FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Kristýna Zemková

Composition of quadratic forms over number fields

Department of Algebra

Supervisor of the master thesis:	Mgr. Vítězslav Kala, Ph.D.
Study programme:	Mathematics
Study branch:	Mathematical Structures

Prague 2018

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

Prague, 1 May 2018 signature of the author

I would like to thank to my supervisor, Mgr. Vítězslav Kala, PhD., for his friendly and encouraging approach.

I would like to dedicate the thesis to my parents: to my father, who ignited my passion for mathematics already in my early childhood, and to my mother, who supports me in studying theoretical mathematics, although she does not fully agree with my choice.

Title: Composition of quadratic forms over number fields

Author: Kristýna Zemková

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The thesis is concerned with the theory of binary quadratic forms with coefficients in the ring of algebraic integers of a number field. Under the assumption that the number field is of narrow class number one, there is developed a theory of composition of such quadratic forms. For a given discriminant, the composition is determined by a bijection between classes of quadratic forms and a so-called relative oriented class group (a group closely related to the class group). Furthermore, Bhargava cubes are generalized to cubes with entries from the ring of algebraic integers; by using the composition of quadratic forms, the composition of Bhargava cubes is proved in the generalized case.

Keywords: number field, binary quadratic form, composition, class group, Bhargava cube

Contents

Introduction

Throughout the history, mathematicians have been excited about discovering new identities. One of the famous is the *Brahmagupta's identity*:

$$\left(x_1^2 + ny_1^2\right)\left(x_2^2 + ny_2^2\right) = \left(x_1x_2 + ny_1y_2\right)^2 + n\left(x_1y_2 - y_1x_2\right)^2.$$

The beauty of this identity resides in the fact that if you have two integers, m_1 and m_2, such that both of them can be written in the form $x^2 + ny^2$ for some integers x and y, then their product, m_1m_2, can be written again in the same form; we say that $x^2 + ny^2$ *represents* the numbers m_1, m_2 and m_1m_2. One may naturally ask if this is an isolated identity, or if it is just one example from some wider family of identities. Assume that we are given two binary quadratic forms, Q_1 and Q_2. Can we find any binary quadratic form Q with the following property?

$$Q_1(x_1, y_1) = m_1 \;\&\; Q_2(x_2, y_2) = m_2 \;\Rightarrow\; \exists x_0, y_0 : \; Q(x_0, y_0) = m_1m_2 \qquad (*)$$

This is what we call *composition of quadratic forms*; we are seeking a law with the property $(*)$ on the set of binary quadratic forms.

Inspired by the Brahmagupta's identity, we may want the composition to be just a multiplication together with some rearrangement of the variables. Formally, we can define a binary quadratic form Q to be a composition of two binary quadratic forms Q_1 and Q_2, if we are able to find some numbers a_i, b_i, c_i, d_i, $i = 1, 2$, such that

$$\begin{aligned} &Q_1(x_1, y_1) \cdot Q_2(x_2, y_2) = Q(B_1(x_1, y_1; x_2, y_2), B_2(x_1, y_1; x_2, y_2)),\\ \text{where}&\\ &B_i(x_1, y_1; x_2, y_2) = a_ix_1x_2 + b_ix_1y_2 + c_iy_1x_2 + d_iy_1y_2, \quad i = 1, 2, \end{aligned} \qquad (\dagger)$$

are two bilinear forms. In this way, we have quite a great freedom in how to compose two quadratic forms, and it will always satisfy the property $(*)$.

There are many different binary quadratic forms. But looking a bit closer, we can see that actually many of them are basically the same: at the first glance, the quadratic forms $x^2 + 5y^2$ and $49x^2 + 64xy + 21y^2$ do not seem to have anything in common, but once we notice that

$$49x^2 + 64xy + 21y^2 = (2x + y)^2 + 5(3x + 2y)^2,$$

and, more surprisingly,

$$x^2 + 5y^2 = 49(2x - y)^2 + 64(2x - y)(-3x + 2y) + 21(-3x + 2y)^2,$$

we can conclude that these two binary quadratic forms represent the same numbers. In this way, we can group the "similar" binary quadratic forms into *classes*. An interesting property of these classes is the fact that all quadratic forms within one class have the same *discriminant*. We can now seek the law of composition only on these classes; we can still use the same composition as in $(\dagger)$, but now the problem is that by using different ways, we may end up with quadratic forms from different classes. Thus, we have to restrict our freedom; it turns out that the following must hold:

$$a_1b_2 - a_2b_1 = Q_1(1,0), \qquad a_1c_2 - a_2c_1 = Q_2(1,0)$$

(see Cox [1997]). Furthermore, this definition has another advantage: it preserves the discriminant, i.e. if the quadratic forms Q_1 and Q_2 have the same discriminant, then their composition Q has again the same discriminant. So we can actually study only classes of binary quadratic forms with a fixed discriminant. And that is much simpler task, since there are only finitely many of them!

We have just described the approach taken by Gauss in his Disquisitiones Arithmeticae in 1801, where he considered the *integral* quadratic forms, i.e. quadratic forms with coefficients from $\mathbb{Z}$. Another approach is attributed to Gauss's student, Dirichlet. He discovered so-called *united forms*, which are easy to compose; the composition can be written explicitely:

$$\left(a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2\right)\left(a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2\right) = a_1a_2x^2 + Bxy + Cy^2,$$

where $x = x_1x_2 - Cx_2y_2$ and $y = a_1x_1y_2 + a_2y_1x_2 + By_1y_2$. The trick behind this composition is that for any pair of (primitive) binary quadratic forms of the same discriminant, we can find another pair of quadratic forms within the same classes, which are of the form $a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2$ and $a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2$ for some a_1, a_2, B and C.

Yet completely different approach was taken by Dedekind. In modern terms, his idea was to associate a binary quadratic form with an appropriate module:

$$ax^2 + bxy + cy^2 \longmapsto \left[a, \frac{-b + \sqrt{b^2 - 4ac}}{2}\right]_{\mathbb{Z}};$$

the composition of quadratic forms is then translated as module multiplication. Again, this is defined on classes of quadratic forms, and hence we group together some modules on the right side as well; the resulting structure is called *class group* and depends on the considered discriminant.

Although very different from each other, all these three approaches actually result in the same composition law and equip the set of classes of binary quadratic forms (all of the quadratic forms having the same discriminant) with a group structure.

Later on, combination of all the three aforementioned approaches and some new methods taken by Butts and Estes [1968], Kaplansky [1968], Dulin and Butts [1972], Towber [1980], Kneser [1982] led to composition of quadratic forms over an arbitrary commutative ring with 1. It is worth noting that in all the aforementioned articles, whenever some kind of classes of quadratic forms are considered, they always arise from an equivalence, which is given by action on (x, y) by matrices of determinant 1. This can be seen as somewhat unnatural, as the base ring may contain another units as well. In the case of the ring of integers of a number field, the most natural choice seems to be to consider action by matrices, determinant of which is a totally positive unit. Indeed, this approach was taken by Mastropietro [2000], but only under the additional conditions that the base field is a real quadratic number field of class number one, and that the discriminant of the quadratic forms is totally negative.

At this point we are coming to the first goal of this thesis, and that is to take into account an equivalence of binary quadratic forms given by all totally positive units of the base number field, and to develop, in such settings, a Dedekind-like correspondence between classes of forms and some kind of class group. As the base field we will consider an arbitrary number field of narrow class number one; this is equivalent to having class number one together with the existence of units of all signs. These conditions are quite restrictive, but there still exist infinitely many such number fields, and the conditions are necessary for our approach: first, the class number has to be one for a free module basis of any fractional ideal to exist, and second, units of all signs are needed in order for such a basis to be able to have any orientation. The construction together with some applications can be found in Chapter 2; this part of the thesis has already been submitted for publication as the article Zemková [2017].

The story about composition of quadratic forms over $\mathbb{Z}$ did not end after its generalization to an arbitrary ring. It was not until the beginning of the 21st century that Bhargava [2004] redefined Gauss composition, and discovered another 13 composition laws on other polynomials. The beauty of these composition laws is in using cubes of integers:

$$\begin{tikzcd}
& e \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[dd, dash] & \\
& g \arrow[rr, dash] \arrow[dl, dash] & & h \arrow[dl, dash] \\
c \arrow[rr, dash] & & d &
\end{tikzcd} .$$

Similarly as Gauss, Dirichlet and others, Bhargava grouped such cubes into classes. His result is then based on a correspondence between these classes of integral cubes and certain triples of elements of narrow class group. Later on, some generalizations were given by Wood [2011] and O'Dorney [2016].

Having the composition of quadratic forms over rings of algebraic integers from Chapter 2, naturally the question is arising, whether this composition could be generalized to composition of cubes; we give the answer in Chapter 3. Contrary to Bhargava, our aim is not to redefine the composition of quadratic forms, but to use it to construct a new composition law on cubes. Despite that, we will also obtain a new description of composition of quadratic forms.

All along the way, we are meeting different kind of class groups. Class groups are very interesting (and difficult) topic on their own, so we will devote at least Chapter 4 to them. We will be especially interested in the relationship between class group and narrow class group. This relationship is well known in the case of a quadratic number field, and not so widely known, although fully described, in general. We prove this relationship by using a new description of narrow class group.

1. Preliminaries

Before we can immerse into all the promised correspondences themselves, we need to do some preparatory work. Most of the time we will work with a base field K and its quadratic extension L. Hence, after setting the notation, we will investigate properties of the ring of algebraic integers of the number field L and of its ideals, where we will use the information that it is a quadratic extension of K. We will also take a look at binary quadratic forms with coefficients in the ring of algebraic integers of K. Importantly, we will define a new class group, which will be used in all the correspondences later.

1.1 Basic notation

Let F be a number field. The *norm* of $a \in F$ is defined by

$$\mathcal{N}_F(a) = \prod_{\sigma} \sigma(a),$$

where σ runs over all embeddings of F into $\mathbb{C}$. We will be usually interested only in the embeddings of the field F into real numbers; denote by R^F the set of all such embeddings. We say that an element $a \in F$ is *totally positive* if $\sigma(a) > 0$ for every $\sigma \in R^F$. Note that if F is totally complex, i.e. it has no embeddings into real numbers, the condition of being totally positive is trivially satisfied for all nonzero elements.

We write $\mathcal{O}_F$ for the ring of algebraic integers of F, and we denote by $\mathcal{U}_F$ the *group of units*, i.e.

$$\mathcal{U}_F = \{u \in \mathcal{O}_F \mid \mathcal{N}_F(u) = \pm 1\},$$

and by $\mathcal{U}_F^+$ its subgroup of *totally positive units*, i.e.

$$\mathcal{U}_F^+ = \left\{u \in \mathcal{U}_F \mid \operatorname{sgn}(\sigma(u)) = +1 \ \forall \sigma \in R^F\right\}.$$

If E/F is a Galois extension of fields, then we define the *relative norm* and the *relative trace* of $\alpha \in E$ respectively by

$$\mathcal{N}_{E/F}(\alpha) = \prod_{\tau \in \mathrm{Gal}(E/F)} \tau(\alpha),$$
$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{\tau \in \mathrm{Gal}(E/F)} \tau(\alpha).$$

Throughout the whole thesis, we fix a number field K of narrow class number one; this is equivalent to K being of class number one and having units of all signs (this fact will be proved in Corollary 4.3). Assume that K has exactly r embeddings into real numbers, and let $\sigma_1, \dots, \sigma_r$ be these embeddings; hence

$$R^K = \{\sigma_1, \dots, \sigma_r\}.$$

Furthermore, we fix a relative quadratic extension L of the number field K. Note that the Galois group $\mathrm{Gal}(L/K)$ has two elements; let τ be the nontrivial element of this group. For $\alpha \in L$, we write $\overline{\alpha}$ instead of $\tau(\alpha)$: if $L = K\left(\sqrt{D}\right)$

and $\alpha = a + b\sqrt{D}$ for some $a, b \in K$, then $\overline{\alpha} = a - b\sqrt{D}$. Note that then, for $\alpha \in L$,

$$\begin{aligned} \mathcal{N}_{L/K}(\alpha) &= \alpha\overline{\alpha}, \\ \mathrm{Tr}_{L/K}(\alpha) &= \alpha + \overline{\alpha}. \end{aligned}$$

We will denote elements of the field K by latin letters and elements of the field L by greek letters.

1.2 Ring of algebraic integers $\mathcal{O}_L$

We will describe the ring of algebraic integers of the field L as the $\mathcal{O}_K$-module. The module basis of an $\mathcal{O}_L$-ideal will be always written in square brackets, e.g. $[\alpha, \beta]_{\mathcal{O}_K}$; the index $\mathcal{O}_K$ will be often omitted, and the ideal will be denoted simply by $[\alpha, \beta]$. On the other hand, by (α, β) we understand the $\mathcal{O}_L$-ideal generated by the elements α, β.

Recall that we assume $h^+(K) = 1$, which implies $h(K) = 1$.[1] As $h(K) = 1$ holds if and only if every quadratic extension of K has a relative integral basis (see [Narkiewicz, 2004, Cor. p. 388]), there exists an $\mathcal{O}_K$-module basis of $\mathcal{O}_L$. In the next proposition, we will take a closer look at this basis. At this point, we can say that the condition $h(K) = 1$ is crucial, because otherwise $\mathcal{O}_L$ would not be any free $\mathcal{O}_K$-module. It will be explained in Section 1.5 why we need even stronger condition $h^+(K) = 1$.

Proposition 1.1. *There exists $\Omega \in \mathcal{O}_L$ such that $\mathcal{O}_L = [1, \Omega]_{\mathcal{O}_K}$.*

Proof. Let n be an integer, and suppose that $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ are chosen in such way that $\mathcal{O}_L = [\alpha_1, \dots, \alpha_n]_{\mathcal{O}_K}$. Since $[L : K] = 2$, the elements $\alpha_1, \dots, \alpha_n$ are linearly dependent over K if $n \geq 3$. Then they are linearly dependent over $\mathcal{O}_K$ as well, because K is the field of fractions of the ring $\mathcal{O}_K$. Hence, $n \leq 2$. Suppose that $n = 1$, i.e. $\mathcal{O}_L = [\alpha_1]_{\mathcal{O}_K}$. Since $1 \in \mathcal{O}_L$, there must exist $z \in \mathcal{O}_K$ such that $z\alpha_1 = 1$; but then $\alpha_1 = \frac{1}{z} \in K$, and thus $\mathcal{O}_L \subset K$ which is a contradiction. Therefore, $n = 2$ and $\mathcal{O}_L = [\alpha_1, \alpha_2]_{\mathcal{O}_K}$ for some elements $\alpha_1, \alpha_2 \in \mathcal{O}_L$.

We have

$$\begin{aligned} \mathrm{Disc}(\mathcal{O}_L/\mathcal{O}_K) &= \det \begin{pmatrix} \mathrm{Tr}_{L/K}(\alpha_1^2) & \mathrm{Tr}_{L/K}(\alpha_1\alpha_2) \\ \mathrm{Tr}_{L/K}(\alpha_1\alpha_2) & \mathrm{Tr}_{L/K}(\alpha_2^2) \end{pmatrix} \\ &= \det \begin{pmatrix} \alpha_1^2 + \overline{\alpha_1^2} & \alpha_1\alpha_2 + \overline{\alpha_1\alpha_2} \\ \alpha_1\alpha_2 + \overline{\alpha_1\alpha_2} & \alpha_2^2 + \overline{\alpha_2^2} \end{pmatrix} \\ &= (\alpha_1^2 + \overline{\alpha_1^2})(\alpha_2^2 + \overline{\alpha_2^2}) - (\alpha_1\alpha_2 + \overline{\alpha_1\alpha_2})^2 \\ &= (\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2})^2. \end{aligned}$$

Denote $\Omega = \overline{\alpha_1}\alpha_2$, and note that $\overline{\Omega} = \alpha_1\overline{\alpha_2}$. Let us look at the ideal $[1, \Omega]_{\mathcal{O}_K}$:

$$\begin{aligned} &\det \begin{pmatrix} \mathrm{Tr}_{L/K}(1^2) & \mathrm{Tr}_{L/K}(1 \cdot \Omega) \\ \mathrm{Tr}_{L/K}(1 \cdot \Omega) & \mathrm{Tr}_{L/K}(\Omega^2) \end{pmatrix} = \det \begin{pmatrix} 1 + 1 & \Omega + \overline{\Omega} \\ \Omega + \overline{\Omega} & \Omega^2 + \overline{\Omega^2} \end{pmatrix} \\ &= 2\left(\Omega^2 + \overline{\Omega^2}\right) - \left(\Omega + \overline{\Omega}\right)^2 = \left(\Omega - \overline{\Omega}\right)^2 \\ &= (\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2})^2 = \mathrm{Disc}(\mathcal{O}_L/\mathcal{O}_K). \end{aligned}$$

[1] $h(K)$ and $h^+(K)$ stands for the class number and the narrow class number of the number field K, respectively; see Chapter 4 for details.

