clear that it also holds for $\tau \in \mathbb{R} \setminus \mathbb{Q}$.

Proof. Since $\lambda_\Delta : Cl(\Delta) \to \mathrm{Pic}(\mathcal{O}_\Delta)$ is a group homomorphism by Proposition 2.27, it is enough to verify that λ_Δ is a bijection. This follows from the following more precise result which constructs an inverse to λ_Δ.

Proposition 2.28 *Let $L \in \mathrm{Lat}(\mathcal{O}_\Delta)$, where $\Delta < 0$, and write $L = \mathbb{Z}\alpha + \mathbb{Z}\beta$ with $\beta/\alpha \in \mathfrak{H}$. Put*

$$f_{\alpha,\beta}(x,y) = N(x\alpha - y\beta)/N(L). \tag{2.53}$$

Then $f_{\alpha,\beta} \in Q_\Delta$, and the class $cl(L) := cl(f_{\alpha,\beta}) \in Cl(\Delta)$ does not depend on the choice of the basis $\{\alpha,\beta\}$ of L. Moreover, the rule $L \mapsto cl(L)$ defines a map

$$\Phi_\Delta : \mathrm{Pic}(\mathcal{O}_\Delta) \to Cl(\Delta)$$

which is inverse to $\lambda_\Delta : Cl(\Delta) \to \mathrm{Pic}(\mathcal{O}_\Delta)$.

Proof. We first observe that if $A \in \mathrm{SL}_2(\mathbb{Z})$ and if $T = T_{A,\mathcal{B}}$, where $\mathcal{B} = \{\alpha,\beta\}$, then $\{T(\alpha), T(\beta)\}$ is another basis of L with the property that $T(\beta)/T(\alpha) \in \mathfrak{H}$. Moreover, we have

$$f_{T(\alpha),T(\beta)}(\vec{x}) = f_{\alpha,\beta}(A^*\vec{x}), \quad \text{for all } \vec{x} \in \mathbb{Z}^2, \text{ where } A^* = \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right) A \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right). \tag{2.54}$$

Indeed, if $A = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ and $\vec{x} = (x,y)^t$, then $A^* = \left(\begin{smallmatrix}a & -b\\ -c & d\end{smallmatrix}\right)$ and so $A^*(\vec{x}) = (ax-by, -cx+dy)^t$. Thus, since $T(\alpha) = a\alpha + c\beta$, $T(\beta) = b\alpha + d\beta$ (cf. (2.7)), we obtain $N(L) f_{T(\alpha),T(\beta)}(\vec{x}) = N_K(xT(\alpha) - yT(\beta)) = N_K(x(a\alpha + c\beta) - y(b\alpha + d\beta)) = N_K((xa - yb)\alpha + (xc - yd)\beta) = N(L) f_{\alpha,\beta}(xa - yb, -xc + yd) = N(L) f_{\alpha,\beta}(A^*\vec{x})$, which proves (2.54).

From this we see that the equivalence class of $f_{\alpha,\beta}$ does not depend on the choice of the basis $\{\alpha,\beta\}$ of L. Indeed, if $\{\alpha',\beta'\}$ is another basis of L with $\beta'/\alpha' \in \mathfrak{H}$, then $\exists A \in \mathrm{SL}_2(\mathbb{Z})$ such that $T(\alpha) = \alpha'$, $T(\beta) = \beta'$, where $T = T_{A,\mathcal{B}}$. (Note that by Remark 2.1 there exists $A \in \mathrm{GL}_2(\mathbb{Z})$ with this property, and the fact that $\beta/\alpha, \beta'/\alpha' \in \mathfrak{H}$ force that $\det(A) = 1$.) Since also $A^* \in \mathrm{SL}_2(\mathbb{Z})$, it follows from (2.54) that $f_{\alpha',\beta'} = f_{\alpha,\beta}A^* \sim f_{\alpha,\beta}$.

We next observe that

$$f_{\lambda\alpha,\lambda\beta} = f_{\alpha,\beta}, \quad \text{for all } \lambda \in K^\times. \tag{2.55}$$

Indeed, since $\{\lambda\alpha, \lambda\beta\}$ is a basis of λL and since $N(\lambda L) = |N_K(\lambda)||N(L) = N_K(\lambda)N(L)$ by (2.44) and (2.39) (and the fact that $N_K(\lambda) > 0$ because $\Delta < 0$), we see that $f_{\lambda\alpha,\lambda\beta}(x,y) = N_K(x\lambda\alpha - y\lambda\beta)/N(\lambda L) = N_K(\lambda(x\alpha - y\beta))/N(\lambda L) = N_K(\lambda)N_K(x\alpha - y\beta))/N(\lambda L) = N_K(x\alpha - y\beta))/(N(L) = f_{\alpha,\beta}(x,y)$, which proves (2.55).

We can now show that $f_{\alpha,\beta} \in Q_\Delta$. By Corollary 2.19 $\exists f = [a,b,c] \in Q_\Delta$ and $r \in \mathbb{Q}^\times$ such that $L = rL(f)$, and so $\{ra, r\beta_f\}$ is a basis of L. Thus, $f_{\alpha,\beta} \sim f_{ra,r\beta_f}$, and so by (2.55) and (2.33) we obtain

$$f_{\alpha,\beta} \sim f_{ra,r\beta_f} = f_{a,\beta_f} = f, \tag{2.56}$$

and so $f_{\alpha,\beta} \sim f \in Q_\Delta$; in particular, $f_{\alpha,\beta} \in Q_\Delta$. We thus see that

$$\Phi_\Delta(L) := cl(f_{\alpha,\beta}), \quad \text{for } L = \mathbb{Z}\alpha + \mathbb{Z}\beta \text{ with } \beta/\alpha \in \mathfrak{H},$$

does not depend on the choice of $\{\alpha, \beta\}$. Moreover, by (2.55) we have that $\Phi_\Delta(\lambda L) = \Phi_\Delta(L)$, for all $\lambda \in K^\times$, and so Φ_Δ induces a map $\Phi_\Delta : \mathrm{Pic}(\mathcal{O}_\Delta) \to Cl(\Delta)$. Moreover, by (2.56) we have that $\Phi_\Delta(\lambda_\Delta(cl(f))) = cl(f)$, for all $f \in Q_\Delta$. Thus, λ_Δ is injective and hence is bijective by Proposition 2.27. It thus follows that Φ_Δ is the inverse of λ_Δ.

Dedekind's Theorem 2.1 may no longer be valid in the case that $\Delta > 0$, as the following example shows.

Example 2.6 Let $\Delta = 12$ and consider $f = [-1, 2, 2] \in Q_{12}$. Then f is not equivalent to $1_\Delta = [1, 0, -3] \sim f_0 = [1, 2, -2]$ because f is reduced and the cycle of $[1, 2, -2]$ is $\{[1, 2, -2], [-2, 2, 1]\}$; cf. [Bu], p. 30. On the other hand,

$$L(f) = \mathbb{Z}(-1) + \mathbb{Z}(-1 + \sqrt{3}) = \mathcal{O}_{12} = \mathbb{Z}(1) + \mathbb{Z}(-1 + \sqrt{3}) = L(f_0),$$

so $\lambda_\Delta(cl(f)) = \lambda(cl(f_0))$, and hence λ_Δ is not injective.

In order to extend Theorem 2.1 to the indefinite case, we thus have to replace the group $\mathrm{Pic}(\mathcal{O}_\Delta)$ by a larger group, as follows.

Notation. Let R be a quadratic order in K, and let

$$P^+(R) \;=\; \{\alpha R : \alpha \in K^\times, N_K(\alpha) > 0\}.$$

Clearly, $P^+(R)$ is a subgroup of $P(R)$. Put $\mathrm{Pic}^+(R) = \mathrm{Lat}(R)/P^+(R)$, and let

$$\pi_R^+ : \mathrm{Lat}(R) = I(R) \;\to\; \mathrm{Pic}^+(R)$$

denote the quotient map. We say that two lattices $L_1, L_2 \in \mathrm{Lat}(R)$ are *properly equivalent* (notation: $L_1 \overset{+}{\sim} L_2$) if $\pi_R^+(L_1) = \pi_R^+(1) \Leftrightarrow L_1 = \alpha L_2$ with $N_K(\alpha) > 0$. Note that the map π_R factors as $\pi_R = \overline{\pi}_R \circ \pi_R^+$, and so $\mathrm{Pic}(R)$ is a quotient of $\mathrm{Pic}^+(R)$.

Remark 2.7 (a) If $\Delta < 0$, then $N_K(\alpha) > 0$ for all $\alpha \in K^\times = \mathbb{Q}(\sqrt{\Delta})^\times$, and so $P^+(R) = P(R)$ and $\mathrm{Pic}^+(R) = \mathrm{Pic}(R)$ in this case.

(b) If $\Delta > 0$, then $K_+ := \{\alpha \in K^\times : N_K(\alpha) > 0\}$ has index 2 in $K^\times$ because we have $K^\times = K_+ \dot\cup \sqrt{\Delta} K_+$. (Note that $N_K(\sqrt{\Delta}) = -\Delta < 0$.) Thus, $c := [P(R) : P^+(R)] \leq 2$ and hence $|\mathrm{Pic}^+(R)| = c|\mathrm{Pic}(R)|$. Moreover:

$$P^+(R) \;=\; P(R) \quad \Leftrightarrow \quad \exists \mu \in R^\times \text{ with } N_K(\mu) < 0. \tag{2.57}$$

Indeed, suppose $\exists \mu \in R^\times$ with $N_K(\mu) < 0$, and let $\alpha R \in P(R)$. If $N_K(\alpha) > 0$, then $\alpha R \in P^+(R)$; otherwise $N_K(\mu\alpha) > 0$ and then $\alpha R = \alpha\mu R \in P^+(R)$. Thus $P(R) = P^+(R)$. Conversely, suppose $P^+(R) \;=\; P(R)$. Then $\sqrt{\Delta} R = \alpha R$, for some $\alpha \in K^\times$ with $N_K(\alpha) > 0$. Put $\mu = \sqrt{\Delta}/\alpha$. Then $\mu R = R$, so $\mu \in R^\times$. Since $N_K(\sqrt{\Delta}) = -\Delta < 0$, we see that $N_K(\mu) < 0$. This proves (2.57).

Theorem 2.2 (Dedekind) *If Δ is any discriminant, then the map*

$$\tilde{\lambda}^+_\Delta : Q_\Delta \to \mathrm{Pic}^+(\mathcal{O}_\Delta)$$

defined by

$$\tilde{\lambda}^+_\Delta(f) = \begin{cases} \pi^+_\Delta(L(f)) & \text{if } a := f(1,0) > 0 \\ \pi^+_\Delta(L(f)\sqrt{\Delta}) & \text{otherwise} \end{cases} \tag{2.58}$$

induces an isomorphism

$$\lambda^+_\Delta : Cl(\Delta) \xrightarrow{\sim} \mathrm{Pic}^+(\mathcal{O}_\Delta).$$

In particular,

$$|\mathrm{Pic}^+(\mathcal{O}_\Delta)| = h(\Delta). \tag{2.59}$$

Proof. This is similar to that of Theorem 2.1. (Note that $\tilde{\lambda}^+_\Delta = \tilde{\lambda}_\Delta$, if $D < 0$.) Here the inverse map $\Phi^+_\Delta : \mathrm{Pic}^+(\mathcal{O}_\Delta) \to Cl(\Delta)$ is given by the rule

$$\Phi^+_\Delta(L) = cl(f_{\alpha,\beta}) \quad \text{if } L = \mathbb{Z}\alpha + \mathbb{Z}\beta \text{ and } (\sigma(\alpha)\beta - \alpha\sigma(\beta))/\sqrt{D} > 0, \tag{2.60}$$

where, as before, $f_{\alpha,\beta}(x,y) = N_K(x\alpha - y\beta)/N(L)$.

Example 2.7 Let $\Delta = 12$. Then $Cl(\Delta) = \{cl(1_\Delta), cl(f)\}$, where $f = [-1,2,2]$; cf. Example 2.6 and/or [Bu], p. 30. Put $R := \mathcal{O}_\Delta = \mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. Then we have

$$\lambda^+_\Delta(cl(1_\Delta)) = \pi^+_R(R) \quad \text{and} \quad \lambda^+_\Delta(cl(f)) = \pi^+_R(L(f)\sqrt{\Delta}) = \pi^+_R(R\sqrt{\Delta}).$$

Note that $\pi^+_R(R) \neq \pi^+_R(R\sqrt{\Delta})$. Indeed, if it were, then by the argument of Remark 2.7(b) we would have a $\mu \in R^\times$ with $N_K(\mu) < 0$, i.e. $N_K(\mu) = -1$. But no such $\mu \in R = \mathbb{Z}[\sqrt{3}]$ exists, for the equation $x^2 - 3y^2 = -1$ cannot have any solution in integers because $x^2 \not\equiv -1 \pmod 3$. Thus, $\pi^+_R(R) \neq \pi^+_R(R\sqrt{\Delta})$, and so we see that the map λ^+_Δ is injective.

2.4.5 Reinterpretation of the representation problem

The theorems of previous subsection show that proper equivalence classes of forms corresponds bijectively to proper equivalence classes of lattices. Since the study of the elements of an equivalence class $cl(f)$ of a form f is closely clonnected with the solution of the Representation Problem 1.2 (as we saw in Subsection 1.3.5), one might expect that the problem itself can be reinterpreted as a problem about lattices. This is indeed the case: the set $\mathrm{Aut}^+(f)\backslash S(f,n)$ has a natural identification with the set $Id_n(\mathcal{O}_\Delta, L(f)^{-1})$ of $\mathcal{O}_\Delta$-ideals of norm n which are properly equivalent to $L(f)^{-1}$; cf. Corollary 2.31 below. In addition, there is a similar interpretations of the set $\mathrm{Aut}^+(f)\backslash P(f,n)$.