Hence $[1, \Omega]_{\mathcal{O}_K} = \mathcal{O}_L$ (see e.g. [Milne, 2008, Prop. 2.24]). □

It will be useful to describe Ω and the elements of the ring $\mathcal{O}_L$ in general. As an algebraic integer over $\mathcal{O}_K$, Ω is a root of a monic quadratic polynomial x^2+wx+z for some $w, z \in \mathcal{O}_K$; the other root is of course $\overline{\Omega}$. Set $D_\Omega = w^2 - 4z$. It follows from the proof of Proposition 1.1 that the elements Ω and $\overline{\Omega}$ are interchangeable; thus, without loss of generality,

$$\Omega = \frac{-w + \sqrt{D_\Omega}}{2}, \qquad \overline{\Omega} = \frac{-w - \sqrt{D_\Omega}}{2}. \tag{1.1}$$

From now on, Ω will be fixed, and $[1, \Omega]$ will be the canonical basis of $\mathcal{O}_L$ (as an $\mathcal{O}_K$-module). Note that $L = K\left(\sqrt{D_\Omega}\right)$, and that

$$D_\Omega = \left(\Omega - \overline{\Omega}\right)^2. \tag{1.2}$$

Corollary 1.2. $\mathcal{O}_L \subseteq \left\{ \frac{a}{2} + \frac{b}{2}\sqrt{D_\Omega} \;\middle|\; a, b \in \mathcal{O}_K \right\}$

Proof. Every element of $\mathcal{O}_L$ is of the form

$$a + b\Omega = a + b\frac{-w + \sqrt{D_\Omega}}{2} = \frac{2a - bw}{2} + \frac{b}{2}\sqrt{D_\Omega}$$

for some $a, b \in \mathcal{O}_K$. □

One may expect the element D_Ω to be square-free (i.e. not divisible by q^2 for any $q \in \mathcal{O}_K \backslash \mathcal{U}_K$), but since D_Ω is the discriminant of a binary quadratic form, it may not always be the case. Hence, instead of that, we introduce the following definition of fundamental element: an element, which is “almost square-free” and a quadratic residue modulo 4 at the same time. Note that the condition $h^+(K)$ implies that we work in a principal ideal domain, and thus the definition makes sense.

Definition 1.3. *An element d of $\mathcal{O}_K$ is called* fundamental *if d is a quadratic residue modulo 4 in $\mathcal{O}_K$ and*

- *either d is square-free,*
- *or for every $p \in \mathcal{O}_K \backslash \mathcal{U}_K$ such that $p^2 \mid d$ the following holds: $p \mid 2$ and $\frac{d}{p^2}$ is not a quadratic residue modulo 4 in $\mathcal{O}_K$.*

In the case $K = \mathbb{Q}$, this definition agrees with the one of the *fundamental discriminant.* The following lemma shows that, from this point of view, D_Ω is “a fundamental discriminant over K”.

Lemma 1.4. *D_Ω is a fundamental element of $\mathcal{O}_K$.*

Proof. Clearly D_Ω is a quadratic residue modulo 4. Assume that there exists $p \in \mathcal{O}_K$ which is not a unit, and such that $p^2 \mid D_\Omega$; set $D' = \frac{D_\Omega}{p^2}$. Since $\sqrt{D'}$ is a root of the polynomial $x^2 - D'$, and thus $\sqrt{D'} \in \mathcal{O}_L$, there exist $a, b \in \mathcal{O}_K$ such that $\sqrt{D'} = a + b\Omega$ where $\Omega = \frac{-w+p\sqrt{D'}}{2}$. Comparing the coefficients at $\sqrt{D'}$, we get that p must be a divisor of 2 in $\mathcal{O}_K$.

For contradiction, suppose that there exists an element $t \in \mathcal{O}_K$ such that $D' \equiv t^2 \pmod 4$. We can find $m \in \mathcal{O}_K$ such that $D' = t^2 - 4m$; then the quadratic polynomial $x^2 + tx + m$ has the discriminant equal to D' and a root $\kappa = \frac{-t+\sqrt{D'}}{2}$, which is an element of $\mathcal{O}_L$. Hence, there exist $a', b' \in \mathcal{O}_K$ such that $\kappa = a' + b'\Omega$, i.e.

$$\frac{-t+\sqrt{D'}}{2} = a' + b'\frac{-w+p\sqrt{D'}}{2}.$$

Comparing the coefficients at $\sqrt{D'}$, we obtain that $b'p = 1$. But that is not possible, because $b' \in \mathcal{O}_K$, and p is not a unit. Hence, we have found the desired contradiction. □

On the other hand, if we take $D \in \mathcal{O}_K$ such that $K\left(\sqrt{D}\right) = L$, then clearly $p^2 D = q^2 D_\Omega$ for some $p, q \in \mathcal{O}_K$. Furthermore, if D is fundamental, then $\frac{p}{q}$ has to be a unit, because both $\frac{p^2 D}{q^2}$ and $\frac{q^2 D_\Omega}{p^2}$ are quadratic residues modulo 4. We have proved the following lemma.

Lemma 1.5. *Let D be a fundamental element of $\mathcal{O}_K$ and $K\left(\sqrt{D}\right) = L$. Then there exists $u \in \mathcal{U}_K$ such that $D = u^2 D_\Omega$.*

1.3 Quadratic forms with coefficients in $\mathcal{O}_K$

By *binary quadratic forms* over K we mean homogeneous polynomials of degree 2 with coefficients in $\mathcal{O}_K$, i.e. $Q(x,y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathcal{O}_K$. For abbreviation, we will refer to them as *quadratic forms.* By $\mathrm{Disc}(Q)$ we denote the *discriminant* of the quadratic form Q, i.e. $\mathrm{Disc}(Q) = b^2 - 4ac$. Comparing to the case of quadratic forms over $\mathbb{Q}$, we need to slightly redefine the equivalence relation.

Definition 1.6. *Two quadratic forms $Q(x,y)$ and $\widetilde{Q}(x,y)$ are* equivalent, *denoted by $Q \sim \widetilde{Q}$, if there exist elements $p, q, r, s \in \mathcal{O}_K$ satisfying $ps - qr \in \mathcal{U}_K^+$ and a totally positive unit $u \in \mathcal{U}_K^+$ such that $\widetilde{Q}(x,y) = u\, Q(px + qy, rx + sy)$.*

We may also write a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ as a matrix

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

Then the equivalence of two quadratic forms Q and $\widetilde{Q}$ can be written in the form

$$\begin{pmatrix} x & y \end{pmatrix} \widetilde{Q} \begin{pmatrix} x \\ y \end{pmatrix} = u \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} Q \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Let $Q(x,y) = ax^2 + bxy + cy^2$ be a quadratic form. Let $p, q, r, s \in \mathcal{O}_K$ be such that $ps - qr \in \mathcal{U}_K^+$, and $u \in \mathcal{U}_K^+$. Consider the binary quadratic form $\widetilde{Q}(x,y) = u\, Q(px + qy, rx + sy) = \widetilde{a}x^2 + \widetilde{b}xy + \widetilde{c}y^2$ equivalent to $Q(x,y)$. Then

$$\begin{pmatrix} \widetilde{a} & \frac{\widetilde{b}}{2} \\ \frac{\widetilde{b}}{2} & \widetilde{c} \end{pmatrix} = u \begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix};$$

thus,

$$\begin{aligned}\widetilde{a} &= u(ap^2 + bpr + cr^2),\\ \widetilde{b} &= u(2apq + b(ps + qr) + 2crs),\\ \widetilde{c} &= u(aq^2 + bqs + cs^2),\end{aligned} \tag{1.3}$$

and

$$\operatorname{Disc}(\widetilde{Q}) = \widetilde{b}^2 - 4\widetilde{a}\widetilde{c} = u^2(ps - qr)^2(b^2 - 4ac) = u^2(ps - qr)^2 \operatorname{Disc}(Q). \tag{1.4}$$

On the other hand, we have

$$\begin{aligned}a &= \frac{1}{u(ps - qr)^2}(\widetilde{a}s^2 - \widetilde{b}rs + \widetilde{c}r^2),\\ b &= \frac{1}{u(ps - qr)^2}(-2\widetilde{a}qs + \widetilde{b}(ps + qr) - 2\widetilde{c}pr),\\ c &= \frac{1}{u(ps - qr)^2}(\widetilde{a}q^2 - \widetilde{b}pq + \widetilde{c}p^2).\end{aligned} \tag{1.5}$$

For $m \in \mathcal{O}_K$, we say that $Q(x, y)$ *represents* m if there exist $x_0, y_0 \in \mathcal{O}_K$ such that $Q(x_0, y_0) = m$.

Lemma 1.7. *Equivalent quadratic forms represent the same elements of $\mathcal{O}_K$ up to the multiplication by a totally positive unit.*

Proof. Let $\widetilde{Q}$ represent $m \in \mathcal{O}_K$, i.e. $\widetilde{Q}(x_0, y_0) = m$ for some $x_0, y_0 \in \mathcal{O}_K$, and let $Q \sim \widetilde{Q}$, i.e. $\widetilde{Q}(x, y) = u\, Q(px + qy, rx + sy)$. Then

$$Q(px_0 + qy_0, rx_0 + sy_0) = u^{-1}\, \widetilde{Q}(x_0, y_0) = u^{-1}m,$$

and hence Q represents the element $u^{-1}m$. □

We say that a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is *primitive* if $\gcd(a, b, c) \in \mathcal{U}_K$. The following lemma shows that a quadratic form equivalent to a primitive quadratic form is primitive as well.

Lemma 1.8. *Let Q be a primitive quadratic form, and $\widetilde{Q} \sim Q$. Then $\widetilde{Q}$ is also primitive.*

Proof. Let $Q(x, y) = ax^2 + bxy + cy^2$ and $\widetilde{Q}(x, y) = \widetilde{a}x^2 + \widetilde{b}xy + \widetilde{c}y^2$. Assume that there exists $p \in \mathcal{O}_K$ such that $p \mid \gcd\left(\widetilde{a}, \widetilde{b}, \widetilde{c}\right)$. Then, for every $\widetilde{m} \in \mathcal{O}_K$ represented by $\widetilde{Q}$, it holds that $p \mid \widetilde{m}$. In other words, $\widetilde{Q}$ represents only numbers from $p\mathcal{O}_K$. Since Q represents the same numbers as $\widetilde{Q}$ (up to the multiplication by a totally positive unit) by Lemma 1.7, there is

$$\left.\begin{aligned} a &= Q(1, 0)\\ c &= Q(0, 1)\\ b &= Q(1, 1) - a - c \end{aligned}\right\} \in p\mathcal{O}_K,$$

and hence $p \mid a, b, c$. Since Q is primitive, p must be unit. Thus, $\widetilde{Q}$ is primitive. □

We are interested in quadratic forms of given discriminant, namely of discriminant $D_\Omega = \left(\Omega - \overline{\Omega}\right)^2$. But from (1.4) we can see that equivalent quadratic forms do not always have the same discriminant; their discriminants may differ from each other by a square of a totally positive unit. Therefore, we will consider all quadratic forms of discriminants belonging to the set

$$\mathcal{D} = \left\{ u^2 \left(\Omega - \overline{\Omega}\right)^2 \;\middle|\; u \in \mathcal{U}_K^+ \right\}.$$

Note that all the elements of $\mathcal{D}$ are almost square-free (by Lemma 1.4). We will denote by $\mathcal{Q}_\mathcal{D}$ the set of all primitive quadratic forms of discriminant in $\mathcal{D}$ modulo the equivalence relation described above:

$$\mathcal{Q}_\mathcal{D} = \left\{ Q(x,y) = ax^2 + bxy + cy^2 \;\middle|\; \begin{array}{l} a,b,c \in \mathcal{O}_K,\ \gcd(a,b,c) \in \mathcal{U}_K, \\ \operatorname{Disc}(Q) \in \mathcal{D} \end{array} \right\} \Big/ \sim .$$

Remark. Note that if $\operatorname{Disc}(Q) = u^2 D_\Omega$ for $u \in \mathcal{U}_K^+$, then $\operatorname{Disc}\left(\frac{1}{u}Q\right) = D_\Omega$. Hence, in every class of $\mathcal{Q}_\mathcal{D}$, there is a quadratic form of discriminant exactly D_Ω.

If K is totally real (and of narrow class number one), then every totally positive unit is square of a unit (for a reference, see [Edgar et al., 1986, Prop. 2.4]). Consider equivalent quadratic forms Q and Q' such that $\operatorname{Disc}(Q) = \operatorname{Disc}(Q')$, i.e.

$$Q'(x,y) = \frac{1}{ps - qr} Q(px + qy, rx + sy)$$

for some $p,q,r,s \in \mathcal{O}_K$. If $u \in \mathcal{U}_K$ is such that $ps - qr = u^2$, then

$$Q\left(\frac{p}{u}x + \frac{q}{u}y, \frac{r}{u}x + \frac{s}{u}y\right) = Q'(x,y)$$

gives the equivalence of Q and Q' with determinant 1. Therefore, in this case, our approach could be simplified to quadratic forms of discriminant exactly D_Ω, and to the equivalence by the matrices of determinant 1.

On the other hand, if K is not totally real, then the units other than 1 become important. For example, take $K = \mathbb{Q}(\mathrm{i})$, and consider the quadratic forms $Q(x,y) = x^2 + 4xy + 2y^2$ and $Q'(x,y) = \mathrm{i}x^2 + 4xy - 2\mathrm{i}y^2$. It clearly holds that $Q'(x,y) = -\mathrm{i}Q(\mathrm{i}x, y)$, but there is no matrix of determinant 1 which would provide the equivalence between Q and Q'. That can be seen as follows: by the first equality of (1.3), we need to find $p, r \in \mathbb{Z}[\mathrm{i}]$ such that $p^2 + 4pr + 2r^2 = \mathrm{i}$. But that is not possible, because the imaginary part of $p^2 + 4pr + 2r^2$ is divisible by 2.

At the end of this section, we look at roots of equivalent quadratic forms.

Lemma 1.9. *Let $Q(x,y) = ax^2 + bxy + cy^2$ be a quadratic form, $p,q,r,s \in \mathcal{O}_K$ such that $ps - qr \in \mathcal{U}_K^+$. Consider $\widetilde{Q}(x,y) = Q(px + qy, rx + sy) = \widetilde{a}x^2 + \widetilde{b}xy + \widetilde{c}y^2$, the quadratic form equivalent to $Q(x,y)$. Denote $D = \operatorname{Disc}(Q)$ and $\widetilde{D} = \operatorname{Disc}(\widetilde{Q})$. Then*

$$\frac{p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + q}{r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + s} = \frac{-b + \sqrt{D}}{2a}.$$

Proof. As $\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}$ is a root of the quadratic polynomial $\widetilde{Q}(x,1)=\widetilde{a}x^2+\widetilde{b}x+\widetilde{c}$, we can write

$$\begin{aligned}
\begin{pmatrix}\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} & 1\end{pmatrix} \quad \widetilde{Q} \quad \begin{pmatrix}\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} \\ 1\end{pmatrix} &= 0 \\
\begin{pmatrix}\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} & 1\end{pmatrix}\begin{pmatrix}p & r\\ q & s\end{pmatrix} \quad Q \quad \begin{pmatrix}p & q\\ r & s\end{pmatrix}\begin{pmatrix}\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} \\ 1\end{pmatrix} &= 0 \\
\begin{pmatrix}p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+q & r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s\end{pmatrix} \quad Q \quad \begin{pmatrix}p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+q \\ r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s\end{pmatrix} &= 0 \\
\begin{pmatrix}\frac{p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+q}{r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s} & 1\end{pmatrix} \quad Q \quad \begin{pmatrix}\frac{p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+q}{r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s} \\ 1\end{pmatrix} &= 0
\end{aligned}$$

In particular, the expression

$$\frac{p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+q}{r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s}$$

has to be one of the roots of $Q(x,1)$; either $\frac{-b+\sqrt{D}}{2a}$ or $\frac{-b-\sqrt{D}}{2a}$. One can check by direct computation (using the expressions (1.3) and (1.4)) that the former case holds. □

1.4 $\mathcal{O}_L$-ideals

In the following, the word "ideal" will generally stand for a fractional ideal, while to the usual meaning will be referred as to the "integral ideal". We assume all ideals to be nonzero. Since K has narrow class number one, every $\mathcal{O}_L$ ideal can be seen as a free $\mathcal{O}_K$ module; let us focus on some properties of these modules for a while.

Proposition 1.10. *Let I be an $\mathcal{O}_L$-ideal. Then there exist $\alpha,\beta\in L$, $\alpha,\beta\neq 0$, such that $I=[\alpha,\beta]$. If I is integral, then $\alpha,\beta\in\mathcal{O}_L$. Every other $\mathcal{O}_K$-module basis of I is of the form $[p\alpha+r\beta, q\alpha+s\beta]$ for some $p,q,r,s\in\mathcal{O}_K$ such that $ps-qr\in\mathcal{U}_K$.*

Proof. First, assume that I is an integral ideal. Then, similarly as in the proof of Proposition 1.1, any three or more elements of $\mathcal{O}_L$ are linearly dependent over $\mathcal{O}_K$. Hence, it is sufficient to prove that every possible $\mathcal{O}_K$-module basis of I needs to have at least two elements, and thus is of the form $I=[\alpha,\beta]$ for some nonzero elements α,β of $\mathcal{O}_L$.

For a contradiction, assume that $I=[\alpha]$ for a nonzero element α of $\mathcal{O}_L$, i.e. $I=\alpha\mathcal{O}_K$. Then it must hold that $\alpha\overline{\alpha}\in\alpha\mathcal{O}_K$; hence $\alpha\overline{\alpha}=\alpha t$ for an element $t\in\mathcal{O}_K$, so $\alpha(\overline{\alpha}-t)=0$. Since $\alpha\neq 0$, we have that $\overline{\alpha}=t$, and thus $\alpha\in\mathcal{O}_K$.

But then $\alpha\Omega \notin K$ and $I = \alpha\mathcal{O}_K \subseteq K$ at the same time; therefore $\alpha\Omega \notin I$. That is a contradiction with the fact that I is an $\mathcal{O}_L$-ideal.

If I is a fractional ideal, then there exists an element $r \in \mathcal{O}_K$ such that $rI \subseteq \mathcal{O}_L$. By the first part of the proof there exist $\alpha, \beta \in \mathcal{O}_L$, $\alpha, \beta \neq 0$, such that $rI = [\alpha, \beta]$; therefore, $\frac{\alpha}{r}, \frac{\beta}{r} \in L$, and $I = \left[\frac{\alpha}{r}, \frac{\beta}{r}\right]$. The rest of the proposition is clear. □

Consider an ideal $I = [\alpha, \beta]$ in $\mathcal{O}_L$. Then there exists a 2×2 matrix M consisting of elements of K such that

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = M \cdot \begin{pmatrix} 1 \\ \Omega \end{pmatrix}.$$

Then also

$$\begin{pmatrix} \overline{\alpha} & \alpha \\ \overline{\beta} & \beta \end{pmatrix} = M \cdot \begin{pmatrix} 1 & 1 \\ \overline{\Omega} & \Omega \end{pmatrix}, \tag{1.6}$$

and thus

$$\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}}. \tag{1.7}$$

The proof of the following lemma is just a direct computation.

Lemma 1.11. *Let $I = [\alpha, \beta]$ be an ideal and M the same matrix as above. Assume that $[p\alpha + r\beta, q\alpha + s\beta]$ is another $\mathcal{O}_K$-module basis of I, and $\widetilde{M}$ the matrix corresponding to this basis. Then $\det \widetilde{M} = (ps - qr) \det M$.*

Lemma 1.12. $\det M \in K$*, and if $\alpha, \beta \in \mathcal{O}_L$, then* $\det M \in \mathcal{O}_K$*.*

Proof. The first part is clear, since M is a matrix consisting of elements of K. To prove the second part, consider $\alpha, \beta \in \mathcal{O}_L$. Using Proposition 1.1, we can write $\alpha = a_1 + a_2\Omega$, $\beta = b_1 + b_2\Omega$ with $a_1, a_2, b_1, b_2 \in \mathcal{O}_K$. Hence, we can compute

$$\begin{aligned} \det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}} &= \frac{(a_1 + a_2\overline{\Omega})(b_1 + b_2\Omega) - (a_1 + a_2\Omega)(b_1 + b_2\overline{\Omega})}{\Omega - \overline{\Omega}} \\ &= \frac{(a_1b_2 - a_2b_1)(\Omega - \overline{\Omega})}{\Omega - \overline{\Omega}} = a_1b_2 - a_2b_1 \in \mathcal{O}_K. \end{aligned}$$ □

If I is a fractional $\mathcal{O}_L$-ideal, then $\mathcal{N}_{L/K}(I) = \big(\mathcal{N}_{L/K}(\alpha) \mid \alpha \in I\big)$ is the *relative norm of the ideal I*. Note that if I, J are two $\mathcal{O}_L$-ideals such that $I \subseteq J$, then $\mathcal{N}_{L/K}(I) \subseteq \mathcal{N}_{L/K}(J)$. Since $\mathcal{N}_{L/K}(I)$ is an $\mathcal{O}_K$-ideal and $h(K) = 1$ by the assumption, this ideal has to be principal. If $I = (\alpha)$ is a principal ideal, then it clearly holds that $\mathcal{N}_{L/K}((\alpha)) = \big(\mathcal{N}_{L/K}(\alpha)\big)$. Generally, the generator of the ideal $\mathcal{N}_{L/K}(I)$ can be written explicitly in terms of the $\mathcal{O}_K$-module basis of I, as the following lemma shows.

Lemma 1.13. *Let $I = [\alpha, \beta]$ be an ideal, and M the same matrix as above. Then $\det M$ generates the $\mathcal{O}_K$-ideal $\mathcal{N}_{L/K}(I)$.*

Proof. This is a well-known result holding for any finite Galois extension E/F such that $h(F) = 1$. The proof can be found e.g. in [Mann, 1958, Th. 1]. □

Let us now determine what will be later recognized as the inverse class of an ideal. We need to start with a technical lemma, which will also turn out to be useful later in the proof of Proposition 2.1, as the elements here will be exactly the coefficients of the quadratic form obtained from the ideal $[\alpha, \beta]$.

Lemma 1.14. *Let $[\alpha, \beta]$ be an ideal, and M the same matrix as above. Then*

$$\frac{\alpha\overline{\alpha}}{\det M}, \frac{\beta\overline{\beta}}{\det M}, \frac{\overline{\alpha}\beta + \alpha\overline{\beta}}{\det M}$$

are coprime elements of $\mathcal{O}_K$.

Proof. We start by proving that $\frac{\alpha\overline{\alpha}}{\det M}, \frac{\beta\overline{\beta}}{\det M}, \frac{\overline{\alpha}\beta+\alpha\overline{\beta}}{\det M}$ are elements of $\mathcal{O}_K$. First, assume that $\alpha, \beta \in \mathcal{O}_L$. Then $\det M \in \mathcal{O}_K$ by Lemma 1.12; hence we need to show that the elements $\alpha\overline{\alpha}, \beta\overline{\beta}, \overline{\alpha}\beta + \alpha\overline{\beta}$ are divisible by $\det M$ in $\mathcal{O}_K$. Since $\alpha \in [\alpha, \beta]$, there is $(\alpha) \subset [\alpha, \beta]$. It follows from Lemma 1.13 that

$$(\alpha\overline{\alpha}) = \Big(\mathcal{N}_{L/K}(\alpha)\Big) \subset \mathcal{N}_{L/K}([\alpha, \beta]) = (\det M),$$

and therefore $\alpha\overline{\alpha}$ is divisible by $\det M$ in $\mathcal{O}_K$. By the same argument, $\beta\overline{\beta}$ is divisible by $\det M$ in $\mathcal{O}_K$. Similarly, $(\alpha + \beta) \subset [\alpha, \beta]$ implies that $\mathcal{N}_{L/K}(\alpha + \beta)$ is divisible by $\det M$. Since $\mathcal{N}_{L/K}(\alpha + \beta) = \alpha\overline{\alpha} + \beta\overline{\beta} + \overline{\alpha}\beta + \alpha\overline{\beta}$, we see that $\overline{\alpha}\beta + \alpha\overline{\beta} = \mathcal{N}_{L/K}(\alpha + \beta) - \alpha\overline{\alpha} - \beta\overline{\beta}$ is divisible by $\det M$ in $\mathcal{O}_K$ as well.

In the general case, we can find $k \in \mathcal{O}_K$ such that $k\alpha, k\beta \in \mathcal{O}_L$. Hence, we may apply the first part of the proof to the ideal $[k\alpha, k\beta]$. Since the corresponding determinant is equal to $k^2 \det M$; the terms k^2 cancel out in the fractions.

Denote $a = \frac{\alpha\overline{\alpha}}{\det M}$, $b = \frac{\overline{\alpha}\beta+\alpha\overline{\beta}}{\det M}$, $c = \frac{\beta\overline{\beta}}{\det M}$. To prove that a, b, c are coprime, first note that $b^2 - 4ac = \left(\Omega - \overline{\Omega}\right)^2 = D_\Omega$. Therefore, if a, b, c were divisible by an element p in $\mathcal{O}_K \backslash \mathcal{U}_K$, then $\frac{D_\Omega}{p^2}$ would be a quadratic residue modulo 4, which is not possible, as D_Ω is fundamental by Lemma 1.4. □

Proposition 1.15. *Let $[\alpha, \beta]$ be an ideal. Then*

$$[\alpha, \beta] \cdot \left[\overline{\alpha}, -\overline{\beta}\right] = (\det M)$$

as $\mathcal{O}_L$-ideals.

Proof. Denote

$$I = [\alpha, \beta], \quad J = \left[\frac{\overline{\alpha}}{\det M}, \frac{-\overline{\beta}}{\det M}\right].$$

We will prove that $IJ = [1, \Omega]$, which is equivalent to the statement of the lemma. Note that

$$\mathcal{N}_{L/K}(J) = \frac{1}{(\det M)^2}\mathcal{N}_{L/K}\left([\overline{\alpha}, -\overline{\beta}]\right) = \left(\frac{1}{\det M}\right);$$

therefore, $\mathcal{N}_{L/K}(IJ) = (1)$ by the multiplicativity of the norm. Since we have also $\mathcal{N}_{L/K}([1, \Omega]) = (1)$, to prove that $[1, \Omega] = IJ$, we only need to show that $1, \Omega \in IJ$ (see [Mann, 1958, Cor. to Th. 1]). As IJ is an $\mathcal{O}_L$-ideal as well, it even suffices to prove that $1 \in IJ$.

Clearly,

$$IJ = \left[\frac{\alpha\overline{\alpha}}{\det M}, \frac{-\alpha\overline{\beta}}{\det M}, \frac{\overline{\alpha}\beta}{\det M}, \frac{-\beta\overline{\beta}}{\det M}\right]_{\mathcal{O}_K}.$$

By Lemma 1.14,

$$\gcd\left(\frac{\alpha\overline{\alpha}}{\det M}, \frac{\overline{\alpha}\beta+\alpha\overline{\beta}}{\det M}, \frac{\beta\overline{\beta}}{\det M}\right) = 1;$$

therefore, $1 \in IJ$. □

1.5 Relative oriented class group

In the traditional correspondence, there are binary quadratic forms on one side, and the class group $\mathcal{C}\ell_L = {}^{\mathcal{I}_L}/_{\mathcal{P}_L}$, or the narrow class group $\mathcal{C}\ell_L^+ = {}^{\mathcal{I}_L}/_{\mathcal{P}_L^+}$, on the other side (for details about class groups see Chapter 4). Since we are working with number fields of higher degrees, the situation is a bit more complicated. Inspired by Bhargava's definition of the class group, which consider the orientation of the bases of the ideals, we define the *relative oriented class group* with respect to the extension L/K. Compared to the rational numbers, our base field K has r real embeddings; therefore, instead of one sign, we consider r signs: one for every real embedding. Later, in Section 2.5, we will see that these signs are closely connected to the positive definiteness of the corresponding quadratic forms.

Definition 1.16. *For $a \in K$ write $\underline{\operatorname{sgn}}(a) = (\operatorname{sgn}(\sigma_1(a)), \ldots, \operatorname{sgn}(\sigma_r(a)))$, and set*

$$\begin{aligned}\mathcal{I}^o_{L/K} &= \{(I;\varepsilon_1,\ldots,\varepsilon_r) \mid I \text{ a fractional } \mathcal{O}_L\text{-ideal}, \varepsilon_i \in \{\pm 1\}, i = 1,\ldots,r\},\\ \mathcal{P}^o_{L/K} &= \left\{\left((\gamma);\underline{\operatorname{sgn}}\left(\mathcal{N}_{L/K}(\gamma)\right)\right) \mid \gamma \in L\right\};\end{aligned}$$

here, $(I;\varepsilon_1,\ldots,\varepsilon_r)$ is called the oriented ideal. *Then the* relative oriented class group *of the field extension L/K is defined as*

$$\mathcal{C}\ell^o_{L/K} = {}^{\mathcal{I}^o_{L/K}}\Big/_{\mathcal{P}^o_{L/K}}.$$

The multiplication on $\mathcal{I}^o_{L/K}$ is defined componentwise as

$$(I;\varepsilon_1,\ldots,\varepsilon_r)\cdot(J;\delta_1,\ldots,\delta_r) = (IJ;\varepsilon_1\delta_1,\ldots,\varepsilon_r\delta_r);$$

thus, $\mathcal{I}^o_{L/K}$ is clearly an abelian group, and $\mathcal{P}^o_{L/K}$ is its subgroup. Therefore, the group $\mathcal{C}\ell^o_{L/K}$ is well-defined.

If two oriented ideals $(I;\varepsilon_1,\ldots,\varepsilon_r)$ and $(J;\delta_1,\ldots,\delta_r)$ lie in the same class of $\mathcal{C}\ell^o_{L/K}$, we say that they are *equivalent* and write $(I;\varepsilon_1,\ldots,\varepsilon_r) \sim (J;\delta_1,\ldots,\delta_r)$.

Let us first compare the relative oriented class group $\mathcal{C}\ell^o_{L/K}$ with the class group $\mathcal{C}\ell_L$ of the number field L. In the following, by $\mathcal{O}_L$ is meant the principal $\mathcal{O}_L$-ideal generated by a unit (hence the identity element in the group $\mathcal{C}\ell_L$), and by $\{\mathcal{O}_L\}$ the one-element group; $\langle\pm 1\rangle^r$ stands for r copies of the (unique) multiplicative group on 2 elements.

Proposition 1.17. *Denote $H = \left\{\underline{\operatorname{sgn}}\left(\mathcal{N}_{L/K}(\mu)\right) \mid \mu \in \mathcal{U}_L\right\}$. Then*

$$\mathcal{C}\ell_L \simeq {}^{\mathcal{C}\ell^o_{L/K}}\Big/_{\left(\{\mathcal{O}_L\}\times {}^{\langle\pm1\rangle^r}/_H\right)}.$$

Proof. Define maps f and g:

$$\begin{array}{cccc} f: & \{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r & \longrightarrow & \mathcal{I}^o_{L/K} \\ & (\mathcal{O}_L; \underline{\varepsilon}) & \longmapsto & (\mathcal{O}_L; \underline{\varepsilon}) \end{array}$$

$$\begin{array}{cccc} g: & \mathcal{I}^o_{L/K} & \longrightarrow & \mathcal{I}_L \\ & (I; \underline{\varepsilon}) & \longmapsto & I \end{array}$$

Then f is injective, g surjective, and $\operatorname{Ker} g = \{(\mathcal{O}_L; \underline{\varepsilon}) \mid \underline{\varepsilon} \in \langle \pm 1 \rangle^r\} = \operatorname{Im} f$. Consider restrictions f' and g' of these two maps:

$$\begin{array}{cccc} f': & \{\mathcal{O}_L\} \times H & \longrightarrow & \mathcal{P}^o_{L/K} \\ & \Big(\mathcal{O}_L; \underline{\operatorname{sgn}}\left(\mathcal{N}_{L/K}(\mu)\right)\Big) & \longmapsto & \Big((\mu); \underline{\operatorname{sgn}}\left(\mathcal{N}_{L/K}(\mu)\right)\Big) \\ g': & \mathcal{P}^o_{L/K} & \longrightarrow & \mathcal{P}_L \\ & \Big((\gamma); \underline{\operatorname{sgn}}\left(\mathcal{N}_{L/K}(\gamma)\right)\Big) & \longmapsto & (\gamma) \end{array}$$

Note that f' is indeed a restricton of f, as $(\mu) = \mathcal{O}_L$ for any $\mu \in \mathcal{U}_L$. Again, f' is injective, g' is surjective, and $\operatorname{Ker} g' = \Big\{\Big((\gamma); \underline{\operatorname{sgn}}\left(\mathcal{N}_{L/K}(\gamma)\right)\Big) \mid \gamma \in \mathcal{U}_L\Big\} = \operatorname{Im} f'$. Hence, we obtain the following commutative diagram:

$$\begin{tikzcd} 1 \arrow[r] & \{\mathcal{O}_L\} \times \langle \pm 1 \rangle^r \arrow[r, "f"] & \mathcal{I}^o_{L/K} \arrow[r, "g"] & \mathcal{I}_L \arrow[r] & 1 \\ 1 \arrow[r] & \{\mathcal{O}_L\} \times H \arrow[r, "f'"] \arrow[u, hook, "i_1"] & \mathcal{P}^o_{L/K} \arrow[r, "g'"] \arrow[u, hook, "i_2"] & \mathcal{P}_L \arrow[r] \arrow[u, hook, "i_3"] & 1 \end{tikzcd}$$

Note that $\operatorname{Coker} i_1 = \{\mathcal{O}_L\} \times {}^{\langle \pm 1 \rangle^r}/_{H}$, $\operatorname{Coker} i_2 = \mathcal{C}\ell^o_{L/K}$, $\operatorname{Coker} i_3 = \mathcal{C}\ell_{L/K}$, and $\operatorname{Ker} i_3 = 1$. Hence, by snake lemma, there is a short exact sequence:

$$1 \longrightarrow \{\mathcal{O}_L\} \times {}^{\langle \pm 1 \rangle^r}/_{H} \longrightarrow \mathcal{C}\ell^o_{L/K} \longrightarrow \mathcal{C}\ell_L \longrightarrow 1$$

This sequence gives us the required isomorphism

$$\mathcal{C}\ell_L \simeq {}^{\mathcal{C}\ell^o_{L/K}} \Big/ {}_{\{\mathcal{O}_L\} \times {}^{\langle \pm 1 \rangle^r}/_{H}} \, . \qquad \square$$

Remark. The relative oriented class group could be defined for any finite Galois extension E/F such that $h^+(F) = 1$; Proposition 1.17 would remain true without any modifications.

We know that for every $\mathcal{O}_L$-ideal I, we can find $\alpha, \beta \in L$ such that $I = [\alpha, \beta]$. We would like to define orientation of such an ideal by using its basis. To do that, consider once again the matrix M satisfying

$$\begin{pmatrix} \overline{\alpha} & \alpha \\ \overline{\beta} & \beta \end{pmatrix} = M \cdot \begin{pmatrix} 1 & 1 \\ \overline{\Omega} & \Omega \end{pmatrix},$$

and take the determinant of this matrix, i.e. $\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}}$. Then define the orientation of the ideal $[\alpha, \beta]$ as $\underline{\operatorname{sgn}}(\det M)$: we obtain the oriented ideal

$$\Big([\alpha, \beta]; \underline{\operatorname{sgn}}(\det M)\Big) = ([\alpha, \beta]; \operatorname{sgn}(\sigma_1(\det M)), \dots, \operatorname{sgn}(\sigma_r(\det M))) \, .$$

The question is if we are able to find a well-oriented basis for any oriented ideal $(I; \varepsilon_1, \dots, \varepsilon_r)$.