We begin with the study of the set $R(f)$ of numbers which are primitively represented by f; cf. Problem 1.1. For this, we introduce the following definition and notation.

Definition. If L is a lattice, then an element $\alpha \in L$ is called *primitive* in L if $\alpha\mathcal{O}(L)$ is a primitive sublattice of L (cf. p. 70). We write

$$\mathrm{Prim}(L) = \{\alpha \in L : \alpha \text{ is primitive in } L\}.$$

Remark 2.8 If $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice, then

$$\text{Prim}(L) = \{x\omega_1 + y\omega_2 : x, y \in \mathbb{Z},\ \gcd(x,y) = 1\}. \tag{2.61}$$

To see this, let $\alpha = x\omega_1 + y\omega_2 \in L$, and put $g = \gcd(x,y)$. Suppose first that $g > 1$. Since $\alpha \in gL$, we have $\alpha\mathcal{O}(L) \subset gL$ because gL is an $\mathcal{O}(L)$-module, and so α is not primitive in L. Conversely, if α is not primitive, then $\alpha \in \alpha\mathcal{O}(L) \subset nL = \mathbb{Z}n\omega_1 + \mathbb{Z}n\omega_2$, for some $n > 1$, and then $x = nx'$ and $y = ny'$ with $x', y' \in \mathbb{Z}$ and so $n|g$. This proves (2.61).

Proposition 2.29 *Let $f = [a,b,c] \in Q_\Delta$, consider the map*

$$k_f : \mathbb{Z}^2 \to K = \mathbb{Q}(\sqrt{\Delta})$$

defined by $k_f(x,y) = ax - \beta_f y$, where $\beta_f = \frac{-b+\sqrt{D}}{2}$. Then for each $n \in \mathbb{Z}$, the map k_f induces a bijections

$$k_{f,n} : S(f,n) \ \tilde{\to}\ \{\alpha \in L(f) : N_K(\alpha) = na\}, \tag{2.62}$$

$$k^*_{f,n} : P(f,n) \ \tilde{\to}\ \{\alpha \in \text{Prim}(L(f)) : N_K(\alpha) = na\}, \tag{2.63}$$

In particular, $n \in P(f)$ if and only if there exists $\alpha \in \text{Prim}(L(f))$ such that $n = \frac{1}{a}N_K(\alpha)$.

Proof. Note first that k_f is injective because a and β_f are linearly independent. Since $k_f(\mathbb{Z}^2) = L(f)$ (by definition), we see that $k_f : \mathbb{Z}^2 \to L(f)$ is a bijection. Moreover, since $N(k_f(x,y)) = af(x,y)$ by (2.33), it follows that the restriction of k_f to $S(f,n)$ induces the desired bijection (2.62). In addition, since $\{a, \beta_f\}$ is a basis of $L(f)$, we see from (2.61) that k_f restricts to the bijection (2.63).

We next show that the group $\text{Aut}^+(f)$ of automorphs can be identified with the group $U_1(\Delta) = U_1(\mathcal{O}_\Delta) := \{\alpha \in \mathcal{O}_\Delta^\times : N(\alpha) = 1\}$ of units of $\mathcal{O}_\Delta$ with norm 1. More precisely:

Proposition 2.30 *Let $f \in Q_\Delta$, and put*

$$\kappa_f(T) = a - c\tau(f), \quad \text{if } T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \text{Aut}^+(f). \tag{2.64}$$

Then κ_f defines an isomorphism of groups $\kappa_f : \text{Aut}^+(f) \tilde{\to} U_1(\Delta)$ with the property that

$$k_f(T(\vec{x})) = \kappa_f(T)k_f(\vec{x}) \quad \text{for all } \vec{x} \in \mathbb{Z}^2,\ T \in \text{Aut}^+(f). \tag{2.65}$$

To prove this, we shall use the following fact.

Lemma 2.3 *Let $f \in Q_\Delta$, and let $T \in \text{SL}_2(\mathbb{Z})$. Then there is a unique $\lambda_{f,T} \in K^\times$ such that*

$$k_f(T(\vec{x})) \ = \ \lambda_{f,T}k_{fT}(\vec{x}), \quad \text{for all } \vec{x} \in \mathbb{Z}^2. \tag{2.66}$$

Proof. We first observe that $\lambda_{f,T}$ is uniquely determined by (2.66). Indeed, since k_f and k_{fT} are injective, we have $k_f(T(\vec{x})) \neq 0$ and $k_{fT}(\vec{x}) \neq 0$, when $\vec{x} \neq \vec{0}$, and so $\lambda_{f,T} = k_f(T(1,0))/k_{fT}(1,0) \neq 0$ is uniquely determined by f and T.

To prove the existence of $\lambda_{f,T}$, we first observe that by (2.31) we have

$$k_f(x,y) = A(x - y\tau(f)) = \mathrm{sign}(f)N(L(f))[(x,y)\cdot(1,-\tau(f))] \tag{2.67}$$

where $f = [A,*,*]$, $\mathrm{sign}(f) = \mathrm{sign}(A)$ and $\cdot$ denotes the dot-product of two vectors. Next we note that if $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in \mathbb{C}$, then we have

$$T(\vec{x})\cdot(1,-\alpha) \;=\; \beta_{T,\alpha}[\vec{x}\cdot(1,-T^{-1}(\alpha))], \quad \forall \vec{x} \in \mathbb{Z}^2, \tag{2.68}$$

where $\beta_{T,\alpha} = a - c\alpha$. Indeed, writing $\vec{x} = (x,y)$, then we have $\beta_{f,T}[\vec{x}\cdot(1,-T^{-1}(\alpha))] = \beta_{f,T}\left(x - y\left(\frac{d\alpha - b}{-c\alpha + a}\right)\right) = x(a-c\alpha) - y(d\alpha - b) = (ax+by) - \alpha(cx+dy) = T(\vec{x})\cdot(1,-\alpha)$.

In addition, we note that by (2.51) we have $L(fT) = \lambda_1 L(f)$, for some $\lambda_1 \in K = \mathbb{Q}(\sqrt{\Delta})$, and so $N(L(fT)) = |N_K(\lambda_1)|N(L)$ by (2.44) and (2.39). Thus, since $T^{-1}\tau(f) = \tau(fT)$ by (1.42), we obtain

$$\begin{aligned} k_f(T(\vec{x})) &\overset{(2.67)}{=} \mathrm{sign}(f)N(L(f))[T(\vec{x})\cdot(1,-\tau(f))] \\ &\overset{(2.68)}{=} \mathrm{sign}(f)|N(\lambda_1)|^{-1}N(L(fT))\beta_{T,\tau(f)}[\vec{x}\cdot(1,-\tau(fT))] \\ &\overset{(2.67)}{=} \lambda_{f,T}k_{fT}(\vec{x})), \end{aligned}$$

with $\lambda_{f,T} = \mathrm{sign}(f)\mathrm{sign}(fT)|N(\lambda_1)|^{-1}\beta_{T,\tau(f)}$. This proves (2.66).

Proof of Proposition 2.30. We first observe that

$$\kappa_f(T) \;=\; \frac{k_f(T(1,0))}{k_f(1,0)} \;=\; \lambda_{f,T}, \quad \text{if } T \in \mathrm{Aut}^+(f). \tag{2.69}$$

Indeed, the second equality is clear from (2.66) (and the fact that $fT = f$). Moreover, if $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $f = [A,B,C]$, then $T(1,0) = (a,c)$ and so $k_f(T(1,0))/k_f(1,0) = A(a - c\tau(f))/A = \kappa_f(T)$. This proves (2.69) and hence (2.65) follows from (2.66). Moreover, we see that $N_K(\kappa_f(T)) = 1$ because by (2.69) and (2.33) we have $N_K(\kappa_f(T)) = \frac{N_K(k_f(T(1,0)))}{N_K(k_f(1,0))} = \frac{Af(T(1,0))}{Af(1,0)} = 1$ since $f(T(1,0)) = (fT)(1,0) = f(1,0)$.

Next we note that $\kappa_f(T) \in \mathcal{O}_\Delta^\times$. For this we observe that by (2.65) we have $L(f) = k_f(\mathbb{Z}^2) = k_f(T(\mathbb{Z}^2)) = \kappa_f(T)k_f(\mathbb{Z}^2) = \kappa_f(T)L(f)$. Thus $L(f) = \kappa_f(T)L(f)$ and so $\kappa_f(T) \in \mathcal{O}(L(f))^\times = \mathcal{O}_D^\times$. (Note that $L = \lambda L \Rightarrow \lambda, \lambda^{-1} \in \mathcal{O}(L) = (L:L)_K$ because $\lambda^{-1}L = L$.) Thus $\kappa_f(T) \in U_1(\Delta)$, and so we have a map $\kappa_f : \mathrm{Aut}^+(f) \to U_1(\Delta)$. This is a homomorphism because for $T_1, T_2 \in \mathrm{Aut}^+(f)$ and $\vec{x} \in \mathbb{Z}^2$ we have by (2.65) that $\kappa_f(T_1T_2)k_f(\vec{x}) = k_f((T_1T_2)(\vec{x})) = \kappa_f(T_1)k_f(T_2(\vec{x})) = \kappa_f(T_1)\kappa_f(T_2)k_f(\vec{x})$, and hence $\kappa_f(T_1T_2) = \kappa_f(T_1)\kappa_f(T_2)$.

It is immediate that κ_f is injective. Indeed, if $\kappa_f(T) = 1$, then $k_f(T(\vec{x})) = k_f(\vec{x})$, for all $\vec{x} \in \mathbb{Z}^2$. Since k_f is injective, this means $T(\vec{x}) = \vec{x}$, for all $\vec{x} \in \mathbb{Z}^2$ and so $T = I$.

Finally, to show that κ_f is surjective, let $\alpha \in U_1(\Delta)$. Since $\alpha \in \mathcal{O}_\Delta$, we have $\alpha = \frac{1}{2}(x + y\sqrt{\Delta})$ where $x, y \in \mathbb{Z}$ satisfy $x + By \equiv x + \Delta y \equiv 0(2)$. Thus, the matrix

$$T_f(\alpha) = \begin{pmatrix} \frac{x+yB}{2} & Cy \\ -Ay & \frac{a-yB}{2} \end{pmatrix}, \quad \text{where } f = [A, B, C],$$

has integral entries and has determinant $\det(T_f(\alpha)) = \frac{1}{4}(x^2 - \Delta y^2) = N_K(\alpha) = 1$. Thus, $T_f(\alpha) \in \mathrm{SL}_2(\mathbb{Z})$. Moreover, it is easy to check that $T_f(\alpha) \in \mathrm{Aut}^+(f)$; cf. [Bu], p. 31. Since $\kappa_f(T_f(\alpha)) = \frac{1}{2}(x + yB) - (-Ay)\tau(f) = \frac{1}{2}[(x + yB) + y(-B + \sqrt{\Delta})] = \alpha$, it follows that κ_f is surjective and hence an isomorphism.

Finally, we can interpret the (finite) sets $\mathrm{Aut}^+(f)\backslash S(f,n)$ and $\mathrm{Aut}^+(f)\backslash P(f,n)$ (which were studied in subsection 1.3.5) in terms of sets of invertible $\mathcal{O}_\Delta$-ideals.

Notation. Let $L \in \mathrm{Lat}(R)$, and let n be a positive integer. We let

$$Id_n^+(R, L) \;=\; \{L' \in \mathrm{Lat}(R) : L' \subset R,\, N(L') = n,\, L' \overset{+}{\sim} L\}$$

denote the set of invertible R-ideals of norm n which are properly equivalent to L. Moreover, as on p. 70, we let $PrId(R)$ denote the set of primitive R-ideals.

Corollary 2.31 *If $f = [a, b, c] \in Q_\Delta$ with $a > 0$ and if $n > 0$, then the rule $\vec{x} \mapsto k_f(\vec{x})L(f)^{-1}$ induces bijections*

$$\bar{k}_{f,n} : \mathrm{Aut}^+(f)\backslash S(f,n) \;\overset{\sim}{\to}\; Id_n^+(\mathcal{O}_\Delta, L(f)^{-1}) \tag{2.70}$$

$$\bar{k}^*_{f,n} : \mathrm{Aut}^+(f)\backslash P(f,n) \;\overset{\sim}{\to}\; Id_n^+(\mathcal{O}_\Delta, L(f)^{-1}) \,\cap\, PrId(\mathcal{O}_\Delta). \tag{2.71}$$

Proof. If $\vec{x} \in S(f,n)$, then by (2.62) we have $k_f(\vec{x}) \in L(f)$, so $L' := k_f(\vec{x})L(f)^{-1} \subset L(f)L(f)^{-1} = \mathcal{O}_\Delta$ is an invertible $\mathcal{O}_\Delta$-ideal. Moreover, by (2.62) we also have that $N_K(k_f(\vec{x})) = na > 0$, and so $L' \overset{+}{\sim} L(f)^{-1}$ with norm $N(L') = |N(k_f(\vec{x})|N(L(f)^{-1}) = naN(L(f))^{-1} = n$ by (2.31). Thus, $L' \in Id(L(f)^{-1}, n)$. Moreover, if $T \in \mathrm{Aut}^+(f)$, then by (2.65) we have $k_f(T(\vec{x}))L(f)^{-1} = \kappa_f(T)k_f(\vec{x})L(f)^{-1} = k_f(\vec{x})L(f)^{-1}$ because $\kappa_f(T) \in \mathcal{O}_\Delta^\times$. Thus, the given rule defines a map $\bar{k}_{f,n} : \mathrm{Aut}^+(f)\backslash S(f,n) \to Id(L(f)^{-1}, n)$.

If $L' \in Id(L(f)^{-1}, n)$, then $L' = \alpha L(f)^{-1} \subset \mathcal{O}_\Delta$ with $N_K(\alpha) > 0$ and $N(L') = n$. By reversing the above calculations we see that $\alpha \in L(f)$ and $N_K(\alpha) = na$. By (2.65), $\exists \vec{x} \in S(f,n)$ such that $\alpha = k_f(\vec{x})$, and so the map is surjective.

To show that $\bar{k}_{f,n}$ is injective, let $\vec{x}_1, \vec{x}_2 \in S(f,n)$ be such that $k_f(\vec{x}_1)L(f)^{-1} = k_f(\vec{x}_2)L(f)^{-1}$. Then $u := k_f(\vec{x}_2)/k_f(\vec{x}_1) \in \mathcal{O}_\Delta^\times$ and so $u \in U_1(\Delta)$ because $N_K(u) = \frac{na}{na} = 1$. Thus, by Proposition 2.30 $\exists T \in \mathrm{Aut}^+(f)$ such that $\kappa_f(T) = u$, and then (2.65) shows that $k_f(T(\vec{x}_1)) = \kappa_f(T)k_f(\vec{x}_1) = k_f(\vec{x}_2)$, so $T(\vec{x}_1) = \vec{x}_2$ because k_f is injective. This shows that $\bar{k}_{f,n}$ is injective and hence bijective. This proves (2.70). From this, (2.71) follows readily by using (2.63) and the obvious fact that $\alpha \in \mathrm{Prim}(L(f)) \Leftrightarrow \alpha L(f)^{-1} \in PrId(\mathcal{O}(L(f)))$.

2.4.6 The Homomorphism $\bar{\rho} : \mathrm{Pic}(\mathcal{O}_\Delta) \to \mathrm{Pic}(\mathcal{O}_K)$

We now want to compare the Picard group $\mathrm{Pic}(R)$ of a quadratic order R with the Picard group of its maximal order $\mathcal{O}_K$ or, more generally, with that of any order R' containing R. This will be done by studying the following map $\rho = \rho_{R,R'} : \mathrm{Lat}(R) \to \mathrm{Lat}(R')$.

Proposition 2.32 *Let $R \subset R'$ be two quadratic orders, and let $\rho = \rho_{R,R'} : \mathrm{Lat}(R) \to \mathrm{Lat}(R')$ be defined by $\rho(L) = LR'$. Then ρ is a homomorphism with finite kernel*

$$\begin{aligned} \mathrm{Ker}(\rho) &= \{L \in \mathrm{Lat}_K : LR' = R' \text{ and } [R' : L] = [R' : R]\} \\ &= \{L \in \mathrm{Lat}(R) : L \subset R' \text{ and } [R' : L] = [R' : R]\}. \end{aligned} \tag{2.72}$$

Proof. If $L \in \mathrm{Lat}(R)$, then by (2.43) we have $\mathcal{O}(LR') = \mathcal{O}(L)\mathcal{O}(R') = RR' = R'$, so $\rho(L) \in \mathrm{Lat}(R')$. Thus, ρ defines a map $\rho : \mathrm{Lat}(R) \to \mathrm{Lat}(R')$. Moreover, ρ is a homomorphism because $\rho(L_1)\rho(L_2) = L_1R'L_2R' = L_1L_2R'R' = L_1L_2R' = \rho(L_1L_2)$.

To prove (2.72), let $L \in \mathrm{Ker}(\rho)$. Then $LR' = R'$. Since R' is an order, we have $N(R') = [\mathcal{O}(R') : R'] = [R' : R'] = 1$, and so we have by (2.44) that $N(L) = N(L)N(R') = N(LR') = N(R') = 1$. Thus, since $\mathcal{O}(L) = R$, we obtain that $[R' : R] = [R' : R]N(L) = [R' : R][R : L] = [R' : L]$, and so $L \in \mathcal{K}_1 := \{L \in \mathrm{Lat}_K : LR' = R'$ and $[R' : L] = [R' : R]\}$. Thus $\mathrm{Ker}(\rho) \subset \mathcal{K}_1$.

Next, if $L \in \mathcal{K}_1$, then $L = L \cdot 1 \subset LR' = R'$, i.e. $L \subset R'$. Moreover, by (2.43) we have $\mathcal{O}(L)\mathcal{O}(R') = \mathcal{O}(LR') = \mathcal{O}(R') = R'$, so $\mathcal{O}(L) \subset R'$. In addition, as above we have $N(L) = 1$ because $N(L) = N(L)N(R') = N(LR') = N(R') = 1$. Thus $[R' : R] = [R' : L] = [R' : L]/N(L) = [R' : L]/[\mathcal{O}(L) : L] = [R' : \mathcal{O}(L)]$, and so $R = \mathcal{O}(L)$ because R is the only suborder of R' of index $[R' : R]$. Thus $L \in \mathrm{Lat}(R)$ and hence $L \in \mathcal{K}_2 := \{L \in \mathrm{Lat}(R) : L \subset R'$ and $[R' : L] = [R' : R]\}$. This proves $\mathcal{K}_1 \subset \mathcal{K}_2$.

Now let $L \in \mathcal{K}_2$. Then $N(L) = [R : L] = [R : L]/[R' : R] = 1$, and hence $N(LR') = N(L)N(R') = 1 \cdot 1 = 1$. Now since $\mathcal{O}(LR') = \mathcal{O}(L)\mathcal{O}(R') = RR' = R'$, we thus have $1 = N(LR') = [R' : LR']$. But since $L \subset R'$, we have $LR' \subset R'$ and so this forces $LR' = R'$. Thus $L \in \mathrm{Ker}(\rho)$, and so $\mathcal{K}_2 \subset \mathrm{Ker}(\rho)$. We thus have the inclusions $\mathrm{Ker}(\rho) \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \mathrm{Ker}(\rho)$, which proves (2.72).

Note that it follows from (2.72) that $\mathrm{Ker}(\rho)$ is finite because if we put $n = [R' : R]$, then we have $|\mathrm{Ker}(\rho)| \le \#\{L \le R' : [R' : L] | n\} = \#(\text{subgroups of } R'/nR') < \infty$, the latter because R'/nR' is a finite group.

We observe that $\rho_{R,R'}$ induces homomorphisms

$$\bar{\rho}_{R,R'} : \mathrm{Pic}(R) \to \mathrm{Pic}(R') \quad \text{and} \quad \bar{\rho}^+_{R,R'} : \mathrm{Pic}^+(R) \to \mathrm{Pic}^+(R')$$

because $\rho_{R,R'}(xR) = xR'$ for $x \in K^\times$, and hence $\rho_{R,R'}(P(R)) = P(R')$ and $\rho_{R,R'}(P^+(R)) = P^+(R')$. Note that via the basic identifications of the Picard groups with classes of forms (cf. Theorems 2.1 and 2.2), the above maps correspond to compositions of forms. More precisely, it follows from the definitions and Proposition 2.25 that we have

$$\bar{\rho}_{\mathcal{O}_\Delta,\mathcal{O}_{\Delta'}}(\lambda_\Delta(cl(f))) = \lambda_{\Delta'}(cl(f \circ 1_{\Delta'})), \quad \bar{\rho}^+_{\mathcal{O}_\Delta,\mathcal{O}_{\Delta'}}(\lambda^+_\Delta(cl(f))) = \lambda^+_{\Delta'}(cl(f \circ 1_{\Delta'})). \tag{2.73}$$

We next observe that the kernels of $\bar{\rho}_{R,R'}$ and of $\bar{\rho}_{R,R'}$ are closely related to the kernel of $\rho_{R,R'}$:

Proposition 2.33 *The rule $\alpha \mapsto \alpha R$ induces isomorphisms*

$$(2.74)\quad \mu : (R')^\times/R^\times \xrightarrow{\sim} \mathrm{Ker}(\rho_{R,R'}) \cap P(R),\ \mu^+ : U_1(R')/U_1(R) \xrightarrow{\sim} \mathrm{Ker}(\rho_{R,R'}) \cap P^+(R),$$

and these lead to the exact sequences

$$(2.75)\qquad 0 \to (R')^\times/R^\times \xrightarrow{\mu} \mathrm{Ker}(\rho_{R,R'}) \xrightarrow{\pi_R} \mathrm{Ker}(\bar{\rho}_{R,R'}) \to 0,$$

$$(2.76)\qquad 0 \to U_1(R')/U_1(R) \xrightarrow{\mu^+} \mathrm{Ker}(\rho_{R,R'}) \xrightarrow{\pi_R^+} \mathrm{Ker}(\bar{\rho}^+_{R,R'}) \to 0.$$

Proof. Consider the homomorphism $\tilde{\mu} : (R')^\times \to P(R)$ defined by $\tilde{\mu}(\alpha) = \alpha R$. Since $\tilde{\mu}(\alpha)R' = \alpha R' = R'$, it is clear that $\tilde{\mu}(\alpha) \in \mathrm{Ker}(\rho) \cap P(R)$. Moreover, if $L = \alpha R \in \mathrm{Ker}(\rho) \cap P(R)$, then $R' = LR' = \alpha R'$, so $\alpha \in (R')^\times$, and hence $L \in \mathrm{Im}(\tilde{\mu})$. Thus $\mathrm{Im}(\tilde{\mu}) = \mathrm{Ker}(\rho) \cap P(R)$. Now $\alpha \in \mathrm{Ker}(\tilde{\mu}) \Leftrightarrow \alpha R = R \Leftrightarrow \alpha \in R^\times$, i.e. $\mathrm{Ker}(\tilde{\mu}) = R^\times$. We thus obtain the desired isomorphism $\mu : (R')^\times/R^\times \xrightarrow{\sim} \mathrm{Ker}(\rho) \cap P(R)$. Since the construction of μ^+ is similar, this proves (2.74).

Next, consider the restriction π of π_R to $\mathrm{Ker}(\rho)$. Then $\pi(\mathrm{Ker}(\rho)) \subset \mathrm{Ker}(\bar{\rho})$ because $\pi_{R'} \circ \rho = \bar{\rho} \circ \pi_R$, and so π defines a homomorphism $\pi : \mathrm{Ker}(\rho) \to \mathrm{Ker}(\bar{\rho})$. This map is surjective, for if $LP(R) \in \mathrm{Ker}(\bar{\rho})$, then $LR' \in P(R')$, so $LR' = xR'$ for some $x \in K^\times$, and then $\frac{1}{x}L \in \mathrm{Ker}(\rho)$ and $\pi(\frac{1}{x}L) = LP(R)$. Thus, since $\mathrm{Ker}(\pi) = \mathrm{Ker}(\rho) \cap P(R)$, we see from (2.74) that (2.75) is exact. The proof of (2.76) is analogous.

We next want to show that $\rho_{R,R'}$ and hence $\bar{\rho}_{R,R'}$ and $\bar{\rho}^+_{R,R'}$ are surjective. For this, we shall study the restriction of $\rho_{R,R'}$ to certain subgroups $I(R,m) \leq \mathrm{Lat}(R)$ which are defined as follows.

Definition. Let R be a quadratic order , and let $m \geq 1$ be an integer. A lattice $L \in \mathrm{Lat}(R)$ is said to be *prime to m* if $L + mR = R$. If this is the case, then $L \subset R$, so L is an invertible R-ideal. We let $Id(R,m)$ denote the set of invertible R-ideals which are prime to m, i.e.

$$Id(R,m) \;=\; \{L \in \mathrm{Lat}(R) : L + mR = R\}.$$

Furthermore, we let $I(R,m) = \langle Id(R,m)\rangle \leq I(R) = \mathrm{Lat}(R)$ denote the subgroup of $\mathrm{Lat}(R)$ generated by $Id(R,m)$. We first observe:

Proposition 2.34 *Let R be an order in K, and let $L \in \mathrm{Lat}(R)$. If $m \geq 1$ is an integer, then there exists $\lambda \in K_+ = \{\lambda \in K : N_K(\lambda) > 0\}$ such that $\lambda L \in Id(R,m)$. Thus $Id(R,m)P^+(R) = Id(R,m)P(R) = \mathrm{Lat}(R)$.*

Proof. By Corollary 2.19 we have that $L = rL(f)$, for some $f \in Q_\Delta$ and $r \in \mathbb{Q}^\times$. Moreover, by Proposition 1.39 and/or its refinement Lemma 2.4 below, $\exists n \in R(f)$ such

that $(n,m) = 1$ and $\text{sign}(n) = \text{sign}(f(1,0))$, and so by Proposition 1.6 $\exists T \in \text{SL}_2(\mathbb{Z})$ such that $f_1 := fT = [n,*,*]$. Clearly $L(f_1) \in Id(R,m)$ because $1 \in mR + L(f_1) = mR + \mathbb{Z}n + \mathbb{Z}\beta_{f_1}$. Moreover, by Lemma 2.2(b) $\exists \lambda' \in K^\times$ such that $\lambda' L(f) = L(f_1)$ and $N_K(\lambda') = \frac{n}{f(1,0)} > 0$. Thus, if we put $\lambda = \frac{\lambda'}{r}$, then $\lambda \in K_+$ and $\lambda L = \lambda' L(f) = L(f_1) \in Id(R,m)$, as desired.

In the above proof we used the following refinement of Proposition 1.39.