Lemma 1.18. *Let $(I; \varepsilon_1, \ldots, \varepsilon_r)$ be an oriented ideal. Then there exists a basis $[\alpha, \beta]$ of I such that $\underline{\operatorname{sgn}}\,(\det M) = (\varepsilon_1, \ldots, \varepsilon_r)$, where $\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}}$.*

Proof. Consider any basis $[\alpha, \beta]$ of the ideal I, and multiply α by a unit $u \in \mathcal{U}_K$ with the appropriate $\underline{\operatorname{sgn}}\,(u)$; such a unit exists by the assumption that the narrow class number of K is one. □

If $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$ and $\big([\alpha', \beta']\,; \underline{\operatorname{sgn}}\,(\det M')\big)$ are two oriented ideals, then their multiple is the ideal $[\alpha, \beta] \cdot [\alpha', \beta']$ with the orientation given by $\underline{\operatorname{sgn}}\,(\det M \cdot \det M')$. The existence of a basis of the ideal $[\alpha, \beta] \cdot [\alpha', \beta']$ with such an orientation is guaranteed by the previous lemma. Note that here we need the condition $h^+(K) = 1$; otherwise, there may not exist any basis of the multiple of two ideals with the required orientation.

The orientation of a principal ideal is given directly by the definition as

$$\big((\gamma)\,; \underline{\operatorname{sgn}}\,(\gamma\overline{\gamma})\big) = ((\gamma); \operatorname{sgn}(\sigma_1(\gamma\overline{\gamma})), \ldots, \operatorname{sgn}(\sigma_r(\gamma\overline{\gamma}))) .$$

Note that if

$$\begin{pmatrix} \overline{\gamma\alpha} & \gamma\alpha \\ \overline{\gamma\beta} & \gamma\beta \end{pmatrix} = \widetilde{M} \cdot \begin{pmatrix} 1 & 1 \\ \overline{\Omega} & \Omega \end{pmatrix},$$

then $\det \widetilde{M} = \gamma\overline{\gamma} \det M$, and therefore,

$$\big((\gamma)\,; \underline{\operatorname{sgn}}\,(\gamma\overline{\gamma})\big) \cdot \big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big) = \Big([\gamma\alpha, \gamma\beta]\,; \underline{\operatorname{sgn}}\,\Big(\det \widetilde{M}\Big)\Big) .$$

Lemma 1.19. *The identity element of the group $\mathcal{C}\ell^{o}_{L/K}$ is $([1, \Omega]; +1, \ldots, +1)$, and the inverse to $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$ is $\Big(\big[\overline{\alpha}, -\overline{\beta}\big]\,; \underline{\operatorname{sgn}}\,(\det M)\Big)$ (taking all of the oriented ideals as representatives of classes in $\mathcal{C}\ell^{o}_{L/K}$).*

Proof. The orientation of the ideal $[1, \Omega]$ is $(+1, \ldots, +1)$, because M is in this case the unit matrix. Hence, the oriented ideal $([1, \Omega]; +1, \ldots, +1)$ is a representative of the identity element of the group $\mathcal{C}\ell^{o}_{L/K}$.

We know from Proposition 1.15 that $[\alpha, \beta] \cdot \big[\overline{\alpha}, -\overline{\beta}\big] = (\det M)$; since the orientation of the product $[\alpha, \beta] \cdot \big[\overline{\alpha}, -\overline{\beta}\big]$ is $\underline{\operatorname{sgn}}\,((\det M)^2) = \underline{\operatorname{sgn}}\,\Big(\det M \overline{\det M}\Big)$, we even have that

$$\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big) \cdot \Big(\big[\overline{\alpha}, -\overline{\beta}\big]\,; \underline{\operatorname{sgn}}\,(\det M)\Big) = \Big((\det M)\,; \underline{\operatorname{sgn}}\,\Big(\det M \overline{\det M}\Big)\Big) ,$$

which is an element of $\mathcal{P}^{o}_{L/K}$. Thus, the oriented ideals $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$ and $\Big(\big[\overline{\alpha}, -\overline{\beta}\big]\,; \underline{\operatorname{sgn}}\,(\det M)\Big)$ represent inverse classes in the group $\mathcal{C}\ell^{o}_{L/K}$. □

The following lemma states an easy but very useful observation; the proof is immediate.

Lemma 1.20. *Two oriented ideals $(I; \varepsilon_1, \ldots, \varepsilon_r)$ and $(J; \delta_1, \ldots, \delta_r)$ are equivalent if and only if there exists $\gamma \in L$ such that $\gamma I = J$ and $\underline{\operatorname{sgn}}\,(\gamma\overline{\gamma}) = \Big(\frac{\varepsilon_1}{\delta_1}, \ldots, \frac{\varepsilon_r}{\delta_r}\Big)$. Moreover, if $I = J$, then γ has to be a unit.*

2. Correspondence between ideals and quadratic forms

Finally, we are prepared to look at the first one of the correspondences, namely the one between the classes of quadratic forms and the relative oriented class group. The strategy is to define maps in both directions, prove that these maps are well-defined (on the equivalence classes) and that both of their compositions are identity maps. Afterward, we will take a closer look at the quadratic fields; we will see see that our new correspondence is actually a natural generalization of the traditional correspondence with $\mathbb{Q}$ as the base field. At the end of this chapter, we will restrict ourselves to quadratic forms of totally negative discriminant, and, in such a setting, we will compare the orientation of an ideal with positive definiteness of the associated quadratic form.

2.1 From ideals to quadratic forms

Let us define a map assigning a quadratic form to an oriented ideal.

$$\begin{array}{cccc}\Phi: & \mathcal{C}\ell^{o}_{L/K} & \longrightarrow & \mathcal{Q}_{\mathcal{D}} \\ & \Big([\alpha,\beta]\,;\underline{\operatorname{sgn}}\,(\det M)\Big) & \longmapsto & \frac{1}{\det M}\mathcal{N}_{L/K}\left(\alpha x-\beta y\right)=\frac{\alpha\overline{\alpha}x^2-(\overline{\alpha}\beta+\alpha\overline{\beta})xy+\beta\overline{\beta}y^2}{\det M}\end{array}$$

To be accurate, the map Φ goes between the classes of oriented ideals and classes of quadratic forms; we omit to write the classes to relax the notation. We have to check that this map is well-defined. First, let us see that the image of this map lies in $\mathcal{Q}_{\mathcal{D}}$.

Proposition 2.1. *Consider a representative* $\Big([\alpha,\beta]\,;\underline{\operatorname{sgn}}\,(\det M)\Big)$ *of a class in* $\mathcal{C}\ell^{o}_{L/K}$*, and denote by* $Q_{\alpha,\beta}$ *its image under the map* Φ*. Then* $Q_{\alpha,\beta}$ *is a representative of a class of* $\mathcal{Q}_{\mathcal{D}}$*.*

Proof. We have

$$Q_{\alpha,\beta}(x,y)=\frac{\alpha\overline{\alpha}x^2-(\overline{\alpha}\beta+\alpha\overline{\beta})xy+\beta\overline{\beta}y^2}{\det M}.$$

Lemma 1.14 ensures both that the coefficients of $Q_{\alpha,\beta}$ are elements of $\mathcal{O}_K$, and that this quadratic form is primitive. Thus, it only remains to verify the discriminant of $Q_{\alpha,\beta}$; one easily computes that

$$\operatorname{Disc}(Q_{\alpha,\beta})=\left(\Omega-\overline{\Omega}\right)^2,$$

which is an element of $\mathcal{D}$. □

To prove that the map Φ does not depend on the choice of the representative of the class in $\mathcal{C}\ell^{o}_{L/K}$, we start with two lemmas, which connect units from the quadratic extension L with the equivalence of quadratic forms.

Lemma 2.2. *Let* $\mu\in\mathcal{U}_L$*, and let* $Q(x,y)$ *be a quadratic form with* $\operatorname{Disc}(Q)\in\mathcal{D}$*. Then there exist some elements* $p_0,q_0,r_0,s_0\in\mathcal{O}_K$ *such that* $p_0s_0-q_0r_0=\mu\overline{\mu}$ *and* $Q(x,y)=\frac{1}{p_0s_0-q_0r_0}Q(p_0x+q_0y,r_0x+s_0y)$*.*

Proof. Let $Q(x,y) = ax^2 + bxy + cy^2$, and assume that $\operatorname{Disc}(Q) = D_\Omega$ (multiply Q by a suitable totally positive unit if needed). There exist $u, v \in \mathcal{O}_K$ such that $\mu = \frac{u}{2} + \frac{v}{2}\sqrt{D_\Omega}$; hence $\mu\overline{\mu} = \left(\frac{u}{2}\right)^2 + D_\Omega \left(\frac{v}{2}\right)^2$. From the condition $p_0s_0 - q_0r_0 = \mu\overline{\mu}$ and by comparing the coefficients of the quadratic forms $(p_0s_0 - q_0r_0)Q(x,y)$ and $Q(p_0x + q_0y, r_0x + s_0y)$, we get the following system of equations:

$$\begin{aligned} p_0s_0 - q_0r_0 &= \left(\tfrac{u}{2}\right)^2 + D_\Omega \left(\tfrac{v}{2}\right)^2, \\ (p_0s_0 - q_0r_0)a &= ap_0^2 + bp_0r_0 + cr_0^2, \\ (p_0s_0 - q_0r_0)b &= 2ap_0q_0 + b(p_0s_0 + q_0r_0) + 2cr_0s_0, \\ (p_0s_0 - q_0r_0)c &= aq_0^2 + bq_0s_0 + cs_0^2. \end{aligned} \tag{2.1}$$

One can check that

$$p_0 = \frac{u - bv}{2}, \qquad q_0 = -cv, \qquad r_0 = av, \qquad s_0 = \frac{u + bv}{2}$$

fulfill the system of equations (2.1). It remains to show that p_0, q_0, r_0, s_0 are elements of $\mathcal{O}_K$. This is obvious for q_0 and r_0; for p_0 and s_0, it follows from the computation

$$\mu\overline{\mu} = \left(\frac{u}{2}\right)^2 + D_\Omega \left(\frac{v}{2}\right)^2 = \left(\frac{u}{2}\right)^2 + (b^2 - 4ac)\left(\frac{v}{2}\right)^2 = \frac{u^2 - b^2v^2}{4} + acv^2,$$

and from the fact that both acv^2 and $\mu\overline{\mu}$ are elements of $\mathcal{O}_K$. □

Lemma 2.3. *Let Q be a primitive quadratic form, and $p, q, r, s \in \mathcal{O}_K$ be such that $ps - qr \in \mathcal{U}_K$. If there exists $\mu \in \mathcal{U}_L$ such that $\underline{\operatorname{sgn}}\,(\mu\overline{\mu}) = \underline{\operatorname{sgn}}\,(ps - qr)$, then $Q(x,y) \sim \frac{1}{ps-qr} Q(px - qy, -rx + sy)$.*

Proof. Use the elements p_0, q_0, r_0, s_0 from Lemma 2.2: $p_0s_0 - q_0r_0 = \mu\overline{\mu}$, and

$$Q(x,y) = \frac{1}{p_0s_0 - q_0r_0} Q(p_0x + q_0y, r_0x + s_0y).$$

Note that $\underline{\operatorname{sgn}}\,(p_0s_0 - q_0r_0) = \underline{\operatorname{sgn}}\,(\mu\overline{\mu}) = \underline{\operatorname{sgn}}\,(ps - qr)$, and thus $\frac{ps-qr}{p_0s_0-q_0r_0} \in \mathcal{U}_K^+$. We can find the equivalence between the quadratic forms $\frac{1}{ps-qr}Q(px-qy, -rx+sy)$ and $\frac{1}{p_0s_0-q_0r_0}Q(p_0x + q_0y, r_0x + s_0y)$; this equivalence is obtained by the change of coordinates given by the matrix

$$\begin{pmatrix} p_0 & q_0 \\ r_0 & s_0 \end{pmatrix} \begin{pmatrix} p & -q \\ -r & s \end{pmatrix}^{-1},$$

and by the multiplication by the totally positive unit $\frac{ps-qr}{p_0s_0-q_0r_0}$. Finally,

$$\frac{1}{ps - qr} Q(px - qy, -rx + sy) \sim \frac{1}{p_0s_0 - q_0r_0} Q(p_0x + q_0y, r_0x + s_0y) = Q(x,y). \ \square$$

Proposition 2.4. *The map Φ does not depend on the choice of the representative $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$.*

Proof. First, we would like to show that the definition of Φ is independent on the choice of the basis $[\alpha, \beta]$ of an ideal, i.e. that the quadratic form arising from the basis $[p\alpha + r\beta, q\alpha + s\beta]$, such that $p, q, r, s \in \mathcal{O}_K$, $ps - qr \in \mathcal{U}_K$, is equivalent to the one obtained from the basis $[\alpha, \beta]$; but this is not true in general, since the change of the basis may change the orientation as well. Thus, we have to add an assumption that the oriented ideals obtained from these two bases are equivalent in $\mathcal{C}\ell^o_{L/K}$: consider two oriented ideals

$$\mathfrak{I} = \Big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\Big), \qquad \widetilde{\mathfrak{I}} = \Big([p\alpha + r\beta, q\alpha + s\beta]\,; \underline{\operatorname{sgn}}\,\Big(\det \widetilde{M}\Big)\Big),$$

such that $p, q, r, s \in \mathcal{O}_K$, $ps - qr \in \mathcal{U}_K$, and assume $\mathfrak{I} \sim \widetilde{\mathfrak{I}}$. Denote $Q(x, y) = \Phi(\mathfrak{I})$, $\widetilde{Q}(x, y) = \Phi(\widetilde{\mathfrak{I}})$; we need to prove that $Q \sim \widetilde{Q}$. We have

$$\begin{aligned}\widetilde{Q}(x, y) &= \frac{\mathcal{N}_{L/K}\left((p\alpha + r\beta)x - (q\alpha + s\beta)y\right)}{\det \widetilde{M}} \\ &= \tfrac{\left(p^2\alpha\overline{\alpha} + pr(\overline{\alpha}\beta + \alpha\overline{\beta}) + r^2\beta\overline{\beta}\right)x^2 - \left(2pq\alpha\overline{\alpha} + (ps+qr)(\overline{\alpha}\beta + \alpha\overline{\beta}) + 2rs\beta\overline{\beta}\right)xy + \left(q^2\alpha\overline{\alpha} + qs(\overline{\alpha}\beta + \alpha\overline{\beta}) + s^2\beta\overline{\beta}\right)y^2}{(ps - qr)\det M} \\ &= \tfrac{\alpha\overline{\alpha}(px - qy)^2 - \left(\overline{\alpha}\beta + \alpha\overline{\beta}\right)(px - qy)(-rx + sy) + \beta\overline{\beta}(-rx + sy)^2}{(ps - qr)\det M} = \frac{1}{ps - qr} Q(px - qy, -rx + sy),\end{aligned}$$

where $\det \widetilde{M} = (ps - qr)\det M$ by Lemma 1.11. Since we have $\mathfrak{I} \sim \widetilde{\mathfrak{I}}$ and $[\alpha, \beta] = [p\alpha + r\beta, q\alpha + s\beta]$, there exists $\mu \in \mathcal{U}_L$ by Lemma 1.20, such that $\underline{\operatorname{sgn}}\,(\mu\overline{\mu}) = \underline{\operatorname{sgn}}\,(ps - qr)$. Thus, the quadratic forms $Q(x, y)$ and $\widetilde{Q}(x, y)$ are equivalent by Lemma 2.3.

Now, let us consider any two equivalent oriented ideals; the equivalence is given by multiplication by a principal oriented ideal $\Big((\gamma)\,; \underline{\operatorname{sgn}}\,(\gamma\overline{\gamma})\Big)$, i.e. we have a pair of oriented ideals $\Big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\Big)$ and $\Big([\gamma\alpha, \gamma\beta]; \underline{\operatorname{sgn}}\,(\gamma\overline{\gamma}\det M)\Big)$. The situation in this case is much easier, because the image of the oriented ideal $\Big([\gamma\alpha, \gamma\beta]; \underline{\operatorname{sgn}}\,(\gamma\overline{\gamma}\det M)\Big)$ under the map Φ is the quadratic form

$$\begin{aligned}\frac{1}{\gamma\overline{\gamma}\det M}\mathcal{N}_{L/K}\left(\gamma\alpha x - \gamma\beta y\right) &= \frac{\gamma\alpha\overline{\gamma\alpha}x^2 - (\overline{\gamma\alpha}\gamma\beta + \gamma\alpha\overline{\gamma\beta})xy + \gamma\beta\overline{\gamma\beta}y^2}{\gamma\overline{\gamma}\det M} \\ &= \frac{\alpha\overline{\alpha}x^2 - (\overline{\alpha}\beta + \alpha\overline{\beta})xy + \beta\overline{\beta}y^2}{\det M},\end{aligned}$$

which is identical to the quadratic form obtained from $\Big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\Big)$. □

2.2 From quadratic forms to ideals

To get an oriented ideal from a quadratic form, define a map

$$\begin{array}{cccc}\Psi : & \mathcal{Q}_{\mathcal{D}} & \longrightarrow & \mathcal{C}\ell^o_{L/K} \\ & Q(x, y) = ax^2 + bxy + cy^2 & \longmapsto & \left(\left[a, \frac{-b + \sqrt{\operatorname{Disc}(Q)}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right)\end{array}$$

By abuse of notation, we omit to write the classes; we have to show that this map is well-defined.