Lemma 2.4 *If $f = [a,b,c]$ is primitive, then for any integer $d \geq 1$, there exist integers $n_1, n_2 \in R(f)$ such that $(n_i, d) = 1$ and $\text{sign}(n_1) = \text{sign}(a)$ and $\text{sign}(n_2) = \text{sign}(c)$.*

Proof. Choose x_2, x_3, x_4 as in the proof of Proposition 1.39, so $n := f(x_2, x_3, x_4) \in R(f)$ satisfies $(n,d) = 1$. Now choose any prime p with $p \nmid acd$. Then the same proof (with d replaced by dp and x_4 replaced by $x_4 p$) shows that $m_p := f(x_2, x_3, x_4 p)$ satisfies $(m_p, dp) = 1$. Now if p is sufficiently large, then $\text{sign}(m_p) = \text{sign}(c)$, so we can take $n_2 = m_p$, provided that p is sufficiently large.

Applying the above argument to $f_1 := [c,b,a]$ shows that there exists $n_1 \in R(f_1)$ such that $(n_1, d) = 1$ and $\text{sign}(n_1) = \text{sign}(a)$. But since $f_1 = f \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \approx f$, we have $R(f) = R(f_1)$ by Proposition 1.3, and so the assertion follows.

Corollary 2.35 *Let $P(R,m) := P(R) \cap I(R,m)$ and $P^+(R,m) := P^+(R) \cap I(R,m)$. Then the inclusion map $j_{R,m} : I(R,m) \hookrightarrow I(R)$ induces isomorphisms*

$$\bar{j}_{R,m} : I(R,m)/P(R,m) \xrightarrow{\sim} \text{Pic}(R) \quad \text{and} \quad \bar{j}^+_{R,m} : I(R,m)/P^+(R,m) \xrightarrow{\sim} \text{Pic}^+(R).$$

Proof. Put $\pi_m = \pi_R \circ j_{R,m} : I(R,m) \to \text{Pic}(R)$; thus, π_m is the restriction of the quotient map $\pi_R : I(R) \to \text{Pic}(R)$ to $I(R,m)$. Clearly, π_m is surjective by Proposition 2.34 and has kernel $\text{Ker}(\pi_m) = P(R) \cap I(R,m) = P(R,m)$, so the isomorphism theorem (of groups) shows that we obtain the desired isomorphism $\bar{j}_{R,m}$. The proof for $\bar{j}^+_{R,m}$ is similar.

The key result about the groups $I(R,m)$ is the following.

Theorem 2.3 *Let $R \subset R'$ be orders and let m be an integer with $[R' : R] | m$. If $L' \in Id(R',m)$, then $L' \cap R \in Id(R,m)$ and*

$$\rho_{R,R'}(L' \cap R) = L'. \tag{2.77}$$

As a result, $\rho_{R,R'}$ is surjective and its restriction to $I(R,m)$ defines an isomorphism

$$\rho_m = \rho_{R,R',m} : I(R,m) \xrightarrow{\sim} I(R',m) \tag{2.78}$$

which maps $Id(R,m)$ to $Id(R',m)$.

The proof of this uses the following useful fact.

Lemma 2.5 *If $L \in \mathrm{Lat}(R)$ is an R-ideal, and $m \geq 1$, then*

$$L \in Id(R,m) \quad \Leftrightarrow \quad \gcd(N(L),m) = 1. \tag{2.79}$$

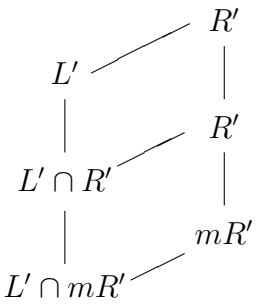
In particular, $Id(R,m)$ is closed under multiplication and hence

$$I(R,m) \;=\; \{L_1 L_2^{-1} : L_1, L_2 \in Id(R,m)\}. \tag{2.80}$$

Proof. Consider the quotient group R/L which has order $N(L)$, and let $[m] : R/L \to R/L$ be the multiplication by m map. Then $L \in Id(R,m) \Leftrightarrow L + mR = R \Leftrightarrow [m]$ is surjective $\Leftrightarrow$ [m] is injective $\Leftrightarrow \mathrm{Ker}([m]) = 0 \Leftrightarrow \nexists$ prime $p | (m, N(L))$ and $x \in R/L$ of order $p \Leftrightarrow (m, N(L)) = 1$. Here we used the fact that if $A = R/L$ is a finite abelian group, and if $p \mid |A|$, then A has an element $x \in A$ of order p. This proves (2.79).

If $L_i \in Id(R,m)$, then $(N(L_i), m) = 1$, and so by (2.44) we see that also $(N(L_1 L_2), m) = 1$. Thus $L_1 L_2 \in Id(R,m)$, and hence $Id(R,m)$ is closed under multiplication. As a result, the right hand side of (2.80) is a subgroup of $\mathrm{Lat}(R)$ and hence equals $\langle Id(R,m)\rangle = I(R,m)$.

Proof of Theorem 2.3. Note first that $mR' \subset R$ because $[R' : R] | m$. Thus, if $L' \in Id(R', m)$, then the condition $L' + mR' = R'$ shows that we have the following cartesian diagram



which implies by Dedekind's modular law that

$$(L' \cap R) + mR' \;=\; R. \tag{2.81}$$

From this we obtain that

$$(L' \cap R)R' = L'. \tag{2.82}$$

Indeed, since $L'R = L'$ (because L' is an R-module), we obtain, using (2.81) that $L' = L'R = L'((L' \cap R) + mR') \subset R'(L' \cap R) + L'mR' \subset R'(L' \cap R) + L \cap R = R'(L' \cap R) \subset R'L' = L'$, and so we must have equality throughout. Thus (2.82) holds.

From (2.82) we have, putting $L := L' \cap R$, that $[R' : L'] = N(L') = N(LR') = N(L)N(R') = N(L) \cdot 1 = [\mathcal{O}(L) : L] = [\mathcal{O}(L) : R][R : L]$. Since L is an R-ideal and $[R' : L'] = [R : L]$, we have that $\mathcal{O}(L) = R$ and $N(L') = N(L)$. Thus $L \in \mathrm{Lat}(R)$ and $L \in Id(R,m)$ by Lemma 2.5. This proves the first assertion and (2.77).

From this it follows immediately that $\rho = \rho_{R,R'}$ is surjective. Indeed, if $L' \in \mathrm{Lat}(R')$, then by Proposition 2.34 $\exists \lambda \in K^\times$ such that $\lambda L' \in Id(R,m)$. Then $L := \lambda L' \cap R \in Id(R,m) \subset \mathrm{Lat}(R)$, and $\rho(\lambda^{-1}L) = \rho(\lambda^{-1}R)\rho(L) = \lambda^{-1}R'(\lambda L') = L'$, so ρ is surjective.

We next show that $\rho(Id(R,m)) = Id(R',m)$. Indeed, if $L \in Id(R,m)$, then $1 \in L + mR$, so also $1 \in LR' + mR'$, and so $LR' + mR' = R'$ since LR' is an invertible R'-ideal. Thus $LR' \in Id(R',m)$ and hence $\rho(Id(R,m)) \subset Id(R',m)$. Since the opposite inclusion follows from (2.77), the two sets are equal.

It thus follows that the $\rho(I(R,m)) = \rho(\langle Id(R,m)\rangle) = \langle \rho(Id(R,m))\rangle = \langle Id(R',m)\rangle = I(R',m)$, and so the restriction ρ_m of ρ to $I(R,m)$ defines a surjection $\rho_m : I(R,m) \to I(R',m)$.

To prove that ρ_m is injective, note first that we have that

$$LR' \cap R = L, \quad \text{for all } L \in Id(R,m). \tag{2.83}$$

Indeed, the inclusion $L \subset LR' \cap R$ is clear, and the opposite inclusion also holds because $LR' \cap R = (LR' \cap R)R = (LR' \cap R)(L + mR) \subset RL + LmR' \subset RL + LR = L$. Thus, if $L \in \mathrm{Ker}(\rho_m)$, then by (2.80) we have that $L = L_1 L_2^{-1}$ where $L_i \in Id(R,m)$ and $L_1 L_2^{-1} R = R'$. Then $L_1 R' = L_2 R'$, and so by (2.83) we obtain that $L_1 = L_2$, and so $L = R$. Thus ρ_m is also injective and hence is an isomorphism.

The above Theorem 2.3 has the following important consequence.

Corollary 2.36 *Assume as before that $[R' : R] | m$. Then the rule $L' \mapsto (L' \cap R) + P(R)$, where $L' \in Id(R',m)$, defines a surjection $\varphi_{R',R,m} : I(R',m) \to \mathrm{Pic}(R)$ with kernel*

$$\mathrm{Ker}(\varphi_{R',R,m}) = \rho_{R,R'}(P(R,m)) = P(R',n,m) := \langle \alpha R' : \alpha \in R'(n,m)\rangle, \tag{2.84}$$

where $n = [R' : R]$ and

$$R'(n,m) = \{\alpha \in R' : \alpha \equiv a \pmod{nR'} \text{ for some } a \in \mathbb{Z} \text{ with } (a,m) = 1\}.$$

Thus $\varphi_{R',R',m}$ induces an isomorphism

$$\overline{\varphi}_{R',R,m} : I(R',m)/P(R',n,m) \xrightarrow{\sim} \mathrm{Pic}(R).$$

Proof. By Theorem 2.3 we know that $\varphi_{R',R,m} = \overline{j}_{R,m} \circ \rho^{-1}_{R,R',m}$, and so it follows from Corollary 2.35 that $\varphi_{R',R,m}$ is surjective with kernel $\rho_{R,R'm}(\mathrm{Ker}(\bar{j}_{R,m})) = \rho_{R,R',m}(P(R,m))$. This proves the first equation of (2.84).

To prove the second equation of (2.84), we first prove that

$$\rho_{R,R'}(P(R) \cap Id(R',m)) = \{\alpha R' : \alpha \in R'(n,m)\}, \tag{2.85}$$

which in turn will follow easily from the fact that

$$R'(n,m) = \{\alpha \in R : (N(\alpha), m) = 1\}. \tag{2.86}$$

To verify (2.86), first note that $R = \mathbb{Z} + nR'$ (because if $[\mathcal{O}_K : R'] = c$, then by (2.27) we have $R' = \mathbb{Z} + c\omega_{\Delta_K}\mathbb{Z}$ and hence $R = \mathbb{Z} + nc\omega_{\Delta_K}\mathbb{Z} = \mathbb{Z} + n\mathbb{Z} + nc\omega_{\Delta_K}\mathbb{Z} = \mathbb{Z} + nR'$), and so we see that $\alpha \equiv a \pmod{nR'}$, for some $a \in \mathbb{Z}, \Leftrightarrow \alpha \in R$. Moreover, we observe that

$$(2.87) \qquad \alpha = a + n\beta,\ \beta \in R' \ \Rightarrow\ N(\alpha) = a^2 + an\mathrm{Tr}(\beta) + n^2N(\beta) \ \equiv\ a^2 \pmod{n}$$

because $N(\alpha) = (a + n\beta)(a + n\sigma(\beta)) = a^2 + an(\beta + \sigma(\beta)) + n^2\beta\sigma(\beta)$ (and because $\mathrm{Tr}(\beta), N(\beta) \in \mathbb{Z}$). Thus, from (2.87) and the fact that $n|m$ we see that $(a, m) = 1 \Leftrightarrow (a^2, m) = 1 \Leftrightarrow (N(\alpha), m) = 1$, and so (2.86) follows.

From this, the identity (2.85) follows readily. Indeed, if $L \in P(R) \cap Id(R, m)$, then $L = \alpha R$ with $\alpha \in R$ and $(N(\alpha), m) = 1$ by (2.79) (and by (2.39)), so $\alpha \in R'(n, m)$ by (2.86), and hence $\rho_{R,R'}(L) = \alpha R'$ lies in the right hand side of (2.86). Conversely, if $\alpha \in R'(n, m)$, then by (2.86) we have that $\alpha \in R$ and $(N(\alpha), m) = 1$, and so by (2.79) we have $\alpha R \in P(R) \cap Id(R, m)$, and hence $\alpha R' = \rho_{R,R'}(\alpha R) \in \rho_{R,R'}(P(R) \cap Id(R, m))$. This proves (2.85).

Clearly, the second equality of (2.84) follows from (2.85) once we have shown that

$$(2.88) \qquad P(R, m) \ =\ \langle P(R) \ \cap\ Id(R, m)\rangle.$$

To verify this, let $\alpha R \in P(R, m) = P(R) \cap I(R, m)$. Then by (2.80) we have $\alpha R = L_1L_2^{-1}$, for some $L_i \in Id(R, m)$. Put $\alpha_1 = N(L_2)\alpha$ and $\alpha_2 = N(L_2)$. Clearly $\alpha = \alpha_1/\alpha_2$, so $\alpha R = \alpha_1 R(\alpha_2 R)^{-1}$. We claim that $\alpha_i R \in I(R, m)$. To justify this for $i = 1$, we observe that by (2.41) we have $\alpha_1 R = \alpha_2\alpha R = N(L_2)L_1L_2^{-1} = L_1\sigma(L_2) \in Id(R, m)$, the latter because $L_2 \in Id(R, m) \Rightarrow \sigma(L_2) \in Id(R, m)$ (and because $Id(R, m)$ is closed under multiplication). For $i = 2$, this is clear because by (2.79) we have $(N(L_2), m) = 1$, so also $(N(\alpha_2 R), m) = 1$ as $N(\alpha_2 R) = N(L_2)^2$. Thus $\alpha R = \alpha_1 R(\alpha_2 R)^{-1} \in \langle P(R) \cap Id(R, m)\rangle$. This proves one inclusion of (2.88). Since the other inclusion is trivial, this proves (2.88) and hence also (2.85).