Proposition 2.5. *Let $Q(x,y) = ax^2 + bxy + cy^2$ be a representative of a class in $\mathcal{Q}_{\mathcal{D}}$. Then its image under the map Ψ is an element of $\mathcal{I}^o_{L/K}$.*

Proof. Set $D = \operatorname{Disc}(Q)$, and note that

$$\begin{aligned} a\Omega &= \frac{b-uw}{2u}\cdot a + \frac{a}{u}\cdot\frac{-b+\sqrt{D}}{2}, \\ \frac{-b+\sqrt{D}}{2}\Omega &= -\frac{c}{u}\cdot a - \frac{b+uw}{2u}\cdot\frac{-b+\sqrt{D}}{2}, \end{aligned}$$

where $D = u^2 D_\Omega$ for a totally positive unit $u \in \mathcal{U}_K^+$, and $\Omega = \frac{-w+\sqrt{D_\Omega}}{2}$ by (1.1). Hence, $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ is indeed an $\mathcal{O}_L$-ideal, and we only need to compute the orientation of the basis. Let M be such a matrix that

$$\begin{pmatrix} a & a \\ \frac{-b-\sqrt{D}}{2} & \frac{-b+\sqrt{D}}{2} \end{pmatrix} = M\cdot\begin{pmatrix} 1 & 1 \\ \overline{\Omega} & \Omega \end{pmatrix}.$$

We need to prove that $\underline{\operatorname{sgn}}\,(\det M) = \underline{\operatorname{sgn}}\,(a)$. There is

$$\det M = \frac{a\frac{-b+\sqrt{D}}{2} - a\frac{-b-\sqrt{D}}{2}}{\Omega-\overline{\Omega}} = \frac{a\sqrt{D}}{\Omega-\overline{\Omega}} = ua$$

with the same unit u as above, i.e. $\sqrt{D} = u\sqrt{D_\Omega} = u\left(\Omega - \overline{\Omega}\right)$. Since u is totally positive, we have $\underline{\operatorname{sgn}}\,(\det M) = \underline{\operatorname{sgn}}\,(a)$. □

Proposition 2.6. *The map Ψ does not depend on the choice of the representative $Q(x,y)$.*

Proof. Let $Q(x,y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant $D \in \mathcal{D}$, and $u \in \mathcal{U}_K^+$. Then

$$\begin{aligned} \Psi(uQ(x,y)) &= \left(\left[ua, \frac{-ub+\sqrt{u^2D}}{2}\right]; \underline{\operatorname{sgn}}\,(ua)\right) \\ &= \big((u)\,; \underline{\operatorname{sgn}}\,(u\overline{u})\big)\cdot\left(\left[a, \frac{-b+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right), \end{aligned}$$

because both u and $u\overline{u}$ are totally positive. Hence,

$$\Psi(uQ(x,y)) \sim \left(\left[a, \frac{-b+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right) = \Psi(Q(x,y)).$$

Now, let $p, q, r, s \in \mathcal{O}_K$ be such that $ps - qr \in \mathcal{U}_K^+$, and consider the quadratic form $\widetilde{Q}(x,y) = Q(px+qy, rx+sy) = \widetilde{a}x^2 + \widetilde{b}xy + \widetilde{c}y^2$. We have

$$\begin{aligned} \Psi(Q(x,y)) &= \left(\left[a, \frac{-b+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right), \\ \Psi(\widetilde{Q}(x,y)) &= \left(\left[\widetilde{a}, \frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2}\right]; \underline{\operatorname{sgn}}\,(\widetilde{a})\right); \end{aligned}$$

we need to show that these two oriented ideals are equivalent.

Let us first examine only how to come from the basis $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ to the basis $\left[\widetilde{a}, \frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2}\right]$; we will deal with the orientations afterwards.

$$
\begin{aligned}
&\left[\widetilde{a}, \frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2}\right] \xrightarrow{\cdot \frac{1}{\widetilde{a}}} \left[1, \frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}\right] \xrightarrow{\left(\begin{smallmatrix} q & p \\ s & r \end{smallmatrix}\right)} \left[p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + q, r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + s\right] \\
&\xrightarrow{\cdot\left(r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s\right)^{-1}} \left[\frac{p\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+q}{r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}}+s}, 1\right] \overset{\text{(Lemma 1.9)}}{=} \left[\frac{-b+\sqrt{D}}{2a}, 1\right] \\
&\xrightarrow{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)} \left[1, \frac{-b+\sqrt{D}}{2a}\right] \xrightarrow{\cdot a} \left[a, \frac{-b+\sqrt{D}}{2}\right]
\end{aligned}
$$

Recall that the multiplication of the basis by an element γ change the orientation by $\underline{\operatorname{sgn}}\,(\gamma\overline{\gamma})$, and the action by a matrix M on the basis change the orientation by $\underline{\operatorname{sgn}}\,(\det M)$. Since $a \in K$, there is $a\overline{a} = a^2$, which is totally positive. Thus, the multiplication by a does not change the orientation; the same holds for $\frac{1}{\widetilde{a}} \in K$. Also, both $-(ps-qr)$ and -1 are totally negative, and hence both the transformations by the matrices $\left(\begin{smallmatrix} q & p \\ s & r \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ change the orientation to the opposite one; together they does not affect the orientation. Therefore, the only impact might have the multiplication by $\left(r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + s\right)^{-1}$:

$$
\begin{aligned}
&\underline{\operatorname{sgn}} \left(\left(r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + s \right)^{-1} \overline{\left(r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + s \right)^{-1}} \right) \\
&= \underline{\operatorname{sgn}} \left(\left(r\frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2\widetilde{a}} + s \right) \left(r\frac{-\widetilde{b}-\sqrt{\widetilde{D}}}{2\widetilde{a}} + s \right) \right) \\
&= \underline{\operatorname{sgn}} \left(\left(-r\widetilde{b} + 2s\widetilde{a}\right)^2 - r^2\widetilde{D} \right) = \underline{\operatorname{sgn}} \left(r^2\widetilde{b}^2 - 4rs\widetilde{a}\widetilde{b} + 4s^2\widetilde{a}^2 - r^2(\widetilde{b}^2 - 4\widetilde{a}\widetilde{c}) \right) \\
&= \underline{\operatorname{sgn}} \left(4\widetilde{a}(\widetilde{a}s^2 - \widetilde{b}rs + \widetilde{c}r^2) \right) \overset{(1.5)}{=} \underline{\operatorname{sgn}} \left(4\widetilde{a}(ps-qr)^2 a \right) = \underline{\operatorname{sgn}}\,(\widetilde{a}a)
\end{aligned}
$$

(we used the facts that $4\widetilde{a}^2$ and $4(ps-qr)^2$ are totally positive). All the mentioned transformations together changed the orientation of the ideal from $\underline{\operatorname{sgn}}\,(\widetilde{a})$ to $\underline{\operatorname{sgn}}\,(\widetilde{a}) \cdot \underline{\operatorname{sgn}}\,(\widetilde{a}a) = \underline{\operatorname{sgn}}\,(\widetilde{a}^2 a) = \underline{\operatorname{sgn}}\,(a)$, and that is exactly the desired orientation. Hence, the oriented ideals $\left(\left[a, \frac{-b+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right)$ and $\left(\left[\widetilde{a}, \frac{-\widetilde{b}+\sqrt{\widetilde{D}}}{2}\right]; \underline{\operatorname{sgn}}\,(\widetilde{a})\right)$ are equivalent. □

2.3 Proof of the bijection

We are ready to prove that the maps Φ and Ψ defined in the two previous subsections are mutually inverse bijections.

Theorem 2.7. *Let K be a number field of narrow class number one. Let D be a fundamental element of $\mathcal{O}_K$. Set $L = K\left(\sqrt{D}\right)$, and $\mathcal{D} = \left\{u^2 D \mid u \in \mathcal{U}_K^+\right\}$. We have a bijection*

$$\begin{array}{ccc}
\mathcal{Q}_{\mathcal{D}} & \overset{1:1}{\longleftrightarrow} & \mathcal{C}\ell^o_{L/K} \\[1ex]
Q(x,y) = ax^2 + bxy + cy^2 & \overset{\Psi}{\longmapsto} & \left(\left[a, \frac{-b+\sqrt{\operatorname{Disc}(Q)}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right) \\[1ex]
\dfrac{\alpha\overline{\alpha}x^2 - (\overline{\alpha}\beta + \alpha\overline{\beta})xy + \beta\overline{\beta}y^2}{\frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}}} & \overset{\Phi}{\longleftarrow\!\shortmid} & \left([\alpha, \beta]\,; \underline{\operatorname{sgn}}\left(\frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}}\right)\right)
\end{array}$$

Proof. Let Ω be such that $\mathcal{O}_L = [1, \Omega]$. By Lemma 1.5, there is a unit $u \in \mathcal{U}_K$ (not necessarily totally positive) such that $D = u^2 D_\Omega$; then we have $\mathcal{O}_L = [1, u\Omega]$ and $u^2 D_\Omega = (u\Omega - \overline{u\Omega})^2$. If we begin with the canonical basis $[1, u\Omega]$ of $\mathcal{O}_L$ instead of $[1, \Omega]$, we get the same results for D in the place of D_Ω. Therefore, without loss of generality, we may assume that $D = D_\Omega$. Note that under this assumption

$$\frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}} = \det M.$$

Let

$$\mathfrak{I} = \left([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\right)$$

be a representative of a class in $\mathcal{C}\ell^o_{L/K}$, and

$$Q_{\alpha,\beta}(x,y) = \frac{\alpha\overline{\alpha}x^2 - (\overline{\alpha}\beta + \alpha\overline{\beta})xy + \beta\overline{\beta}y^2}{\det M}$$

its image under the map Φ. If we use the map Ψ now, we obtain the oriented ideal

$$\mathfrak{I}' = \left(\left[\frac{\alpha\overline{\alpha}}{\det M}, \frac{\overline{\alpha}\beta + \alpha\overline{\beta}}{2\det M} + \frac{\Omega - \overline{\Omega}}{2}\right]; \underline{\operatorname{sgn}}\left(\frac{\alpha\overline{\alpha}}{\det M}\right)\right).$$

Since $\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}}$, there is $\frac{\overline{\alpha}\beta + \alpha\overline{\beta}}{2\det M} + \frac{\Omega - \overline{\Omega}}{2} = \frac{(\overline{\alpha}\beta + \alpha\overline{\beta}) + (\overline{\alpha}\beta - \alpha\overline{\beta})}{2\det M} = \frac{\overline{\alpha}\beta}{\det M}$. Thus,

$$\mathfrak{I}' = \left(\left[\frac{\alpha\overline{\alpha}}{\det M}, \frac{\overline{\alpha}\beta}{\det M}\right]; \underline{\operatorname{sgn}}\left(\frac{\alpha\overline{\alpha}}{\det M}\right)\right).$$

If we multiply $\mathfrak{I}'$ by the principal oriented ideal $\left(\left(\frac{\det M}{\overline{\alpha}}\right); \underline{\operatorname{sgn}}\left(\frac{\det M}{\overline{\alpha}}\frac{\det M}{\alpha}\right)\right)$, we get exactly the ideal $\mathfrak{I}$. Therefore, $\mathfrak{I} \sim \mathfrak{I}' = \Psi\Phi(\mathfrak{I})$, and $\Psi\Phi = \mathrm{id}_{\mathcal{C}\ell^o_{L/K}}$.

On the other hand, consider

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

a representative of a class in $\mathcal{Q}_{\mathcal{D}}$. Its image under the map Ψ is the oriented ideal

$$\left(\left[a, \frac{-b + \sqrt{\operatorname{Disc}(Q)}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right).$$

Using the map Φ, we get a quadratic form

$$Q'(x,y) = \frac{a^2x^2 + abxy + \frac{b^2 - \operatorname{Disc}(Q)}{4}y^2}{\det M},$$

where

$$\begin{pmatrix} a & a \\ \frac{-b-\sqrt{\operatorname{Disc}(Q)}}{2} & \frac{-b+\sqrt{\operatorname{Disc}(Q)}}{2} \end{pmatrix} = M \cdot \begin{pmatrix} 1 & 1 \\ \Omega & \overline{\Omega} \end{pmatrix},$$

and $\det M = ua$ for a unit $u \in \mathcal{U}_K^+$. Hence,

$$Q'(x,y) = \frac{1}{u}(ax^2 + bxy + cy^2),$$

and $Q \sim Q' = \Phi\Psi(Q)$. Therefore, $\Phi\Psi = \mathrm{id}_{\mathcal{Q}_\mathcal{D}}$. □

Corollary 2.8. *$\mathcal{Q}_\mathcal{D}$ carries a group structure arising from the multiplication of ideals in $K\left(\sqrt{D}\right)$. The identity element of this group is represented by the quadratic form $x^2-(\Omega+\overline{\Omega})xy+\Omega\overline{\Omega}y^2$, and the inverse element to $ax^2+bxy+cy^2$ is the quadratic form $ax^2-bxy+cy^2$.*

Proof. The group structure of $\mathcal{Q}_\mathcal{D}$ is given by the bijection with $\mathcal{C}\ell^o_{L/K}$ from Theorem 2.7. The identity element is given as the image under the map Φ of the oriented ideal $([1,\Omega];+1,\dots,+1)$ (which represents the identity element in $\mathcal{C}\ell^o_{L/K}$); thus, the identity element is $x^2-(\Omega+\overline{\Omega})xy+\Omega\overline{\Omega}y^2$.

Consider the quadratic forms $ax^2+bxy+cy^2$ and $ax^2-bxy+cy^2$, and set $D=b^2-4ac$. The images of these two quadratic forms under the map Φ are the oriented ideals

$$\left(\left[a,\frac{-b+\sqrt{D}}{2}\right];\underline{\operatorname{sgn}}\,(a)\right) \text{ and } \left(\left[a,\frac{b+\sqrt{D}}{2}\right];\underline{\operatorname{sgn}}\,(a)\right),$$

which represent the mutually inverse classes of $\mathcal{C}\ell^o_{L/K}$ by Lemma 1.19. Hence, the quadratic forms $ax^2+bxy+cy^2$ and $ax^2-bxy+cy^2$ are inverse to each other. □

2.4 Quadratic fields

Let us look at the case of quadratic fields: assume $K=\mathbb{Q}$, and $L=\mathbb{Q}\left(\sqrt{D}\right)$. In this case, there exists only one real embedding of K, and that is the identity. Thus, Proposition 1.17 says that

$$\mathcal{C}\ell_L \simeq {\mathcal{C}\ell^o_{L/K}}\Big/_{\{\mathcal{O}_L\}\,\times\,\langle\pm1\rangle/H},$$

where $H=\left\{\operatorname{sgn}\mathcal{N}_{L/K}(\mu) \mid \mu\in\mathcal{U}_L\right\}$. To give more precise results, we need to distinguish three possible cases according to the sign of D and the existence of a negative unit:

1. If $D<0$, then there is $\mathcal{N}_{L/K}(\gamma)>0$ for every $\gamma\in L$; therefore, the oriented ideals $([\alpha,\beta];\operatorname{sgn}(\det M))$ and $([-\alpha,\beta];-\operatorname{sgn}(\det M))$ cannot be equivalent, and it is easy to see that $\mathcal{C}\ell^o_{L/K}\simeq\mathcal{C}\ell_L\times\langle\pm1\rangle$. Moreover, any pair of quadratic forms $ax^2+bxy+cy^2$ and $-ax^2+bxy-cy^2$ cannot be equivalent either; if one of them is positive definite, then the other one is negative definite. This explains the factor $\langle\pm1\rangle$ in the relative oriented class group, because in the usual correspondence only positive definite forms are considered whenever $D<0$.

2. Let $D > 0$, and assume that every unit has positive norm, i.e. for every $\mu \in \mathcal{U}_L$ there is $\mathcal{N}_{L/K}(\mu) = +1$. Consider the following surjective homomorphism:

$$\begin{array}{cccc} f: & \mathcal{I}^o_{L/K} & \longrightarrow & \mathcal{C}\ell^+_L \\ & (I;+1) & \longmapsto & I\mathcal{P}^+_L \\ & (I;-1) & \longmapsto & \sqrt{D}I\mathcal{P}^+_L \end{array}$$

Since $\operatorname{Ker} f = \mathcal{P}^o_{L/K}$, it follows that $\mathcal{C}\ell^o_{L/K} \simeq \mathcal{C}\ell^+_L$. Furthermore, it is well known that in this case is $\mathcal{C}\ell^+_L \simeq \mathcal{C}\ell_L \times \langle \pm 1 \rangle$; hence, we have that $\mathcal{C}\ell^o_{L/K} \simeq \mathcal{C}\ell_L \times \langle \pm 1 \rangle$.

3. Finally, assume that $D > 0$, and that there exists a unit of negative norm, i.e. $\mu_0 \in \mathcal{U}_L$ such that $\mathcal{N}_{L/K}(\mu_0) = -1$; then $H = \{(+1), (-1)\} = \langle \pm 1 \rangle$. Therefore, we get directly from Proposition 1.17 that $\mathcal{C}\ell^o_{L/K} \simeq \mathcal{C}\ell_L$. Since it is well known that in this case the groups $\mathcal{C}\ell_L$ and $\mathcal{C}\ell^+_L$ are isomorphic, we have as well that $\mathcal{C}\ell^o_{L/K} \simeq \mathcal{C}\ell^+_L$.