Remark 2.9 (a) A slight modification of the proof of Corollary 2.36 shows that the rule $L' \mapsto (L' \cap R) + P^+(R)$ induces a homomorphism $\varphi^+_{R',R,m} : I(R', m) \to \mathrm{Pic}^+(R)$ with kernel

$$(2.89) \quad \mathrm{Ker}(\varphi^+_{R',R,m}) \ =\ \rho_{R,R'}(P^+(R, m)) \ =\ P^+(R', n, m) := \langle \alpha R' : \alpha \in R'_+(n, m)\rangle,$$

where $R'_+(n, m) := \{\alpha \in R(n, m) : N(\alpha) > 0\}$. We thus obtain an isomorphism

$$\overline{\varphi}^+_{R',R,m} : I(R', m)/P^+(R', n, m) \ \xrightarrow{\sim}\ \mathrm{Pic}^+(R).$$

(b) For later reference we observe that the proof of Corollary 2.36 shows that

$$(2.90) \qquad \varphi_{R,R,m} \circ \rho_{R,R',m} = \pi_R \circ j_{R,m} \quad \text{and} \quad \varphi^+_{R,R,m} \circ \rho_{R,R',m} = \pi^+_R \circ j_{R,m}.$$

The most important case of the above Corollary 2.36 is the case that $R' = \mathcal{O}_K$ is the maximal order (or ring of integers) of K, for it allows us to identify the groups $\mathrm{Pic}(R)$ and $\mathrm{Pic}^+(R)$ with suitable subquotients (called *ring class groups*) of the group $I_K := I(\mathcal{O}_K)$ of fractional ideals of $\mathcal{O}_K$. In this case it is common to use the following simplified notation.

Notation. If $m \geq 1$ is a positive integer, let $I_K(m) = I(\mathcal{O}_K, m)$ denote the group of *fractional ideals* of K which are prime to m; thus, $I_K(m)$ is the free abelian group generated by the nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ with $m \notin \mathfrak{p}$. Similarly, let $Id_K(m) = Id(\mathcal{O}_K, m)$ denote the set of ideals of $\mathcal{O}_K$ which are prime to m. Moreover, if $f|m$, let

$$P_K(f,m) = P(\mathcal{O}_K, f, m) \quad \text{and} \quad P_K^+(f,m) = P^+(\mathcal{O}_K, f, m)$$

be the subgroups of principal fractional ideals $\alpha\mathcal{O}_K$ generated by the subsets $\mathcal{O}_K(f,m) = \{\alpha \in \mathcal{O}_K : \alpha \equiv a \pmod{f\mathcal{O}_K}$, for some $a \in \mathbb{Z}$ with $(a,m) = 1\}$ and $\mathcal{O}_K(f,m) \cap K_+$, respectively.

We then have the following important special case of Corollary 2.36.

Theorem 2.4 *Let K be an order of K with conductor $f = [\mathcal{O}_K : R]$, and let $f|m$. Then the rules $\mathfrak{a} \mapsto (\mathfrak{a} \cap R) + P(R)$ and $\mathfrak{a} \mapsto (\mathfrak{a} \cap R) + P^+(R)$, where $\mathfrak{a} \in Id_K(m)$, define homomorphisms*

$$\varphi_{R,m} : I_K(m) \to \mathrm{Pic}(R) \quad \textit{and} \quad \varphi_{R,m}^+ : I_K(m) \to \mathrm{Pic}^+(R)$$

which induce isomorphisms

$$\overline{\varphi}_{R,m} : I_K(m)/P_K(f,m) \xrightarrow{\sim} \mathrm{Pic}(R) \quad \textit{and} \quad \overline{\varphi}_{R,m}^+ : I_K(m)/P_K^+(f,m) \xrightarrow{\sim} \mathrm{Pic}^+(R).$$

Proof. This is the special case $R' = \mathcal{O}_K$ of Corollary 2.36 and of Remark 2.9(a).

Some other consequences of Theorem 2.3 are the following.

Corollary 2.37 *If $R \subset R'$, then the following sequences are exact:*

$$0 \to (R')^\times/R^\times \xrightarrow{\mu} \mathrm{Ker}(\rho_{R,R'}) \xrightarrow{\pi_R} \mathrm{Pic}(R) \xrightarrow{\bar{\rho}_{R,R'}} \mathrm{Pic}(R') \to 0, \tag{2.91}$$

$$0 \to U_1(R')/U_1(R) \xrightarrow{\mu^+} \mathrm{Ker}(\rho_{R,R'}) \xrightarrow{\pi_R^+} \mathrm{Pic}^+(R) \xrightarrow{\bar{\rho}_{R,R'}^+} \mathrm{Pic}^+(R') \to 0. \tag{2.92}$$

Proof. Since $\rho_{R,R'}$ is surjective by Theorem 2.3, the same is true for $\bar{\rho}_{R,R'}$ because $\pi'_R\rho_{R,R'} = \bar{\rho}_{R,R'}\pi_R$, and so the sequence

$$0 \to \mathrm{Ker}(\bar{\rho}_{R,R'}) \to \mathrm{Pic}(R) \xrightarrow{\bar{\rho}_{R,R'}} \mathrm{Pic}(R') \to 0$$

is exact. By splicing this sequence with the exact sequence (2.75), we see that (2.91) is exact. The proof for (2.92) is similar.

Corollary 2.38 *If $R \subset R' \subset R''$ are three orders, then*

$$|\mathrm{Ker}(\rho_{R,R''})| \;=\; |\mathrm{Ker}(\rho_{R,R'})| \cdot |\mathrm{Ker}(\rho_{R',R''})|. \tag{2.93}$$

Proof. Since $\rho_{R,R''} = \rho_{R',R''} \circ \rho_{R,R'}$ and since $\rho := \rho_{R,R'}$ is surjective, it follows that the sequence

$$0 \;\to\; \mathrm{Ker}(\rho_{R,R'}) \;\to\; \mathrm{Ker}(\rho_{R,R''}) \;\stackrel{\rho}{\to}\; \mathrm{Ker}(\rho_{R',R''}) \;\to\; 0$$

is exact, and so (2.93) follows.

We can use the previous results to determine the order of the kernel of $\rho_{R,R'}$.

Proposition 2.39 *Let $R \subset R' = \mathcal{O}_{\Delta'}$ and let $n = [R' : R]$. Then*

$$|\mathrm{Ker}(\rho_{R,R'})| \;=\; n \prod_{p|n} \left(1 - \frac{1}{p}\left(\frac{\Delta'}{p}\right)\right). \tag{2.94}$$

Proof. We will prove this by induction on the number r of prime divisors of n (counted with multiplicities).

Case 1: $r = 1$, i.e. $n = p$ is a prime. Here we have:

$$\mathrm{Ker}(\rho_{R,R'}) \;=\; \mathcal{K} \;:=\; \{L \leq R' : [R' : L] = p, LR' \not\subset L\}. \tag{2.95}$$

Indeed, if $L \subset R'$, then $L \subset LR' \subset R'$, so if $[R' : L] = p$, then $LR' = R' \Leftrightarrow LR' \not\subset L$, and so we see that (2.95) follows immediately from (2.72).

For $b \in \mathbb{Z}$ put $L_b = \mathbb{Z}p + \mathbb{Z}(b + \omega_{\Delta'})$. We now claim:

$$L \in \mathrm{Ker}(\rho_{R,R'}) \setminus \{R\} \quad \Leftrightarrow \quad L = L_b \text{ with } (2b + \Delta')^2 \not\equiv \Delta' \pmod{4p}. \tag{2.96}$$

Indeed, if $L \in \mathrm{Ker}(\rho) \setminus \{R\}$, then by Lemma 2.1 we know that L has a Hermite basis (with respect to the basis $\{1, \omega_{\Delta'}\}$ of R'), so $L = \mathbb{Z}a + \mathbb{Z}(b + c\omega_\Delta)$, for some $a, b, c \in \mathbb{Z}$. Without loss of generality we may assume $a > 0$ and $c > 0$ (by replacing (b, c) by $(-b, -c)$, if necessary). Note that $ac = [R' : L] = p$. Now if $a = 1$, then $c = p$ and $L = \mathbb{Z} + \mathbb{Z}(b + p\omega_\Delta) = \mathbb{Z} + \mathbb{Z}p\omega_\Delta = R$, contradiction. Thus $a = p$ and $c = 1$, and hence $L = L_b$. Suppose $(2b + \Delta')^2 \equiv \Delta' \pmod{4p}$, i.e. $(2b + \Delta')^2 - \Delta' = 4pC$, for some $C \in \mathbb{Z}$. Put $f = [p, -2b - \Delta', C]$. Then $\Delta(f) = \Delta'$ and $L(f) = L$ because $\frac{1}{2}(-(-2b - \Delta') + \sqrt{\Delta'}) = b + \omega_{\Delta'}$. But then L is an R'-ideal by Proposition 2.16, which contradicts the hypothesis $LR' \not\subset L$. Thus $(2b + \Delta')^2 \not\equiv \Delta' \pmod{4p}$.

Conversely, suppose $L = L_b$ and $(2b + \Delta')^2 \not\equiv \Delta' \pmod{4p}$. Then clearly $L \neq R$, $L \subset R'$ and $[R' : L] = p$. Suppose that $LR' \subset L$, i.e. that L is an R'-ideal. Since $\frac{2b+\Delta'-\sqrt{\Delta'}}{2} = b + \sigma(\omega_{\Delta'}) \in R'$, this implies that $A := \frac{(2b+\Delta')^2-\Delta'}{4} = (b + \sigma(\omega_{\Delta'}))(b + \omega\Delta') \in L$, so $A = tp + s(b + \omega_{\Delta'})$, for some $s, t \in \mathbb{Z}$. Since $A \in \mathbb{Q}$, we must have $s = 0$, so $A = tp$ and hence $(2b + \Delta')^2 - \Delta' = 4tp$, which is contrary to the hypothesis $(2b + \Delta')^2 \not\equiv \Delta' \pmod{4p}$. Thus $LR' \not\subset L$ and hence $L \in \mathrm{Ker}(\rho) \setminus \{R\}$ by (2.95). This proves (2.96).

Now since $L_{b_1} = L_{b_2} \Leftrightarrow b_1 \equiv b_2 \pmod{p}$, we see from (2.96) that $|\mathrm{Ker}(\rho)| = 1 + \#\{b \pmod{p} : (2b+\Delta')^2 \not\equiv \Delta' \pmod{4}p\} = 1 + p - \#\{b \pmod{p} : (2b+\Delta')^2 \equiv \Delta' \pmod{4}p\}$. Since $\#\{b \pmod{p} : (2b+\Delta')^2 \equiv \Delta' \pmod{4}p\} = \#\{b_1 \pmod{2}p : (b_1 + \Delta')^2 \equiv \Delta' \pmod{4}p\} = \#\{b \pmod{2}p : b^2 \equiv \Delta' \pmod{4}p\} = \#\mathrm{Sqrt}'(\Delta', p) = 1 + \left(\frac{\Delta'}{p}\right)$ by Proposition 1.32, we see that $|\mathrm{Ker}(\rho)| = p - \left(\frac{\Delta'}{p}\right)$, which proves (2.94) for $n = p$.

Case 2: $r > 1$, i.e. $n = pn_1$, where p is a prime and $n_1 > 1$. Let $R_1 = \mathcal{O}_\Delta$ be the unique suborder of R' such that $[R' : R_1] = n_1$. Since $R \subset R_1$ and $[R_1 : R] = p$, we obtain from (2.93) and Case 1 and the induction hypothesis (applied to R'/R_1) that

$$|\mathrm{Ker}(\rho_{R,R'})| = |\mathrm{Ker}(\rho_{R,R_1})| \cdot |\mathrm{Ker}(\rho_{R_1,R'})| = p\left(1 - \frac{1}{p}\left(\frac{\Delta}{p}\right)\right) n_1 \prod_{q|n_1}\left(1 - \frac{1}{q}\left(\frac{\Delta'}{q}\right)\right).$$

Now since $\Delta = n_1^2\Delta'$, we see that this equals the right hand side of (2.94). Indeed, if $p \not| n_1$, then $\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta'}{p}\right)$ and $\{q|n\} = \{q|n_1\}\dot\cup\{p\}$, whereas if $p|n$, then the second factor equals 1 and $\{q|n\} = \{q|n_1\}$, and so the assertion follows.

Corollary 2.40 *If Δ' is a discriminant and if $\Delta = n^2\Delta'$ and $u := [U_1(\Delta') : U_1(\Delta)]$, then*

$$h(\Delta) \;=\; h(\Delta')\frac{n}{u}\prod_{p|n}\left(1 - \frac{1}{p}\left(\frac{\Delta'}{p}\right)\right). \tag{2.97}$$

Proof. Apply the previous results to $R := \mathcal{O}_\Delta \subset R' := \mathcal{O}_{\Delta'}$. Then by the exact sequence (2.92) we have

$$|\mathrm{Pic}^+(R')| \;=\; \frac{1}{u}|\mathrm{Pic}^+(R)||\mathrm{Ker}(\rho_{R,R'})|.$$

By using the formula (2.94) for $|\mathrm{Ker}(\rho_{R,R'})|$, and noting that $|\mathrm{Pic}^+(R')| = h(\Delta')$ and $|\mathrm{Pic}^+(R)| = h(\Delta)$ by Theorems 2.1 and 2.2, we see that formula (2.97) follows. Here in order to apply Theorem 2.1 we had also used the fact that when $\Delta < 0$, then $\mathrm{Pic}(R) = \mathrm{Pic}^+(R)$ and $\mathrm{Pic}(R') = \mathrm{Pic}^+(R')$.