Let us summarize our observations into the following proposition:

Proposition 2.9. *Let $K = \mathbb{Q}$, and let $L = \mathbb{Q}\left(\sqrt{D_\Omega}\right)$ for a fundamental element $D_\Omega \in \mathbb{Z}$.*

1. *If $D_\Omega < 0$, then $\mathcal{C}\ell^o_{L/\mathbb{Q}} \simeq \mathcal{C}\ell_L \times \langle \pm 1 \rangle$.*

2. *If $D_\Omega > 0$ and $\mu\overline{\mu} = 1$ for every $\mu \in \mathcal{U}_L$, then $\mathcal{C}\ell^o_{L/\mathbb{Q}} \simeq \mathcal{C}\ell_L \times \langle \pm 1 \rangle \simeq \mathcal{C}\ell^+_L$.*

3. *If $D_\Omega > 0$ and there exists $\mu \in \mathcal{U}_L$ such that $\mu\overline{\mu} = -1$, then $\mathcal{C}\ell^o_{L/\mathbb{Q}} \simeq \mathcal{C}\ell_L \simeq \mathcal{C}\ell^+_L$.*

Remark. The proposition shows us that the relative oriented class group $\mathcal{C}\ell^o_{L/K}$ (and hence the correspondence between oriented ideals and quadratic forms) is a generalization of Bhargava's view to the classical correspondence; see [Bhargava, 2004, Sec. 3.2].

2.5 Totally positive definite quadratic forms

A very interesting and well-studied class of quadratic forms are the totally positive definite ones, which form a natural generalization of sums of squares. As such, they have been studied for example in the context of representations of totally positive integers, e.g. in Blomer and Kala, 2015], Chan et al. [1996], Earnest and Khosravani [1997], Kala [2016], Siegel [1945]. Of course, a binary quadratic form can never be universal; nevertheless, our results may prove to be useful also in the study of quadratic forms of higher ranks.

If D_Ω is totally negative (i.e. $\sigma(D_\Omega) < 0$ for every $\sigma \in R^K$; this fact will be denoted by $D_\Omega \prec 0$), then we can study the totally positive definite quadratic forms. Recall that a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ is *totally positive definite* if $\sigma(Q(x,y)) = \sigma(a)x^2 + \sigma(b)xy + \sigma(c)y^2$ is positive definite for every $\sigma \in R^K$. It is clear from the matrix notation that $Q(x,y) = ax^2 + bxy + cy^2$ is totally positive definite if and only if $a \succ 0$ (i.e. a is totally positive). Therefore, if $Q(x,y) = ax^2 + bxy + cy^2$ is a totally positive definite quadratic form, then its image under the map Ψ is the oriented ideal $\left(\left[a, \frac{-b+\sqrt{\mathrm{Disc}(Q)}}{2}\right]; +1, \ldots, +1\right)$.

One may ask if it is possible to describe the totally positive definite quadratic forms in terms of the oriented ideals. We start with the following lemma, which says that if $D_\Omega \prec 0$, then all ideals within one class of $\mathcal{C}\ell^o_{L/K}$ have the same orientation.

Lemma 2.10. *If $D_\Omega \prec 0$ and $(I; \varepsilon_1, \dots, \varepsilon_r) \sim (J; \delta_1, \dots, \delta_r)$, then $\varepsilon_i = \delta_i$ for all $i = 1, \dots, r$.*

Proof. By Lemma 1.20, if $(I; \varepsilon_1, \dots, \varepsilon_r) \sim (J; \delta_1, \dots, \delta_r)$, then there exists $\gamma \in L$ such that $J = \gamma I$ and $\delta_i = \operatorname{sgn}(\sigma_i(\gamma\overline{\gamma}))\varepsilon_i$ for all $i = 1, \dots, r$. Since $D_\Omega \prec 0$, there is $\gamma\overline{\gamma} \succ 0$ for every $\gamma \in L$. Therefore, $\operatorname{sgn}(\sigma_i(\gamma\overline{\gamma})) = +1$, and $\delta_i = \varepsilon_i$ for all $i = 1, \dots, r$. □

Proposition 2.11. *Let $D_\Omega \prec 0$, let $Q \in \mathcal{Q}_\mathcal{D}$, and let $i \in \{1, \dots, r\}$. Then the following are equivalent:*

(i) $\sigma_i(Q)$ is positive definite,

(ii) Q is the image under the map Φ of an oriented ideal $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$ such that $\sigma_i(\det M) > 0$,

(iii) Q is the image under the map Φ of an oriented ideal $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$ such that $\sigma_i\left(\Im\left(\frac{\beta}{\alpha}\right)\right) > 0$, where $\Im\left(c_1 + c_2\sqrt{D_\Omega}\right) = c_2$ for any $c_1, c_2 \in K$.

Proof. Let $Q(x, y) = ax^2 + bxy + cy^2$. Since $D_\Omega \prec 0$, the positive definiteness of $\sigma_i(Q)$ is given by the sign of $\sigma_i(a)$. First, we will prove that *(i)* ⇔ *(ii)*: Recall that

$$\Psi(Q) = \left(\left[a, \frac{-b + \sqrt{\operatorname{Disc}(Q)}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right).$$

If $\mathfrak{I} = \big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$ is an oriented ideal such that $\Phi(\mathfrak{I}) = Q(x, y)$, then $\Psi\Phi(\mathfrak{I}) = \Psi(Q)$. Hence, since $\mathfrak{I} \sim \Psi\Phi(\mathfrak{I})$, there is

$$\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big) \sim \left(\left[a, \frac{-b + \sqrt{\operatorname{Disc}(Q)}}{2}\right]; \underline{\operatorname{sgn}}\,(a)\right).$$

By the previous lemma, $\underline{\operatorname{sgn}}\,(\det M) = \underline{\operatorname{sgn}}\,(a)$. On the other hand, consider an oriented ideal $\mathfrak{I} = \big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$. Then the first coefficient of the quadratic form $\Phi(\mathfrak{I})$ is equal to $\frac{\alpha\overline{\alpha}}{\det M}$, and $\underline{\operatorname{sgn}}\left(\frac{\alpha\overline{\alpha}}{\det M}\right) = \underline{\operatorname{sgn}}\,(\det M)$, because $\alpha\overline{\alpha}$ is totally positive. Therefore, $\sigma_i(Q)$ is positive definite if and only if $\sigma_i(\det M) > 0$.

Let us prove *(ii)* ⇔ *(iii)*. Assume that Q is the image under the map Φ of an oriented ideal $\big([\alpha, \beta]\,; \underline{\operatorname{sgn}}\,(\det M)\big)$. Recall that $\Omega = \frac{-w+\sqrt{D_\Omega}}{2}$ by (1.1), and write $\alpha = a_1 + a_2\sqrt{D_\Omega}$, $\beta = b_1 + b_2\sqrt{D_\Omega}$ for some $a_1, a_2, b_1, b_2 \in K$. One can easily compute that

$$\det M = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\Omega - \overline{\Omega}} = 2(a_1b_2 - a_2b_1),$$

and

$$\frac{\beta}{\alpha} = \frac{a_1b_1 - a_2b_2D_\Omega + (a_1b_2 - a_2b_1)\sqrt{D_\Omega}}{a_1^2 - a_2^2D_\Omega}.$$

Thus,

$$\Im\left(\frac{\beta}{\alpha}\right) = \frac{a_1b_2 - a_2b_1}{a_1^2 - a_2^2D_\Omega},$$

where $a_1^2 - a_2^2 D_\Omega = a_1^2 + a_2^2 \left| D_\Omega \right|$ is totally positive. Hence,

$$\underline{\operatorname{sgn}} \left(\Im \left(\frac{\beta}{\alpha} \right) \right) = \underline{\operatorname{sgn}} \left(a_1 b_2 - a_2 b_1 \right) = \underline{\operatorname{sgn}} \left(\det M \right).$$

□

The result about totally positive definite quadratic forms follows immediately from Proposition 2.11.

Corollary 2.12. *Let $D_\Omega \prec 0$. A quadratic form is totally positive definite if and only if it is the image under the map Φ of an oriented ideal $\big([\alpha, \beta] ; \underline{\operatorname{sgn}} \left(\det M \right) \big)$ such that $\Im \left(\frac{\beta}{\alpha} \right)$ is totally positive.*

3. Composition of cubes

In the famous article Bhargava [2004], it is proved the existence of a group law on certain equivalence classes of cubes over $\mathbb{Z}$ by proving a bijection between these classes and *balanced* triples of oriented ideals in a quadratic field. Inspired by this article, we will extend the group law to equivalence classes of cubes over $\mathcal{O}_K$ for any number field K of narrow class number one.

We will start with introducing the cubes, and, in Section 3.2, we will use these cubes to describe composition of quadratic forms in a different way than in Chapter 2. Then we generalize Bhargava's balanced triples of ideals, and provide some equivalent ways how to look at them. Finally, we prove the desired bijection between equivalence classes of cubes and balanced triples of ideals.

3.1 Cubes

Bhargava introduced cubes of integers as elements of $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2$; if we denote by $\{v_1, v_2\}$ the standard $\mathbb{Z}$-basis of $\mathbb{Z}^2$, then the cube

$$\begin{tikzcd}
& a_{211} \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & a_{221} \arrow[dl, dash] \arrow[dd, dash] \\
a_{111} \arrow[rr, dash] \arrow[dd, dash] & & a_{121} \arrow[dd, dash] & \\
& a_{212} \arrow[rr, dash] \arrow[dl, dash] & & a_{222} \arrow[dl, dash] \\
a_{112} \arrow[rr, dash] & & a_{122} &
\end{tikzcd} \tag{3.1}$$

with $a_{ijk} \in \mathbb{Z}$ can be viewed as the expression

$$\sum_{i,j,k=1}^{2} a_{ijk} v_i \otimes v_j \otimes v_k,$$

which is an element of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Similarly, we can consider $\mathcal{O}_K^2 \otimes \mathcal{O}_K^2 \otimes \mathcal{O}_K^2$, this time taking the tensor product over the ring $\mathcal{O}_K$, and represent its elements as cubes with vertices $a_{ijk} \in \mathcal{O}_K$. We will often refer to such a cube as in (3.1) shortly by (a_{ijk}) tacitly assuming $a_{ijk} \in \mathcal{O}_K$ for all $i, j, k \in \{1, 2\}$.

Considering a cube

$$\begin{tikzcd}
& e \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[dd, dash] & \\
& g \arrow[rr, dash] \arrow[dl, dash] & & h \arrow[dl, dash] \\
c \arrow[rr, dash] & & d &
\end{tikzcd}, \tag{3.2}$$

it can be sliced in three different ways, which correspond to three pairs of 2×2

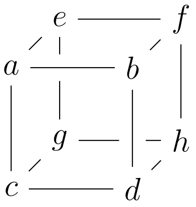
matrices:

$$\begin{aligned} R_1 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad S_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \\ R_2 &= \begin{pmatrix} a & e \\ c & g \end{pmatrix}, \quad S_2 = \begin{pmatrix} b & f \\ d & h \end{pmatrix}, \\ R_3 &= \begin{pmatrix} a & e \\ b & f \end{pmatrix}, \quad S_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}. \end{aligned}$$

To each of these pairs, a binary quadratic form $Q_i(x,y) = -\det(R_ix - S_iy)$ can be assigned:

$$\begin{aligned} Q_1(x,y) &= (bc-ad)x^2 + (ah-bg-cf+de)xy + (fg-eh)y^2 \\ Q_2(x,y) &= (ce-ag)x^2 + (ah+bg-cf-de)xy + (df-bh)y^2 \\ Q_3(x,y) &= (be-af)x^2 + (ah-bg+cf-de)xy + (dg-ch)y^2 \end{aligned} \tag{3.3}$$

Formally, we will look at the assignment of the triple of quadratic forms (3.3) to the cube (3.2) as a map $\widetilde{\Theta}$:



$$\xmapsto{\widetilde{\Theta}} \Big(-\det(R_1x - S_1y), -\det(R_2x - S_2y), -\det(R_3x - S_3y)\Big).$$

One can compute that all the quadratic forms in (3.3) have the same discriminant, namely

$$\begin{aligned} \mathrm{Disc}(Q_i) &= a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ &\quad - 2(abgh + acfh + aedh + bdeg + bfcg + cdef) + 4(adfg + bceh) \end{aligned}$$

for every $i = 1,2,3$. Hence, we can define the *discriminant* of a cube A as the discriminant of any of the three assigned quadratic forms; we denote this value by $\mathrm{Disc}(A)$. Furthermore, we say that a cube is *projective* if all the assigned quadratic forms are primitive.

Consider the group $\widetilde{\Gamma} = \mathcal{M}_2(\mathcal{O}_K) \times \mathcal{M}_2(\mathcal{O}_K) \times \mathcal{M}_2(\mathcal{O}_K)$, where $\mathcal{M}_2(\mathcal{O}_K)$ denotes the group of 2×2 matrices with entries from $\mathcal{O}_K$. This group has a natural action on cubes: if $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ is from the i-th copy of $\mathcal{M}_2(\mathcal{O}_K)$, $1 \le i \le 3$, then it acts on the cube (3.2) by replacing (R_i, S_i) by $(pR_i + qS_i, rR_i + sS_i)$. Note that the first copy acts on (R_2, S_2) by column operations, and on (R_3, S_3) by row operations. Hence, analogous to the fact that row and column operations on rectangular matrices commute, the three copies of $\mathcal{M}_2(\mathcal{O}_K)$ in $\widetilde{\Gamma}$ commute with each other. Therefore, we can always decompose the action by $T_1 \times T_2 \times T_3 \in \widetilde{\Gamma}$ into three subsequent actions:

$$T_1 \times T_2 \times T_3 = (\mathrm{id} \times \mathrm{id} \times T_3)(\mathrm{id} \times T_2 \times \mathrm{id})(T_1 \times \mathrm{id} \times \mathrm{id}). \tag{3.4}$$

Thus, we will usually restrict our attention to the action with only one nontrivial copy.

Consider the action by $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \times \mathrm{id} \times \mathrm{id}$ on the cube (3.2); the resulting cube is

$$\begin{tikzcd}
 & ra+se \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & rb+sf \arrow[dl, dash] \arrow[dd, dash] \\
pa+qe \arrow[rr, dash] \arrow[dd, dash] & & pb+qf \arrow[dd, dash] & \\
 & rc+sg \arrow[rr, dash] \arrow[dl, dash] & & rd+sh\,. \arrow[dl, dash] \\
pc+qg \arrow[rr, dash] & & pd+qh &
\end{tikzcd}$$

Let us investigate the quadratic forms assigned to this cube:

$$\begin{aligned}
Q_1'(x,y) &= -\det\left(\begin{pmatrix} pa+qe & pb+qf \\ pc+qg & pd+qh \end{pmatrix} x - \begin{pmatrix} ra+se & rb+sf \\ rc+sg & rd+sh \end{pmatrix} y\right) \\
&= -\det\left(\left(p\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix} + q\cdot\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) x - \left(r\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix} + s\cdot\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) y\right) \\
&= -\det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(px-ry) - \begin{pmatrix} e & f \\ g & h \end{pmatrix}(-qx+sy)\right) \\
&= Q_1(px-ry, -qx+sy), \\
Q_2'(x,y) &= -\det\left(\begin{pmatrix} pa+qe & ra+se \\ pc+qg & rc+sg \end{pmatrix} x - \begin{pmatrix} pb+qf & rb+sf \\ pd+qh & rd+sh \end{pmatrix} y\right) \\
&= -\det\left(\begin{pmatrix} a & e \\ c & g \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} x - \begin{pmatrix} b & f \\ d & h \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} y\right) \\
&= (ps-qr)\cdot Q_2(x,y), \\
Q_3'(x,y) &= -\det\left(\begin{pmatrix} pa+qe & ra+se \\ pb+qf & rb+sf \end{pmatrix} x - \begin{pmatrix} pc+qg & rc+sg \\ pd+qh & rd+sh \end{pmatrix} y\right) \\
&= -\det\left(\begin{pmatrix} a & e \\ b & f \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} x - \begin{pmatrix} c & g \\ d & h \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} y\right) \\
&= (ps-qr)\cdot Q_3(x,y).
\end{aligned}$$

We can see that

$$\mathrm{Disc}\left(\left(\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \times \mathrm{id} \times \mathrm{id}\right)(A)\right) = (ps-qr)^2\,\mathrm{Disc}(A).$$

Furthermore, for $t \in \mathcal{O}_K$, we understand by tA the cube A with all vertices multiplied by t. It is clear that $\mathrm{Disc}(tA) = t^4\,\mathrm{Disc}(A)$. We can summarize our observations into the following lemma.

Lemma 3.1. *Let A be a cube, $t \in \mathcal{O}_K$ and $T_1, T_2, T_3 \in \mathcal{M}_2(\mathcal{O}_K)$. Then*

$$\mathrm{Disc}\left(t\left(T_1 \times T_2 \times T_3\right)(A)\right) = t^4(\det T_1)^2(\det T_2)^2(\det T_3)^2\,\mathrm{Disc}(A).$$

Let us denote

$$\mathrm{GL}_2^+(\mathcal{O}_K) = \left\{T \in \mathcal{M}_2(\mathcal{O}_K) \;\middle|\; \det T \in \mathcal{U}_K^+\right\},$$

and consider the subgroup

$$\Gamma = \mathrm{GL}_2^+(\mathcal{O}_K) \times \mathrm{GL}_2^+(\mathcal{O}_K) \times \mathrm{GL}_2^+(\mathcal{O}_K)$$

of the group $\widetilde{\Gamma}$. Then Γ acts on cubes. It follows from the computations above that, for $u \in \mathcal{U}_K$ and $T_1 \times T_2 \times T_3 \in \Gamma$, cubes A and $u(T_1 \times T_2 \times T_3)(A)$ give rise to equivalent triples of quadratic forms. This justifies the following definition.