Remark 2.10 If $\Delta' < 0$, then the number u of Corollary 2.40 is just the index $u = [\mathcal{O}_{\Delta'}^\times : \mathcal{O}_\Delta^\times]$ of the groups of units. Now if $\Delta' < -4$, then $\mathcal{O}_{\Delta'}^\times = \{\pm 1\}$ by Proposition 2.30 and Proposition 1.17, and so $u = 1$ whenever $\Delta' < -4$.

In view of the importance of the subgroup $\mathrm{Ker}(\rho_{R,R'})$, we give another description of it in terms of the group of units of the quotient ring R'/nR'.

Proposition 2.41 *Let $R \subset R'$ be orders with $[R' : R] = n$. Then the map $\alpha \mapsto L_\alpha := \mathbb{Z}\alpha + nR'$ induces an exact sequence*

$$0 \;\to\; (\mathbb{Z}/n\mathbb{Z})^\times \;\to\; (R'/nR')^\times \;\xrightarrow{\mathcal{L}}\; \mathrm{Ker}(\rho_{R,R'}) \;\to\; 0. \tag{2.98}$$

Proof. We first observe that if $\alpha \in R'$, then

$$\alpha + nR' \in (R'/nR')^\times \quad \Leftrightarrow \quad (N_K(\alpha), n) = 1. \tag{2.99}$$

Indeed, $\alpha + nR' \in (R'/nR')^\times \Leftrightarrow \exists \beta \in R'$ such that $\alpha\beta \equiv 1 \pmod{nR'}$. By (2.87) this implies that $N_K(\alpha)N_K(\beta) = N_K(\alpha\beta) \equiv 1 \pmod{n}$, and so $(N_K(\alpha), n) = 1$. Conversely, if $(N_K(\alpha), n) = 1$, then $\exists x, y \in \mathbb{Z}$ such that $xN_K(\alpha) + yn = 1$, and then $(\alpha + nR')(x\sigma(\alpha) + nR') = 1 + nR'$, so $\alpha + nR' \in (R'/nR')^\times$. This proves (2.99).

Let $\alpha + nR' \in (R'/nR')^\times$. Then $L_\alpha = \langle \alpha + nR' \rangle$ does not depend on the choice of $\alpha \in \alpha + nR'$, and we have

$$[L_\alpha : nR'] = n. \tag{2.100}$$

Indeed, put $m := [L_\alpha : nR']$. Then $m\alpha = n\beta$ with $\beta \in R'$, and so $m^2 N_K(\alpha) = n^2 N_K(\beta)$. Since $(N_K(\alpha), n) = 1$ by (2.99), it follows that $n^2 | m^2$, and hence that $n|m$. On the other hand, since $n\alpha \in nR'$, we see that $m|n$ and so $m = n$, which proves (2.100).

From this we see that $L_\alpha \in \mathrm{Ker}(\rho)$. Indeed, by (2.100) we have $[R' : L_\alpha] = n$ because $[R' : nR'] = n^2$. Moreover, we note that $L_\alpha R'$ is an R'-ideal which contains 1 because $\alpha\beta \in 1 + nR'$, for some $\beta \in R'$, and so $L_\alpha R' = R'$. Thus, $L_\alpha \in \mathrm{Ker}(\rho)$ by (2.72).

We thus see that the rule $\mathcal{L}(\alpha + nR') = \langle \alpha + nR' \rangle = L_\alpha$ defines a map $\mathcal{L} : (R'/nR')^\times \to \mathrm{Ker}(\rho)$. Clearly, $\mathcal{L}$ is a homomorphism because $(\alpha + nR')(\beta + nR') = \alpha\beta + nR'$.

To see that $\mathcal{L}$ is surjective, let $L \in \mathrm{Ker}(\rho)$. Then by (the proof of) (2.72) we know that $N(L) = 1$ and $[R' : L] = n$, so $nR' \subset L$. By Corollary 2.19 we have $L = rL(f)$, for some $r \in \mathbb{Q}^\times$ and $f = [a, b, c] \in Q_\Delta$. Now by Proposition 1.39 $\exists x, y \in \mathbb{Z}$ such that $(f(x, y), n) = 1$, and then $\alpha := xra - yr\beta_f \in L$ satisfies $(N_K(\alpha), n) = 1$ because $N_K(\alpha) = N_K(\alpha)N(L)^{-1} = \mathrm{sign}(a)f(x, y)$ by (2.33). Thus $\alpha + nR' \in (R'/nR')^\times$ by (2.99) and so $L_\alpha \in \mathrm{Ker}(\rho)$ by what was shown above. But since $L_\alpha = \mathbb{Z}\alpha + nR' \subset L$ and since $[R' : L] = n = [R' : L_\alpha]$, it follows that $L = L_\alpha$, which means that $\mathcal{L}$ is surjective.

Next, consider the map $i_{R',n} : (\mathbb{Z}/n\mathbb{Z})^\times \to (R'/nR')^\times$ given by $(a + n\mathbb{Z}) \mapsto (a + nR')$. This map is an injective homomorphism (of groups) because it is induced by the ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to R'/nR'$ which is well-defined and injective because $nR' \cap \mathbb{Z} = n\mathbb{Z}$.

Now $\alpha + nR' \in \mathrm{Ker}(\mathcal{L}) \Leftrightarrow \alpha\mathbb{Z} + nR' = R = \mathbb{Z} + nR' \Leftrightarrow \alpha + nR' = a + nR'$, for some $a \in \mathbb{Z}$ with $(a, n) = 1$. (To see the last implication, note that since $(N(\alpha), n) = 1$ by (2.99), it follows from (2.86) that $(a, n) = 1$.) Thus $\mathrm{Ker}(\mathcal{L}) = \mathrm{Im}(i_{R',n})$, so the sequence (2.98) is exact.

Remark 2.11 It follows from the above Proposition 2.41 and (2.94) that

$$|(R'/nR')^\times| = \phi(n)|\mathrm{Ker}(\rho_{R,R'})| = n^2 \prod_{p|n} \left(1 - \frac{1}{p}\left(\frac{\Delta'}{p}\right)\right)\left(1 - \frac{1}{p}\right).$$

For $R' = \mathcal{O}_K$ this can also be verified directly by using algebraic number theory; cf. Lang[La2], p. 95. This, therefore, gives an alternate proof of (2.94).

2.4.7 Genus theory

Recall from the end of Chapter 1 that Gauss's genus theory leads to an isomorphism

$$\bar{S}^*_\Delta : \overline{\mathcal{G}}_\Delta := \mathcal{G}_\Delta/\langle\chi_\Delta\rangle \quad \xrightarrow{\sim} \quad \mathrm{Hom}(Cl(\Delta), \{\pm 1\})$$

between the quotient $\overline{\mathcal{G}}_\Delta$ of the group $\mathcal{G}_\Delta$ of genus characters and the group of quadratic characters of the class group $Cl(\Delta)$ (cf. Corollary 1.53), and that conversely this isomorphism encapsulates all the results of Gauss's genus theory; cf. Remark 1.26. In view of Dedekind's fundamental isomorphism between the class group $Cl(\Delta)$ and a suitable quotient of the group $I_K(\Delta)$ of fractional ideals prime to Δ (cf. Theorems 2.2 and 2.4), we thus see that the group $\mathcal{G}_\Delta$ of genus characters induces quadratic characters on $I_K(\Delta)$; these are usually called *genus characters* as well. We now want identify these explicitly.

For this, recall first that the above isomorphism $\bar{S}^*_\Delta$ was induced by the homomorphism $\bar{S}_\Delta : Cl(\Delta) \to ((\mathbb{Z}/\Delta\mathbb{Z})^\times)/\bar{S}(1_\Delta)$ which was constructed in Proposition 1.48. We now show that $\bar{S}_\Delta$ has a natural interpretation in terms of norms of ideals.

Proposition 2.42 *Let $R = \mathcal{O}_\Delta$ be an order in K of discriminant $\Delta = f^2\Delta_K$. Then the rule $\mathfrak{a} \mapsto N(\mathfrak{a}) \pmod\Delta$ induces a homomorphism $N_\Delta : I_K(\Delta) \to (\mathbb{Z}/\Delta\mathbb{Z})^\times$ such that*

$$N_\Delta(P^+_K(f,\Delta)) \;=\; \bar{S}(1_\Delta). \tag{2.101}$$

Thus, N_Δ induces a homomorphism $\overline{N}_\Delta : I_K(\Delta)/P^+_K(f,\Delta) \to ((\mathbb{Z}/\Delta\mathbb{Z})^\times)/\bar{S}(1_\Delta)$ which is related to the map $\bar{S}_\Delta$ by the formula

$$\bar{S}_\Delta = \overline{N}_\Delta \circ (\bar{\varphi}^+_{R,\Delta})^{-1} \circ \lambda^+_\Delta. \tag{2.102}$$

In particular, we have

$$\chi_\Delta(N(\mathfrak{a})) = 1, \quad \text{for all } \mathfrak{a} \in I_K(\Delta). \tag{2.103}$$

Proof. By Lemma 2.5 we have that $(N(\mathfrak{a}),\Delta) = 1$ when $\mathfrak{a} \in Id_K(\Delta)$, so the above rule extends to a homomorphism on $I_K(\Delta) = \langle Id_K(\Delta)\rangle$.

To prove (2.101), let $\lambda \in \mathcal{O}_K(f,\Delta) \cap K_+$. Then $\lambda \in \mathcal{O}_\Delta$ and $(N_K(\lambda),\Delta) = 1$ by (2.86). Thus $\lambda = x + y\omega_\Delta$ with $x, y \in \mathbb{Z}$. Since $N_K(\lambda) > 0$, we have $N(\lambda\mathcal{O}_K) = N_K(\lambda) = 1_\Delta(x,-y)$; cf. (2.33). This shows that $N_\Delta(\lambda\mathcal{O}_K) \in \bar{S}(1_\Delta)$ and so it follows that $N_\Delta(P^+_K(f,\Delta)) \subset \bar{S}(1_\Delta)$ because $P^+_K(f,\Delta)$ is generated by elements of the form $\lambda\mathcal{O}_K$ with $\lambda \in \mathcal{O}_K(f,\Delta) \cap K_+$.

To prove the opposite inclusion, let $\bar{n} \in \bar{S}(1_\Delta)$, so there exist $x, y \in \mathbb{Z}$ such that $1_\Delta(x,y) \equiv \bar{n} \pmod\Delta$. By replacing x by $x' = x + k\Delta$ with k sufficiently large we may assume that $n := 1_\Delta(x',y) > 0$. (Note that $n \equiv 1_\Delta(x,y) \pmod\Delta$.) Thus, if we put $\lambda = x' - y\omega_\Delta$, then $\lambda \in \mathcal{O}_K(f,\Delta) \cap K_+$ and $N(\lambda\mathcal{O}_K) = N_K(\lambda) = 1_\Delta(x',y) = n \equiv \bar{n} \pmod\Delta$. Thus $\bar{S}(1_\Delta) \subset N_\Delta(P^+_K(f,\Delta))$, and so (2.101) is proved. It is thus clear that the rule $\mathfrak{a} \mapsto N_\Delta(\mathfrak{a})\bar{S}(1_\Delta)$ defines a homomorphism $\overline{N}_\Delta : I_K(\Delta)/P^+_K(f,\Delta) \to ((\mathbb{Z}/\Delta\mathbb{Z})^\times)/\bar{S}(1_\Delta)$.

To prove (2.102), let $cl(f) \in Cl(\Delta)$. By Lemma 2.4 and Proposition 1.6 we may assume that $f = [a,b,c]$ with $(a,\Delta) = 1$ and $a > 0$. Then $\bar{S}_\Delta(cl(f)) = a\bar{S}(1_\Delta)$ because

$a \in R(f)$. On the other hand, since $N(L(f)) = |a| = a$ by Proposition 2.16, we have that $L(f) \in Id(\mathcal{O}_\Delta, \Delta)$ by Lemma 2.5 and $\mathfrak{a} := L(f)\mathcal{O}_K \in I_K(\Delta)$ by Theorem 2.3. Thus, since $\lambda^+_\Delta(cl(f)) = L(f)P^+(\mathcal{O}_\Delta)$ and $(\bar\varphi^+_{R,\Delta})^{-1}(L(f)P^+(\mathcal{O}_\Delta)) = \mathfrak{a}P^+_K(f,\Delta)$, and since $a = N(L(f)) = N(\mathfrak{a})$, it follows that $\overline{N}_\Delta((\bar\varphi^+_{R,\Delta})^{-1}(\lambda^+_\Delta(cl(f)))) = \overline{N}_\Delta(\mathfrak{a}P^+_K(f,\Delta)) = N(\mathfrak{a})\bar S(1_\Delta) = a\bar S(1_\Delta) = \bar S_\Delta(cl(f))$, which proves (2.102).

From this, (2.103) follows immediately because we have $\mathrm{Im}(\bar N_\Delta) = \mathrm{Im}(\bar S_\Delta) \le \mathrm{Ker}(\chi_\Delta)$ by (2.102) and (1.114).

Corollary 2.43 *For each $\chi_1 \in \mathcal{G}_\Delta$ there is a unique $\chi \in \mathrm{Hom}(\mathrm{Pic}^+(\mathcal{O}_\Delta), \{\pm 1\}) \simeq \mathrm{Hom}(Cl(\Delta), \{\pm 1\})$ such that*

$$\chi_1 \circ \overline{N}_\Delta \;=\; \chi \circ \overline{\varphi}^+_{\mathcal{O}_\Delta,\Delta}. \tag{2.104}$$

Conversely, if $\chi \in \mathrm{Hom}(\mathrm{Pic}^+(\mathcal{O}_\Delta), \{\pm 1\})$, then there exists $\chi_1 \in \mathcal{G}_\Delta$ such that (2.104) *holds. Moreover, if χ_1 is essentially unique: if $\chi_2 \ne \chi_1$ is another choice, then $\chi_2 = \chi_1\chi_\Delta$.*

Proof. Since $\bar S(1_\Delta) \le \mathrm{Ker}(\chi_1)$ by (1.115), we can view χ_1 as a character on the quotient group $((\mathbb{Z}/\Delta\mathbb{Z})^\times)/\bar S(1_\Delta)$, and so $\chi_1 \circ \overline{N}_\Delta$ is defined. Thus, $\chi := \chi_1 \circ \overline{N}_\Delta \circ (\overline{\varphi}^+_{\mathcal{O}_\Delta,\Delta})^{-1} \in \mathrm{Hom}(\mathrm{Pic}^+(\mathcal{O}_\Delta), \{\pm 1\})$ is the unique character satisfying (2.104).

Conversely, if $\chi \in \mathrm{Hom}(\mathrm{Pic}^+(\mathcal{O}_\Delta), \{\pm 1\})$, then by Corollary 1.53 there exists $\chi_1 \in \mathcal{G}_\Delta$ such that $\chi \circ \lambda^+_\Delta = \chi_1 \circ \bar S_\Delta$. Moreover, by (2.102) we have $\chi \circ \lambda^+_\Delta = \chi_1 \circ \bar S_\Delta = \chi_1 \circ \overline{N}_\Delta \circ (\overline{\varphi}^+_{\mathcal{O}_\Delta,\Delta})^{-1} \circ \lambda^+_\Delta$, and so (2.104) follows because λ^+_Δ is an isomorphism. The last assertion follows from the exact sequence (1.127).

It is interesting to observe that the genus characters $\chi_1 \in \mathcal{G}_\Delta$ are the only characters of $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ which can be lifted in the above way to characters on the class group.

Corollary 2.44 *Let $\chi_1 : (\mathbb{Z}/\Delta\mathbb{Z})^\times \to \mathbb{C}^\times$ be a homomorphism, and suppose that there is a homomorphism $\chi : \mathrm{Pic}^+(\mathcal{O}_\Delta) \to \mathbb{C}^\times$ such that*

$$\chi_1(N(\mathfrak{a})) = \chi(\varphi^+_{\mathcal{O}_\Delta,\Delta}(\mathfrak{a})), \quad \textit{for all } \mathfrak{a} \in I_K(\mathfrak{a}). \tag{2.105}$$

Then $\chi_1 \in \mathcal{G}_\Delta$ is a genus character; in particular, χ_1 is quadratic.

Proof. It is enough to verify that $\bar S(1_\Delta) \le \mathrm{Ker}(\chi_1)$ because by (1.117) we have that $\mathcal{G}_\Delta = \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar S(1_\Delta), \{\pm 1\}) = \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times/\bar S(1_\Delta), \mathbb{C}^\times)$, the latter because it follows from (1.115) that $((\mathbb{Z}/\Delta\mathbb{Z})^\times)^2 \le \bar S(1_\Delta)$.

Now if $n \in \bar S(1_\Delta)$, then by (2.101) we have that $n = N_\Delta(\mathfrak{a})$, for some $\mathfrak{a} \in P^+_K(f,\Delta)$, and then $\chi_1(n) = \chi(N_\Delta(\mathfrak{a})) = \chi(\varphi^+_{\mathcal{O}_\Delta,\Delta}(\mathfrak{a})) = 1$ because $P^+_K(f,\Delta) = \mathrm{Ker}(\varphi^+_{\mathcal{O}_\Delta,\Delta})$ by Theorem 2.4. Thus $\bar S(1_\Delta) \le \mathrm{Ker}(\chi_1)$, and so $\chi_1 \in \mathcal{G}_\Delta$.

Although the above Corollary 2.43 already gives the desired translation of genus characters to characters on $I_K(\Delta)$, it is useful to make this more precise by giving (as in Weber[Web], §104) an alternate description of the characters in $\mathcal{G}_\Delta$ in terms of *fundamental factorizations* of Δ, which will be defined below.

For this, we first observe some useful facts concerning quadratic characters on the group $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. Recall from Remark 1.15 that if $D|\Delta$ is a discriminant, then $\chi_D^\Delta \in \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$ is the unique character such that $\chi_D^\Delta(p) = \left(\frac{D}{p}\right)$, for all primes $p \nmid \Delta$. Here we can restrict D to be a fundamental discriminant in the sense of subsection 2.4.1 because we have the following result.

Lemma 2.6 *The rule $D \mapsto \chi_D^\Delta$ induces a bijection between the set of fundamental discriminants $D|\Delta$ and the set of non-trivial quadratic characters $\chi \in \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$, $\chi \neq 1$, on $(\mathbb{Z}/\Delta\mathbb{Z})^\times$.*

Proof. Since χ_D is a nontrivial character on $(\mathbb{Z}/D\mathbb{Z})^\times$, so is its lift χ_D^Δ to $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. Thus, $D \mapsto \chi_D^\Delta$ maps into $\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\}) \setminus \{1\}$. This map is surjective because if $\chi \in \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$, then by Remark 1.15(b) we have that $\chi = \prod_{d\in S} \chi_d^\Delta$, for some unique subset $S \subset \{d \in \mathcal{P}^* : d|\Delta\} \setminus \{-8\}$, and $S \neq \emptyset$ if $\chi \neq 1$. If all numbers in S are relatively prime, then $D_S := \prod_{d\in S} d$ is a fundamental discriminant by Proposition 2.12, and $D_S|\Delta$. We thus have that $\chi = \prod_{d\in S} \chi_d^\Delta = \chi_{D_S}^\Delta$. On the other hand, if not all numbers in S are relatively prime, then $\{-4, 8\} \subset S$ and then all elements of $S' := \{-8\} \cup (S \setminus \{-4, 8\})$ are relatively prime, and so we have that $D' := D_{S'}|\Delta$ is a fundamental discriminant. Moreover, in view of (1.74) we have that $\chi = \prod_{d\in S} \chi_d^\Delta = \prod_{d\in S'} \chi_d^\Delta = \chi_{D'}^\Delta$, which shows that the map is surjective.

Finally, to see that the given map is injective, suppose that D_1 and D_2 are two fundamental discriminants such that $\chi_{D_1}^\Delta = \chi_{D_2}^\Delta$. If $D_i = \prod_{d\in S_i} d$ is the factorization of D_i into (relatively prime) prime discriminants (cf. Proposition 2.12), then we have that $\chi_{D_i}^\Delta = \prod_{d\in S_i} \chi_d^\Delta$, for $i = 1, 2$. If both $S_1, S_2 \subset B := \{d \in \mathcal{P}^* : d|\Delta, d \neq -8\}$, then $S_1 = S_2$ because $\mathcal{B} := \{\chi_d^\Delta : d \in B\}$ is a basis of $\mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$; cf. Remark 1.15. If $-8 \in S_1$, then by (1.74) we see that both χ_{-4}^Δ and χ_8^Δ occur in the product representation of χ_{Δ_1} in terms of the basis $\mathcal{B}$, and hence the same must be true for $\chi_{D_2}^\Delta$. Thus $-8 \in D_2$, and we must have that $S_1 \setminus \{-8\} = S_2 \setminus \{-8\}$. Thus $S_1 = S_2$ and hence $D_1 = D_2$, as claimed.

Definition. If $\chi \in \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$ is a non-trivial quadratic character, then the unique fundamental discriminant $D|\Delta$ such that $\chi = \chi_D^\Delta$ is called the (signed) *conductor* of χ and is denoted by $f(\chi) := D$.

Remark 2.12 (a) Note that if $D|\Delta$ is any discriminant, then $f(\chi_D^\Delta) = D_{fun}$, where $D_{fun} = D/c^2$ is as in Proposition 2.10. (Indeed, we clearly have $\chi_D^\Delta = \chi_{D_{fun}}^\Delta$ because $\left(\frac{D}{p}\right) = \left(\frac{D_{fun}}{p}\right)$, for all primes $p \nmid \Delta$, and so the formula follows.) In particular, we see that $f(\chi_\Delta) = \Delta_K$, where $K = \mathbb{Q}(\sqrt{\Delta})$.

(b) The above map $\chi \mapsto f(\chi)$ is compatible with multiplication in the sense that we have the formula

$$f(\chi_1\chi_2) = (f(\chi_1)f(\chi_2))_{fun}, \quad \text{if } \chi_1 \neq \chi_2. \tag{2.106}$$

To see this, write $D_i := f(\chi_i)$. Since $D_1 \neq D_2$, we see that $D_1 D_2 \equiv 0, 1 \pmod 4$ is not a square, so $D := (D_1 D_2)_{fun}$ exists and $D_1 D_2 = D c^2$, for some $c \in \mathbb{Z}$. Note that since D is fundamental, it follows that $D | \mathrm{lcm}(D_1, D_2) | \Delta$. Thus, if $p \nmid \Delta$ is a prime, then $p \nmid c$ because $D_i | \Delta$, and so we have that $\chi_D^\Delta(p) = \left(\frac{D}{p}\right) = \left(\frac{c^2 D}{p}\right) = \left(\frac{D_1}{p}\right)\left(\frac{D_2}{p}\right) = \chi_1\chi_2(p)$. Thus $\chi_D^\Delta = \chi_1\chi_2$ and hence $f(\chi_1\chi_2) = D$, which proves (2.106).

(c) On p. 380 of his book, Weber[Web] introduces a "symbolic multiplication" of fundamental discriminants which is defined by the rule $\Delta_1 * \Delta_2 = (\Delta_1\Delta_2)_{fun}$. In view of the above formula (2.106), this symbolic multiplication corresponds exactly to the multiplication of characters.

We can now characterize the non-trivial genus characters $\chi \in \mathcal{G}_\Delta$ as follows.

Proposition 2.45 *Let $\chi \in \mathrm{Hom}((\mathbb{Z}/\Delta\mathbb{Z})^\times, \{\pm 1\})$ be a non-trivial character. Then*

$$\chi \in \mathcal{G}_\Delta \quad \Leftrightarrow \quad \frac{\Delta}{f(\chi)} \equiv 0, 1 \pmod 4. \tag{2.107}$$

Proof. If $D := f(\chi)$ is odd, then the condition on the right hand side is vacuous because $f(\chi) \equiv 1 \pmod 4$. Since $\chi = \prod_{d|D, d\in\mathcal{P}^*} \chi_d^\Delta \in \mathcal{G}_\Delta$, we see that (2.107) holds in this case.

Thus, assume that D is even. Then $D = D_2 D'$ where $D_2 \in \{-4, \pm 8\}$ and $D' \equiv 1 \pmod 4$ is squarefree. Then $\chi = \chi_{D_2}^\Delta \chi_{D'}^\Delta$. From the definition of $\mathcal{G}_\Delta$ and Remark 1.15(b) we see that $\chi_{D'} \in \mathcal{G}_\Delta$ and so $\chi \in \mathcal{G}_\Delta \Leftrightarrow \chi_{D_2}^\Delta \in \mathcal{G}_\Delta \Leftrightarrow D_2 \in \mathcal{P}^*(\Delta) \Leftrightarrow \frac{\Delta}{D_2} \equiv 0, 1 \pmod 4 \Leftrightarrow \frac{\Delta}{D} \equiv 0, 1 \pmod 4$, the latter because $\frac{\Delta}{D} \equiv \frac{\Delta}{D_2} \pmod 4$.

This result can be used to identify the nontrivial elements of the quotient group $\overline{\mathcal{G}}_\Delta = \mathcal{G}_\Delta / \langle \chi_\Delta \rangle$ with the set of *fundamental factorizations* of Δ; the latter are defined as follows.

Definition. A *fundamental factorization* of a discriminant Δ is an (unordered) pair (D_1, D_2) of fundamental discriminants D_1, D_2 such that $\Delta = D_1 D_2 c^2$, for some $c \in \mathbb{Z}$.

Corollary 2.46 *The rule $\chi \mapsto (f(\chi), f(\chi\chi_\Delta))$ induces a bijection between the set $(\overline{\mathcal{G}}_\Delta)' := \mathcal{G}_\Delta / \langle \chi_\Delta \rangle \setminus \{\langle \chi_\Delta \rangle\}$ and the set of fundamental factorizations of Δ.*

Proof. We first show that if $\chi \neq 1, \chi_\Delta$, then $(f(\chi), f(\chi\chi_\Delta))$ is a fundamental factorization of Δ. For this, write $D_1 = f(\chi) | \Delta$. Then $\frac{\Delta}{D_1} \equiv 0, 1 \pmod 4$ by Proposition 2.45, and $\frac{\Delta}{D_1}$ cannot be a perfect square, for else $\chi = \chi_{D_1}^\Delta = \chi_\Delta$. Thus, $\frac{\Delta}{D_1}$ is a discriminant, and so $D_2 := (\frac{\Delta}{D_1})_{fun}$ is defined. This means that $\frac{\Delta}{D_1} = c^2 D_2$ for some $c \in \mathbb{Z}$, and so (D_1, D_2) is a fundamental factorization of Δ. It remains to show that $D_2 = f(\chi\chi_\Delta)$, or equivalently, that $\chi' := \chi_{D_2}^\Delta = \chi\chi_\Delta$. But since $D_1 D_2 c^2 = \Delta$, we have that $(D_1 D_2)_{fun} = \Delta_{fun} = \Delta_K$. Thus $f(\chi_\Delta) = \Delta_K = (D_1 D_2)_{fun} = f(\chi\chi')$ by (2.106), and so $\chi_\Delta = \chi\chi'$ by Lemma 2.6 and hence $\chi' = \chi^{-1}\chi_\Delta = \chi\chi_\Delta$. This shows that $(f(\chi), f(\chi\chi_\Delta)) = (D_1, D_2)$ is a fundamental factorization of Δ.