Definition 3.2. *We say that two cubes A and A' are* equivalent *(which will be denoted by $A \sim A'$) if there exist $u \in \mathcal{U}_K$ and $T_1 \times T_2 \times T_3 \in \Gamma$ such that $A' = u(T_1 \times T_2 \times T_3)(A)$.*

Recall that we denote by $\mathcal{D}$ the set of all possible discriminants, i.e. the set $\left\{u^2\left(\Omega - \overline{\Omega}\right)^2 \;\middle|\; u \in \mathcal{U}_K^+\right\}$. Note that if A is a cube such that $\mathrm{Disc}(A) \in \mathcal{D}$, then all cubes A' equivalent to A satisfy $\mathrm{Disc}(A') \in \mathcal{D}$. We will denote by $\mathcal{C}_\mathcal{D}$ the set of equivalence classes of projective cubes of discriminant in $\mathcal{D}$, i.e.

$$\mathcal{C}_\mathcal{D} = \left\{ A \in \mathcal{O}_K^2 \otimes \mathcal{O}_K^2 \otimes \mathcal{O}_K^2 \mid A \text{ is projective, } \mathrm{Disc}(A) \in \mathcal{D} \right\} \Big/ {\sim}.$$

Note that if A is a representative of an equivalence class in $\mathcal{C}_\mathcal{D}$, then the three quadratic forms assigned to the cube A are representatives of equivalence classes in $\mathcal{Q}_\mathcal{D}$; hence, the map $\widetilde{\Theta}$ restricts to a map $\Theta : \mathcal{C}_\mathcal{D} \longrightarrow \mathcal{Q}_\mathcal{D} \times \mathcal{Q}_\mathcal{D} \times \mathcal{Q}_\mathcal{D}$. To relax the notation, we will often omit to write the equivalence classes; by $A \in \mathcal{C}_\mathcal{D}$ we understand that the cube A which is a representative of the class $[A]$ in $\mathcal{C}_\mathcal{D}$, and $\Theta(A) = (Q_1, Q_2, Q_3)$ actually means $\Theta\big([A]\big) = \big([Q_1], [Q_2], [Q_3]\big)$.

A cube A is called *reduced* if

$$A = \begin{tikzcd}
& 0 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
1 \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[dd, dash] & \\
& g \arrow[rr, dash] \arrow[dl, dash] & & h \arrow[dl, dash] \\
0 \arrow[rr, dash] & & d &
\end{tikzcd}$$

for some $d, f, g, h \in \mathcal{O}_K$. The following lemma will help us to simplify some of the proofs.

Lemma 3.3. *Every projective cube is equivalent to a reduced cube.*

Proof. In the case of cubes over $\mathbb{Z}$, the proof with full details can be found in [Bouyer, Sec. 3.1]. The proof in the case over $\mathcal{O}_K$ is completely analogous, because $\mathcal{O}_K$ is a principal ideal domain. Here we only outline the rough idea. Consider a projective cube

$$\begin{tikzcd}
& e \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[dd, dash] & \\
& g \arrow[rr, dash] \arrow[dl, dash] & & h \arrow[dl, dash] \\
c \arrow[rr, dash] & & d &
\end{tikzcd} .$$

It follows from projectivity that $\gcd(a, b, c, d, e, f, g, h) = 1$; hence, we can find a cube equivalent to the original one with 1 in the place of a. This can be used to clear out the vertices b, c and e. □

We will point out one specific cube, and that is the cube

$$\begin{tikzcd}
 & 1 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & \Omega+\overline{\Omega} \arrow[dl, dash] \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[dd, dash] & \\
 & \Omega+\overline{\Omega} \arrow[rr, dash] \arrow[dl, dash] & & \left(\Omega+\overline{\Omega}\right)^2-\Omega\overline{\Omega} \arrow[dl, dash] \\
1 \arrow[rr, dash] & & \Omega+\overline{\Omega} &
\end{tikzcd} \quad ; \tag{3.5}$$

since the cube is triply symmetric, all the three quadratic forms assigned to this cube are equal to $Q_{\text{id}}(x,y) = x^2 - \left(\Omega + \overline{\Omega}\right) xy + \Omega\overline{\Omega}y^2$, the representative of the identity element in the group $\mathcal{Q}_{\mathcal{D}}$. Therefore, we will denote the cube in (3.5) by A_{id}.

3.2 Composition of binary quadratic forms

Bhargava establishes *Cube Law*, which says that composition of the three binary quadratic forms arising from one cube is the identity quadratic form. He shows that, in the case of projective cubes, this law is equivalent to Gauss composition by using Dirichlet's interpretation. In our case, the coefficients of the quadratic forms lie in $\mathcal{O}_K$ instead of $\mathbb{Z}$, and hence we are not allowed to use Dirichlet composition without reproving a generalized version. Instead of following this path, we will use the bijection between $\mathcal{Q}_{\mathcal{D}}$ and $\mathcal{C}\ell^o_{L/K}$ from Chapter 2, and show that the product of the three obtained ideal classes is a principal ideal class. Recall that the bijection is given by the maps Ψ and Φ:

$$\begin{tikzcd}
\mathcal{Q}_{\mathcal{D}} \arrow[r, leftrightarrow, "1:1"] & \mathcal{C}\ell^o_{L/K} \\
Q(x,y) = ax^2+bxy+cy^2 \arrow[r, mapsto, "\Psi"] & \left(\left[a, \frac{-b+\sqrt{\text{Disc}(Q)}}{2}\right]; \underline{\text{sgn}}\,(a)\right) \\
\frac{\alpha\overline{\alpha}x^2-(\overline{\alpha}\beta+\alpha\overline{\beta})xy+\beta\overline{\beta}y^2}{\det M} & \left([\alpha,\beta]\,; \underline{\text{sgn}}\,(\det M)\right) \arrow[l, mapsto, "\Phi"']
\end{tikzcd}$$

Lemma 3.4. *Let $A \in \mathcal{C}_{\mathcal{D}}$, and denote $\Theta(A) = (Q_1, Q_2, Q_3)$. Let $\mathfrak{J}_i$ be the image of Q_i under the map Ψ, $1 \le i \le 3$. Then there exists an element $\omega \in L$ such that $\mathfrak{J}_1\mathfrak{J}_2\mathfrak{J}_3 = \left((\omega)\,; \underline{\text{sgn}}\,(\omega\overline{\omega})\right)$.*

Proof. Using Lemma 3.3, we can assume that A is reduced. Hence, the quadratic forms arising from this cube are

$$\begin{aligned}
Q_1(x,y) &= -dx^2 + hxy + fgy^2, \\
Q_2(x,y) &= -gx^2 + hxy + dfy^2, \\
Q_3(x,y) &= -fx^2 + hxy + dgy^2,
\end{aligned} \tag{3.6}$$

all of them having discriminant $D = h^2 + 4dfg$. Their images under the map Ψ

are the oriented ideals

$$\begin{aligned} \mathfrak{J}_1 &= \left(\left[-d, \frac{-h+\sqrt{D}}{2} \right] ; \underline{\operatorname{sgn}} \left(-d \right) \right), \\ \mathfrak{J}_2 &= \left(\left[-g, \frac{-h+\sqrt{D}}{2} \right] ; \underline{\operatorname{sgn}} \left(-g \right) \right), \\ \mathfrak{J}_3 &= \left(\left[-f, \frac{-h+\sqrt{D}}{2} \right] ; \underline{\operatorname{sgn}} \left(-f \right) \right). \end{aligned} \tag{3.7}$$

Denote by J the product of the three (unoriented) ideals, and set $\omega = \frac{-h+\sqrt{D}}{2}$; by [Mann, 1958, Cor. to Th. 1], it is sufficient to prove that $\omega \in J$ and that $\mathcal{N}_{L/K}(\omega) = -dfg$.

First, we have

$$\mathcal{N}_{L/K}(\omega) = \frac{-h+\sqrt{D}}{2} \cdot \frac{-h-\sqrt{D}}{2} = \frac{h^2-D}{4} = -dfg,$$

where the last equality follows from $D = h^2 + 4dfg$. Furthermore,

$$\begin{aligned} J &= \left[-dfg, df\omega, dg\omega, fg\omega, -d\omega^2, -f\omega^2, -g\omega^2, \omega^3 \right]_{\mathcal{O}_K} \\ &= \left[-dfg, df\omega, dg\omega, fg\omega, dh\omega, fh\omega, gh\omega, h^2\omega \right]_{\mathcal{O}_K}, \end{aligned}$$

where we have used the relations

$$\omega^2 = dfg - h\omega, \qquad \omega^3 = -dfgh + (h^2 + dfg)\omega.$$

Set $G = \gcd(df, dg, fg, dh, fh, gh, h^2)$; we want to show that G is a unit, because then necessarily $\omega \in J$. It follows from primitiveness of the quadratic forms in (3.6) that $\gcd(d, f, g, h) = 1$; therefore, $G = \gcd(df, dg, fg, h)$. Let $p \in \mathcal{O}_K$ be a prime such that $p \mid G$. Since the quadratic form Q_1 is primitive and p divides both fg and h, we have that $p \nmid d$. But as $p \mid df$, it has to hold that $p \mid f$. Therefore, $p \mid \gcd(f, h, dg) = 1$, and hence both p and G are units. □

As a consequence of this lemma, we get a new description of composition of quadratic forms.

Theorem 3.5. *Let $A \in \mathcal{C}_{\mathcal{D}}$, and let Q_1, Q_2, Q_3 are the three quadratic forms arising from the cube A. Then their composition $Q_1Q_2Q_3$ is a representative of the identity element of the group $\mathcal{Q}_{\mathcal{D}}$.*

Proof. It follows from Lemma 3.4 that $\Psi(Q_1Q_2Q_3) = \Psi(Q_1) \cdot \Psi(Q_2) \cdot \Psi(Q_3)$ is a principal ideal. Therefore, by Theorem 2.7,

$$Q_1Q_2Q_3 \sim \Phi\Psi(Q_1Q_2Q_3) = x^2 - \left(\Omega + \overline{\Omega}\right) xy + \Omega\overline{\Omega} y^2,$$

i.e. $Q_1Q_2Q_3$ is a representative of the identity element of the group $\mathcal{Q}_{\mathcal{D}}$. □

3.3 Balanced ideals

Our main goal is to equip the set $\mathcal{C}_{\mathcal{D}}$ with a group law. In this section, we will focus on the other side of the seeking correspondence: balanced triples of ideals. We will show that there are essentially three equivalent views on such a triple.

Let $\mathfrak{I}_i = \Big(I_i; \underline{\operatorname{sgn}}\,(\det M_i)\Big)$, $1 \le i \le 3$, be oriented $\mathcal{O}_L$-ideals. We say that the triple $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ is *balanced* if $I_1 I_2 I_3 = \mathcal{O}_L$ and $\det M_1 \det M_2 \det M_3 \in \mathcal{U}_K^+$.

Let $(\mathfrak{I}_1', \mathfrak{I}_2', \mathfrak{I}_3')$ be another balanced triple, where $\mathfrak{I}_i' = \Big(I_i'; \underline{\operatorname{sgn}}\,(\det M_i')\Big)$ for $1 \le i \le 3$. The two balanced triples $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ and $(\mathfrak{I}_1', \mathfrak{I}_2', \mathfrak{I}_3')$ are *equivalent* if there exist $\kappa_i \in L$, $1 \le i \le 3$, such that $\mathfrak{I}_i' = \kappa_i \mathfrak{I}_i$. Note that then the equality

$$\mathcal{O}_L = I_1' I_2' I_3' = (\kappa_1 I_1)(\kappa_2 I_2)(\kappa_3 I_3) = (\kappa_1 \kappa_2 \kappa_3)\mathcal{O}_L$$

implies that $\kappa_1\kappa_2\kappa_3 \in \mathcal{U}_L$. Furthermore, since $\det M_i' = \mathcal{N}_{L/K}(\kappa_i) \det M_i$, we have $\mathcal{N}_{L/K}(\kappa_1\kappa_2\kappa_3) \in \mathcal{U}_K^+$. Also note that $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3) \sim \Big(\frac{1}{\kappa}\mathfrak{I}_1, \kappa\mathfrak{I}_2, \mathfrak{I}_3\Big)$ for any $\kappa \in L \backslash \{0\}$.

The equivalence class of balanced triples of oriented ideals will be denoted by $[(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)]$. The set of all equivalence classes of balanced triples of oriented ideals together with ideal multiplication forms a group; we will denote this group by $\mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big)$, i.e.

$$\mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big) = \Big\{ \Big[\,(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)\,\Big] \;\mid\; (\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3) \text{ a balanced triple of } \mathcal{O}_L\text{-ideals} \Big\}.$$

On the other hand, by $([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3])$ we will mean a triple of equivalence classes of oriented ideals such that $[\mathfrak{I}_1] \cdot [\mathfrak{I}_2] \cdot [\mathfrak{I}_3] = [(\mathcal{O}_L; +1, \dots, +1)]$; in other words, $\mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3$ is a principal oriented ideal for any choice of the representatives. Again, the set of all equivalence classes forms a group; we will denote this group by $\mathcal{T}rip\Big(\mathcal{C}\ell^o_{L/K}\Big)$, i.e.

$$\mathcal{T}rip\Big(\mathcal{C}\ell^o_{L/K}\Big) = \Big\{ \Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big) \;\Big|\; \exists\, \omega \in L \text{ s.t. } \mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3 = \Big((\omega)\,; \underline{\operatorname{sgn}}\,(\omega\overline{\omega})\Big) \Big\}.$$

We will show that these two groups, $\mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big)$ and $\mathcal{T}rip\Big(\mathcal{C}\ell^o_{L/K}\Big)$, are naturally isomorphic.

Proposition 3.6. *The maps*

$$\begin{tikzcd}
\mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big) \arrow[r, leftrightarrow] & \mathcal{T}rip\Big(\mathcal{C}\ell^o_{L/K}\Big) \\
\Big[\,(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)\,\Big] \arrow[r, mapsto, "\varphi_1"] & \Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big), \\
\Big[\,\Big(\frac{1}{\omega}\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3\Big)\,\Big] & \begin{array}{c}\Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big), \\ \mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3 = \Big((\omega)\,; \underline{\operatorname{sgn}}\,(\omega\overline{\omega})\Big)\end{array} \arrow[l, mapsto, "\varphi_2"']
\end{tikzcd}$$

are mutually inverse group homomorphisms.

Proof. If a triple $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ is balanced, then $\mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3 = (\mathcal{O}_L; +1, \dots, +1)$, which is a principal ideal. If $(\mathfrak{I}_1', \mathfrak{I}_2', \mathfrak{I}_3') \sim (\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$, then there exist $\kappa_i \in L$, $1 \le i \le 3$, such that $\mathfrak{I}_i' = \kappa_i\mathfrak{I}_i$; hence, $\mathfrak{I}_i' \sim \mathfrak{I}_i$, and $\Big([\mathfrak{I}_1'], [\mathfrak{I}_2'], [\mathfrak{I}_3']\Big) = \Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big)$. Thus, the map φ_1 is well-defined.

On the other hand, assume that $\mathfrak{I}_1$, $\mathfrak{I}_2$, $\mathfrak{I}_3$ are oriented ideals such that $\mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3 = \Big((\omega)\,;\underline{\operatorname{sgn}}\,(\omega\overline{\omega})\Big)$; then $\frac{1}{\omega}\mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3 = (\mathcal{O}_L; +1, \ldots, +1)$. The definition of φ_2 does not depend on the choice of the generator ω of the principal ideal, because any other generator has to be of the form $\mu\omega$ with $\mu \in \mathcal{U}_L$ and $\mathcal{N}_{L/K}(\mu) \in \mathcal{U}_K^+$, and hence $\Big[\Big(\frac{1}{\omega}\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3\Big)\Big] = \Big[\Big(\frac{1}{\mu\omega}\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3\Big)\Big]$. Moreover, if we take different representatives, $\Big([\lambda_1\mathfrak{I}_1], [\lambda_2\mathfrak{I}_2], [\lambda_3\mathfrak{I}_3]\Big) = \Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big)$, then

$$\varphi_2\Big(\Big([\lambda_1\mathfrak{I}_1], [\lambda_2\mathfrak{I}_2], [\lambda_3\mathfrak{I}_3]\Big)\Big) = \Big[\Big(\frac{1}{\lambda_1\lambda_2\lambda_3\omega}\lambda_1\mathfrak{I}_1, \lambda_2\mathfrak{I}_2, \lambda_3\mathfrak{I}_3\Big)\Big] = \Big[\Big(\frac{1}{\omega}\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3\Big)\Big].$$

Therefore, the map φ_2 does not depend on the choice of the representative, and so it is well-defined.