It is immediate that this map is injective, for if $(f(\chi_1), f(\chi_1\chi_\Delta)) = (f(\chi_2), f(\chi_2\chi_\Delta))$, then by Lemma 2.6 we have that $\chi_2 \in \{\chi_1, \chi_1\chi_\Delta\}$, and so the two cosets $\{\chi_i, \chi_i\chi_\Delta\}$, $i = 1, 2$, of $\langle\chi_\Delta\rangle$ in $\mathcal{G}_\Delta$ are identical.

Finally, to prove surjectivity, let (D_1, D_2) be a fundamental factorization of Δ, so $\Delta = D_1D_2c^2$, for some $c \in \mathbb{Z}$. Then $\frac{\Delta}{D_1} = D_2c^2 \equiv 0, 1 \pmod 4$ and similarly $\frac{\Delta}{D_2} = D_1c^2 \equiv 0, 1 \pmod 4$, so by Proposition 2.45 there exist $\chi_i \in \mathcal{G}_\Delta$, $\chi_i \neq 1$, such that $f(\chi_i) = D_i$. Moreover, since $(D_1D_2)_{fun} = \Delta_{fun}$, we have by (2.106) and Lemma 2.6 that $\chi_\Delta = \chi_1\chi_2$, so $\chi_2 = \chi_1^{-1}\chi_\Delta = \chi_1\chi_\Delta$ (and hence also $\chi_1 \neq \chi_\Delta$).

We can now state the main result of genus theory in the following way.

Theorem 2.5 *Let $\Delta = f^2\Delta_K$ be a discriminant, and let (D_1, D_2) be a fundamental factorization of Δ. Put*

$$\chi_{D_1,D_2}(\mathfrak{p}) = \begin{cases} \left(\frac{D_1}{N\mathfrak{p}}\right) & \text{if } (N\mathfrak{p}, D_1) = 1 \\ \left(\frac{D_2}{N\mathfrak{p}}\right) & \text{if } (N\mathfrak{p}, D_2) = 1 \end{cases} \tag{2.108}$$

when $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ with $N\mathfrak{p} \nmid f$. Then χ_{D_1,D_2} defines a non-trivial quadratic character on $I_K(f)/P_K^+(f, f) \simeq cl(\Delta)$, and every non-trivial quadratic character χ is of the form $\chi = \chi_{D_1,D_2}$, for a unique fundamental factorization (D_1, D_2) of Δ.

Proof. We first show that χ_{D_1,D_2} is well-defined, i.e. that $\left(\frac{D_1}{N\mathfrak{p}}\right) = \left(\frac{D_2}{N\mathfrak{p}}\right)$ if $(N\mathfrak{p}, D_1) = (N\mathfrak{p}, D_2) = (N\mathfrak{p}, f) = 1$. To see this, note first that since $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, for some prime p, we have $p\mathcal{O}_K \subset \mathfrak{p}$ and so $N\mathfrak{p}|N(p\mathcal{O}_K) = p^2$. Thus $p \nmid D_1D_2 = \frac{\Delta}{c^2} = (\frac{f}{c})^2\Delta_K$, for some $c \in \mathbb{Z}$ and hence $p \nmid \Delta_K$. Thus $p \nmid f^2\Delta_K = \Delta$, so $\mathfrak{p} \in Id_K(\Delta)$. But then $\left(\frac{D_1}{N\mathfrak{p}}\right)\left(\frac{D_2}{N\mathfrak{p}}\right) = \left(\frac{D_1D_2}{N\mathfrak{p}}\right) = \chi_\Delta(N\mathfrak{p}) = 1$ by (2.103), and so $\left(\frac{D_1}{N\mathfrak{p}}\right) = \left(\frac{D_2}{N\mathfrak{p}}\right)$, as claimed.

Next we observe that if $(N\mathfrak{p}, f) = 1$, then either $(N\mathfrak{p}, D_1) = 1$ or $(N\mathfrak{p}, D_2) = 1$. Indeed, if not, then $p|(D_1, D_2)$ (where p is as above), and hence $p^2|D_1D_2|\Delta = f^2\Delta_K$. If $p \neq 2$, then this forces $p|f$, contrary to the hypothesis. If $p = 2$, then we must have that f is odd and that $\Delta_K \equiv 0 \pmod 4$. But then either $4||\Delta_K$ or $8||\Delta_K$, so in that case at least one of D_1 or D_2 must be odd, and the assertion follows.

From the above we therefore see that the rule (2.108) extends uniquely to a homomorphism $\chi_{D_1,D_2} : I_K(f) \to \{\pm 1\}$ such that $\chi_{D_1,D_2}(\mathfrak{a}) = \chi_{D_1}(N(\mathfrak{a}))$, whenever $\mathfrak{a} \in I_K(fD_i)$. We now show:

Claim: $P_K^+(f, f) \leq \mathrm{Ker}(\chi_{D_1,D_2})$.

To verify this, note first that $P_K^+(f, \Delta) \leq \mathrm{Ker}(\chi_{D_1,D_2})$. Indeed, since (D_1, D_2) is a fundamental factorization of Δ, we know that $\chi_{D_i}^\Delta \in \mathcal{G}_\Delta$ (cf. Corollary 2.46), and from Corollary 2.43 it follows that $\chi := \chi_{D_1}^\Delta \circ N_\Delta = \chi_{D_2}^\Delta \circ N_\Delta$ is trivial on $P_K^+(f, \Delta)$. Thus, since χ is just the restriction of χ_{D_1,D_2} to $I_K(\Delta)$, we see that $P_K^+(f, \Delta) \leq \mathrm{Ker}(\chi_{D_1,D_2})$.

Next, let p be a prime (of $\mathbb{Z}$) with $p \nmid f$. Then, as was pointed out above, we have $p \nmid D_i$ for some $i = 1, 2$, and so $\chi_{D_1,D_2}(p\mathcal{O}_K) = \left(\frac{D_i}{N(p\mathcal{O}_K)}\right) = \left(\frac{D_i}{p^2}\right) = 1$. Thus, using

the notation of Lemma 2.7 below, we have that $P_{K,\mathbb{Z}}(f) \leq \mathrm{Ker}(\chi_{D_1,D_2})$ and so the claim follows from Lemma 2.7.

This, therefore, shows that $\chi_{D_1,D_2} \in \mathrm{Hom}(I_K(f)/P_K^+(f,f), \{\pm 1\})$. Conversely, if $\chi \in \mathrm{Hom}(I_K(f)/P_K^+(f,f), \{\pm 1\})$, then $\chi' := \chi \circ (\overline{\varphi}^+_{\mathcal{O}_\Delta,f})^{-1} \in \mathrm{Hom}(\mathrm{Pic}^+(\mathcal{O}_\Delta), \{\pm 1\})$, and so by Corollary 2.43 there exists $\chi_1 \in \mathcal{G}_\Delta$ such that

$$\chi' \circ \overline{\varphi}^+_{\mathcal{O}_\Delta,\Delta} \;=\; \chi_1 \circ \overline{N}_\Delta \;=\; \chi_1\chi_\Delta \circ \overline{N}_\Delta.$$

Put $\chi_2 = \chi_1\chi_\Delta$ and $D_i = f(\chi_i)$, for $i = 1, 2$. Then by Proposition 2.46 we know that (D_1, D_2) is a fundamental factorization of Δ which is uniquely determined by $\{\chi_1, \chi_2\}$ and hence by χ'. Let $\chi_{D_1,D_2} : I_K(f) \to \{\pm 1\}$ be the homomorphism defined by (2.108). Then by construction we have that

$$\chi_{D_1,D_2}(\mathfrak{a}) = \left(\frac{D_1}{N(\mathfrak{a})}\right) = \chi^\Delta_{D_1}(N(\mathfrak{a})) = \chi' \circ \overline{\varphi}^+_{\mathcal{O}_\Delta,\Delta}(\mathfrak{a})) = \chi(\mathfrak{a}), \quad \text{if } \mathfrak{a} \in I_K(\Delta),$$

and so $\chi_{D_1,D_2} = \chi$ because every class in $I_K(f)/P_K^+(f,f)$ can be represented by an ideal/lattice $\mathfrak{a} \in I_K(\Delta)$; cf. Corollary 2.35 (together with Theorem 2.4).

In the above proof we had used the following elementary fact.

Lemma 2.7 *Let $P_{K,\mathbb{Z}}(m) \leq I_K(m)$ denote the group generated by the principal ideals $p\mathcal{O}_K$, where p is a prime number with $p \nmid m$. If $f|m$, then we have that*

$$P_K(f,m) = P_{K,\mathbb{Z}}(m) \cdot P_{K,1}(f) \quad \textit{and} \quad P_K^+(f,m) = P_{K,\mathbb{Z}}(m) \cdot P^+_{K,1}(f), \tag{2.109}$$

where $P_{K,1}(f)$ and $P_{K,1}(f)$ are the group of principal ideals generated by the set $K_1(f) = 1 + f\mathcal{O}_K$ and $K_1^+(f) = K_1(f) \cap K_+$, respectively. In particular, we have that

$$P_K^+(f,f) \;=\; P_{K,\mathbb{Z}}(f)P_K^+(f,m).$$

Proof. Clearly $P_{K,1}(f) \leq P_K(f,m)$ and $P^+_{K,1}(f) \leq P_K^+(f,m)$. Moreover, if $p \nmid m$, then $p = p + 0f \in \mathcal{O}_K(f,m) \cap K_+$ because $N_K(p) = p^2 > 0$, and so $P_{K,\mathbb{Z}}(m) \leq P_K^+(f,m) \leq P_K(f,m)$. Thus $P_{K,\mathbb{Z}}(m)P_{K,1}(f) \leq P_K(f,m)$ and $P_{K,\mathbb{Z}}(m)P^+_{K,1}(f) \leq P_K^+(f,m)$.

To prove the opposite inclusions, let $\alpha \in \mathcal{O}_K(f,m) \cap K_+$, so $\alpha = a + f\beta$ with $\beta \in \mathcal{O}_K$ and $(a,m) = 1$. Thus $ax + my = 1$, for some $x, y \in \mathbb{Z}$ and so $x\alpha = 1 + f(x\beta - y\frac{m}{f}) \in \mathcal{O}_K(f,m) \cap K_+$ (because $N(x\alpha) = x^2N(\alpha) > 0$). Thus $\alpha\mathcal{O}_K = (x\alpha\mathcal{O}_K)(x\mathcal{O}_K)^{-1} \in P^+_{K,1}(f)P_{K,\mathbb{Z}}(m)$, and so $P_K^+(f,m) \leq P^+_{K,1}(f)P_{K,\mathbb{Z}}(f)$ because $P_K^+(f,m)$ is generated by elements $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K(f,m) \cap K_+$. This proves that $P_K^+(f,m) = P_{K,\mathbb{Z}}(m)P^+_{K,1}(f)$, and the proof for $P_K(f,m)$ is similar.

Finally, since clearly $P_{K,\mathbb{Z}}(m) \leq P_{K,\mathbb{Z}}(f)$, we see from (2.109) that $P_{K,\mathbb{Z}}(f)P^+(f,m) = P_{K,\mathbb{Z}}(f)(P_{K,\mathbb{Z}}(m)P^+_{K,1}(f)) = P_{K,\mathbb{Z}}(f)P^+_{K,1}(f) = P_K^+(f,f)$, as asserted.

Bibliography

[Ah] L. Ahlfors, *Complex Analysis*. Addison-Wesley, Reading, 1965.

[BA] N. Bourbaki, *Algebra*. Chapters 1–3, Hermann/Addison Wesley, Reading, 1974. Chapters 4–7, Springer-Verlag, New York, 1988.

[Bu] D. Buell, *Binary Quadratic Forms*. Springer Verlag, New York, 1989.

[BV] J. Buchmann, U. Vollmer, *Binary Quadratic Forms*. Springer Verlag, New York, 2007.

[Cox] D. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory and Complex Multiplication*. John Wiley, New York, 1989.

[Di] L. Dickson, *History of the Theory of Numbers*, 3 vols. 1919-1923. Reprint: Chelsea Publ. Co., New York, 1971.

[DA] C.F. Gauss, *Untersuchungen über höhere Arithmetik*. Translation (1889) of *Disquisitiones Arithmeticae* (1801) by H. Maser. Reprint: Chelsea Publ. Co., New York, 1981.

[HW] G. Hardy, E. Wright, *An Introduction to the Theory of Numbers*. 4th ed. Oxford Press, London, 1960.

[Hu] Hua Loo Keng, *Introduction to Number Theory*. Springer-Verlag, Berlin, 1982.

[Ko1] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, New York, 1984.

[Ko2] N. Koblitz, *A Course in Number Theory and Cryptography*. 2nd ed., Springer-Verlag, New York, 1994.

[La1] S. Lang, *Diophantine Approximations*. Addison-Wesley, Reading, MA, 1966.

[La2] S. Lang, *Elliptic Functions*. Addison-Wesley, Reading, MA, 1973.

[La3] S. Lang, *Algebra*. Revised 3rd ed. Springer, New York, 2002.

[Se1] J.-P. Serre, *A Course in Arithmetic*. Springer-Verlag, New York, 1973.

[Sh] D. Shanks, *Solved and Unsolved Problems in Number Theory*. 2nd ed. Chelsea Publ. Co., New York, 1978.

[Si] C.L. Siegel, *Topics in Complex Function Theory I.* Wiley, New York, 1969.

[ST] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*. Springer-Verlag, New York, 1992.

[Web] H. Weber, *Lehrbuch der Algebra III.* Teubner, 1908. Chelsea Reprint, ?.

[We] A. Weil, *Number Theory: An Approach through History. From Hammurapi to Legendre*. Birkhäuser, Boston, 1983.