It is clear that both of the maps are group homomorphisms. We will show that they are mutually inverse. If $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ is a balanced triple of ideals, then its image under $\varphi_2\varphi_1$ is again $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$, because the product of the three oriented ideals is the principal ideal $(\mathcal{O}_L; +1, \ldots, +1) = ((1); +1, \ldots, +1)$; thus, $\varphi_2\varphi_1 = \mathrm{id}$. For the other direction, if $\Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big)$ is such that $\mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3 = \Big((\omega)\,;\underline{\operatorname{sgn}}\,(\omega\overline{\omega})\Big)$, then

$$\varphi_1\varphi_2\Big(\Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big)\Big) = \Big(\Big[\frac{1}{\omega}\mathfrak{I}_1\Big], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big) = \Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big);$$

therefore, $\varphi_1\varphi_2 = \mathrm{id}$. □

Proposition 3.7. *The group $\mathcal{T}rip\Big(\mathcal{C}\ell^o_{L/K}\Big)$ is naturally isomorphic to the group $\mathcal{C}\ell^o_{L/K} \times \mathcal{C}\ell^o_{L/K}$.*

Proof. The projection

$$\begin{array}{ccc} \mathcal{T}rip\Big(\mathcal{C}\ell^o_{L/K}\Big) & \longrightarrow & \mathcal{C}\ell^o_{L/K} \times \mathcal{C}\ell^o_{L/K} \\ \Big([\mathfrak{I}_1], [\mathfrak{I}_2], [\mathfrak{I}_3]\Big) & \longmapsto & \Big([\mathfrak{I}_1], [\mathfrak{I}_2]\Big) \end{array}$$

is a group isomorphism, because for given $[\mathfrak{I}_1]$ and $[\mathfrak{I}_2]$, the equivalence class $[\mathfrak{I}_3]$ is given uniquely as $[(\mathfrak{I}_1\mathfrak{I}_2)^{-1}]$. □

3.4 From ideals to cubes

Finally, we have prepared all the ingredients, and so we can start with the construction of the correspondence. As the first step, we will build (an equivalence class of) a cube from a balanced triple of ideals. In this section, we will closely follow the ideas of [Bhargava, 2004, Sec. 3.3].

For $\alpha \in L$ define

$$\tau(\alpha) = \frac{\alpha - \overline{\alpha}}{\Omega - \overline{\Omega}}.$$

If $\alpha = a + b\Omega$ for some $a, b \in K$, then the definition of τ says that $\tau(\alpha) = b$. It follows that τ is additive: for any $\alpha, \beta \in L$, it holds that

$$\tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta).$$

Furthermore, note that if $\Big([\alpha,\beta]\,;\underline{\operatorname{sgn}}\,(\det M)\Big)$ is an oriented ideal, then we can express $\det M$ as $\tau\,(\overline{\alpha}\beta)$. For an oriented ideal, we will often write $[\alpha,\beta]$ instead of $\Big([\alpha,\beta]\,;\underline{\operatorname{sgn}}\,(\det M)\Big)$, the orientation of the ideal implicitly given.

We would like to construct a cube from a given balanced triple of oriented ideals. Consider the following map:

$$\begin{array}{cccc} \Phi' : & \mathcal{B}al\Big(\mathcal{C}\ell^{o}_{L/K}\Big) & \longrightarrow & \mathcal{C}_{\mathcal{D}} \\ & \Big([\alpha_1,\alpha_2],[\beta_1,\beta_2],[\gamma_1,\gamma_2]\Big) & \longmapsto & \Big(\tau(\alpha_i\beta_j\gamma_k)\Big) \end{array} \tag{3.8}$$

(on both sides, the equivalence classes are omitted). The aim of this section is to prove that this map is well-defined. First, we will show how an action by $\widetilde{\Gamma}$ on bases of triples of ideals translates to an action on cubes.

Lemma 3.8. *If A is the image of $\Big([\alpha_1,\alpha_2],[\beta_1,\beta_2],[\gamma_1,\gamma_2]\Big)$ under the map Φ', then the image of*

$$\Big([p_1\alpha_1+r_1\alpha_2,q_1\alpha_1+s_1\alpha_2],[p_2\beta_1+r_2\beta_2,q_2\beta_1+s_2\beta_2],[p_3\gamma_1+r_3\gamma_3,q_3\gamma_1+s_3\gamma_2]\Big)$$

under the map Φ' is the cube

$$\left(\left(\begin{smallmatrix} p_1 & r_1 \\ q_1 & s_1 \end{smallmatrix}\right)\times\left(\begin{smallmatrix} p_2 & r_2 \\ q_2 & s_2 \end{smallmatrix}\right)\times\left(\begin{smallmatrix} p_3 & r_3 \\ q_3 & s_3 \end{smallmatrix}\right)\right)(A).$$

Proof. We will consider only the pair of balanced triples $\Big([\alpha_1,\alpha_2],[\beta_1,\beta_2],[\gamma_1,\gamma_2]\Big)$ and $\Big([p\alpha_1+r\alpha_2,q\alpha_1+s\alpha_2],[\beta_1,\beta_2],[\gamma_1,\gamma_2]\Big)$; the rest follows from (3.4) and symmetry. Denote $a_{ijk}=\tau(\alpha_i\beta_j\gamma_k)$. Then the image of the balanced triple $\Big([p\alpha_1+r\alpha_2,q\alpha_1+s\alpha_2],[\beta_1,\beta_2],[\gamma_1,\gamma_2]\Big)$ under the map Φ' is a cube (b_{ijk}), where

$$\begin{aligned} b_{1jk} &= \tau((p\alpha_1+r\alpha_2)\beta_j\gamma_k) = pa_{1jk}+ra_{2jk}, \\ b_{2jk} &= \tau((q\alpha_1+s\alpha_2)\beta_j\gamma_k) = qa_{1jk}+sa_{2jk}, \end{aligned}$$

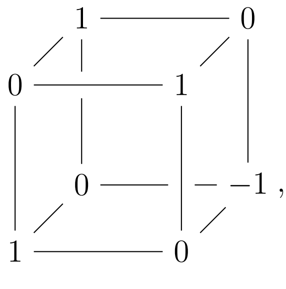
for any $j,k\in\{1,2\}$, and thus

$$(b_{ijk}) = \left(\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)\times\mathrm{id}\times\mathrm{id}\right)\Big((a_{ijk})\Big). \qquad \square$$

In the case over $\mathbb{Z}$, Bhargava says (in the proof of Theorem 11) that if the balanced triple of ideals is replaced by an equivalent triple, the resulting cube does not change. That is not completely true; as we will prove, the two resulting cubes indeed lie in the same equivalence class. But they does not necessarily have to be the same, as shows the following example.

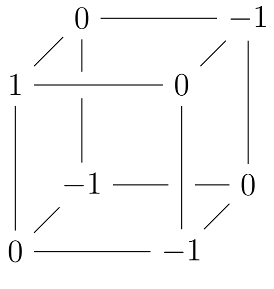
Example. Assume $K=\mathbb{Q}$, $L=\mathbb{Q}(\mathrm{i})$; then $\mathcal{O}_L=[1,\mathrm{i}]$. Both of the triples of oriented ideals $B=\Big([1,\mathrm{i}],[1,\mathrm{i}],[1,\mathrm{i}]\Big)$ and $B'=\Big([\mathrm{i},-1],[1,\mathrm{i}],[1,\mathrm{i}]\Big)$ are balanced; moreover, $B\sim B'$, because $[\mathrm{i},-1]=\mathrm{i}\cdot[1,\mathrm{i}]$, and i is a unit from L with (totally) positive norm. We have

$\Phi'(B) =$



,

$\Phi'(B') =$



;

hence we can see that $\Phi'(B) \neq \Phi'(B')$. But one can check that the cubes are equivalent under the action by $\mathrm{id} \times \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \times \mathrm{id}$.

Proposition 3.9. *The map Φ' does not depend on the choice of the representative $\Big([\alpha_1, \alpha_2], [\beta_1, \beta_2], [\gamma_1, \gamma_2]\Big)$.*

Proof. First, we will prove that Φ' does not depend on the choice of the bases of the oriented ideals. If $[\omega_1, \omega_2]$ and $[p\omega_1 + r\omega_2, q\omega_1 + s\omega_2]$, $p, q, r, s \in \mathcal{O}_K$, are two bases of the same oriented ideal, then $ps - qr \in \mathcal{U}_K^+$ by Lemma 1.11 and the equality of the orientation. Hence, consider a balanced triple $\Big([\alpha_1, \alpha_2], [\beta_1, \beta_2], [\gamma_1, \gamma_2]\Big)$, and let $\Big([p_1\alpha_1{+}r_1\alpha_2, q_1\alpha_1{+}s_1\alpha_2], [p_2\beta_1{+}r_2\beta_2, q_2\beta_1{+}s_2\beta_2], [p_3\gamma_1{+}r_3\gamma_2, q_3\gamma_1{+}s_3\gamma_2]\Big)$ be the same balanced triple with different bases. Then $p_is_i - q_ir_i \in \mathcal{U}_K^+$, $1 \leq i \leq 3$, and it follows from Lemma 3.8 that the images of these two balanced triples under the map Φ' are equivalent cubes.

Now, let $B = (\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ and $B' = (\mathfrak{I}'_1, \mathfrak{I}'_2, \mathfrak{I}'_3)$ be two equivalent balanced triples. First, assume that $\mathfrak{I}_2 = \mathfrak{I}'_2$ and $\mathfrak{I}_3 = \mathfrak{I}'_3$; then there exists $\mu \in \mathcal{U}_L$ such that $\mathcal{N}_{L/K}(\mu) \in \mathcal{U}_K^+$ and $\mathfrak{I}'_1 = \mu\mathfrak{I}_1$. If $\mathfrak{I}_1 = \Big([\alpha_1, \alpha_2]\,; \underline{\operatorname{sgn}}\,(\det M_1)\Big)$, then $\mathfrak{I}'_1 = \Big([\mu\alpha_1, \mu\alpha_2]\,; \underline{\operatorname{sgn}}\,(\det M_1)\Big)$, and there exist some elements $p, q, r, s \in \mathcal{O}_K$ such that $\mu\alpha_1 = p\alpha_1 + r\alpha_2$ and $\mu\alpha_2 = q\alpha_1 + s\alpha_2$. Comparing the expression of the norm of $\mathfrak{I}'_1$ using the bases $[\mu\alpha_1, \mu\alpha_2]$ and $[p\alpha_1 + r\alpha_2, q\alpha_1 + s\alpha_2]$, we get that

$$\begin{aligned} \mathcal{N}_{L/K}(\mu) \det M_1 &= \mathcal{N}_{L/K}([\mu\alpha_1, \mu\alpha_2]) \\ &= \mathcal{N}_{L/K}([p\alpha_1 + r\alpha_2, q\alpha_1 + s\alpha_2]) = (ps - qr) \det M_1; \end{aligned}$$

hence, $ps - qr = \mathcal{N}_{L/K}(\mu)$, and thus $ps - qr \in \mathcal{U}_K^+$. By the first part of the proof, the images of $(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ and $(\mu\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$ are equivalent cubes.

Now, consider the general case; assume $\mathfrak{I}'_i = \kappa_i\mathfrak{I}_i$ for some $\kappa_i \in L$, $1 \leq i \leq 3$. If $B = \Big([\alpha_1, \alpha_2], [\beta_1, \beta_2], [\gamma_1, \gamma_2]\Big)$, then $B' = \Big([\kappa_1\alpha_1, \kappa_1\alpha_2], [\kappa_2\beta_1, \kappa_2\beta_2], [\kappa_3\gamma_1, \kappa_3\gamma_2]\Big)$. We have that

$$\begin{aligned} \Phi'(B) &= \Big(\tau(\alpha_i\beta_j\gamma_k)\Big), \\ \Phi'(B') &= \Big(\tau((\kappa_1\alpha_i)(\kappa_2\beta_j)(\kappa_3\gamma_k))\Big) = \Big(\tau((\kappa_1\kappa_2\kappa_3)\alpha_i\beta_j\gamma_k)\Big). \end{aligned}$$

Therefore, $\Phi'(B') = \Phi'\Big(\,((\kappa_1\kappa_2\kappa_3)\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)\,\Big)$, which is equivalent to $\Phi'(B)$ by the previous part of the proof, because $\kappa_1\kappa_2\kappa_3$ is a unit in L of totally positive norm. □

Proposition 3.10. *Let $B \in \mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big)$. Then* $\operatorname{Disc}\Phi'(B) \in \mathcal{D}$, *and the cube $\Phi'(B)$ is projective.*

Proof. First, assume that $B = ([1, \Omega], [1, \Omega], [1, \Omega])$. Then

$$\Phi'(B) = \begin{tikzcd} & 1 \arrow[rr, dash] \arrow[dd, dash] & & \Omega+\overline{\Omega} \arrow[dd, dash] \\ 0 \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[ur, dash] \arrow[dd, dash] & \\ & \Omega+\overline{\Omega} \arrow[rr, dash] & & \left(\Omega+\overline{\Omega}\right)^2 - \Omega\overline{\Omega} \\ 1 \arrow[ur, dash] \arrow[rr, dash] & & \Omega+\overline{\Omega} \arrow[ur, dash] & \end{tikzcd} = A_{\mathrm{id}};$$

therefore, $\operatorname{Disc}\Phi'(B) = \left(\Omega - \overline{\Omega}\right)^2 \in \mathcal{D}$.

Now, let

$$B = \Big(\left([\alpha_1, \alpha_2]\,; \underline{\operatorname{sgn}}\,(\det M_1)\right), \left([\beta_1, \beta_2]\,; \underline{\operatorname{sgn}}\,(\det M_2)\right), \left([\gamma_1, \gamma_2]\,; \underline{\operatorname{sgn}}\,(\det M_3)\right) \Big).$$

Then there exists $u \in \mathcal{U}_K^+$ such that $\det M_1 \det M_2 \det M_3 = u$. Moreover, recall that

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = M_1 \cdot \begin{pmatrix} 1 \\ \Omega \end{pmatrix}, \qquad \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = M_2 \cdot \begin{pmatrix} 1 \\ \Omega \end{pmatrix}, \qquad \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = M_3 \cdot \begin{pmatrix} 1 \\ \Omega \end{pmatrix}.$$

It follows from Lemma 3.8 that

$$\Phi'(B) = (M_1 \times M_2 \times M_3)\,(A_{\mathrm{id}}).$$

Therefore, by Lemma 3.1, the discriminant of the cube $\Phi'(B)$ is equal to

$$(\det M_1)^2 (\det M_2)^2 (\det M_3)^2 \operatorname{Disc}(A_{\mathrm{id}}) = u^2 \left(\Omega - \overline{\Omega}\right)^2,$$

and thus $\operatorname{Disc}\Phi'(B) \in \mathcal{D}$.

It remains to prove that the cube $\Phi'(B)$ is projective. If the cube $\Phi'(B)$ were not projective, then all the coefficients of the three assigned quadratic forms would be divisible by a prime $p \in \mathcal{O}_K$ (in fact, by a square of a prime), and $\frac{\operatorname{Disc}\Phi'(B)}{u^2 p^2} = \frac{D_\Omega}{p^2}$ would be a quadratic residue modulo 4 in $\mathcal{O}_K$; that would contradict Lemma 1.4. □

3.5 From cubes to ideals

As the second step in the construction of the correspondence, we need to recover a balanced triple of oriented ideals from a given cube (a_{ijk}). For this purpose, Bhargava solves a system of equations

$$\begin{aligned} \alpha_i \beta_j \gamma_k &= c_{ijk} + a_{ijk}\Omega, & 1 \le i, j, k \le 2, \\ \alpha_i \beta_j \gamma_k \cdot \alpha_{i'} \beta_{j'} \gamma_{k'} &= \alpha_{i'} \beta_{j'} \gamma_{k'} \cdot \alpha_i \beta_j \gamma_k, & 1 \le i, i', j, j', k, k' \le 2, \end{aligned}$$

with indeterminates $\alpha_i, \beta_j, \gamma_k, c_{ijk}$. That is computationally difficult,[1] and we will not follow this path. Instead of that, we will use our results from Theorems 2.7 and 3.5, i.e. the bijection (group isomorphism) between $\mathcal{C}\ell^o_{L/K}$ and $\mathcal{Q}_\mathcal{D}$, and the fact that the composition of the three quadratic forms arising from one cube lies within the same class as Q_{id}; denote

$$\mathcal{T}rip\,(\mathcal{Q}_\mathcal{D}) = \left\{ \left([Q_1], [Q_2], [Q_3]\right) \;\middle|\; [Q_i] \in \mathcal{Q}_\mathcal{D},\ 1 \le i \le 3,\ [Q_1 Q_2 Q_3] = [Q_{\mathrm{id}}] \right\}.$$

It follows from Theorem 3.5 that the map Θ (defined as a restriction of the map assigning triple of quadratic forms to a cube) actually goes into $\mathcal{T}rip\,(\mathcal{Q}_\mathcal{D})$. The set $\mathcal{T}rip\,(\mathcal{Q}_\mathcal{D})$ together with the operation of componentwise composition forms a group. It is clear that if the classes $[Q_1], [Q_2]$ are given, the class $[Q_3]$ is determined uniquely. Hence, similarly to Proposition 3.7, we get:

[1] [Bouyer, App. 1.1] mentions a program in Sage running for 24 hours.

Proposition 3.11. *The group $\mathcal{T}rip\left(\mathcal{Q}_{\mathcal{D}}\right)$ is naturally isomorphic to the group $\mathcal{Q}_{\mathcal{D}} \times \mathcal{Q}_{\mathcal{D}}$.*

Proposition 3.11 was the last missing piece to close the cycle of maps as illustrated in Figure 3.1.

$$\begin{tikzcd}
\mathcal{B}al\Big(\mathcal{C}\ell^{o}_{L/K}\Big) \arrow[r, leftrightarrow, "\simeq", "\text{Prop. 3.6}"'] \arrow[d, bend right, "\Phi'"'] & \mathcal{T}rip\Big(\mathcal{C}\ell^{o}_{L/K}\Big) \arrow[r, leftrightarrow, "\simeq", "\text{Prop. 3.7}"'] & \mathcal{C}\ell^{o}_{L/K} \times \mathcal{C}\ell^{o}_{L/K} \arrow[d, bend right, "\Phi \times \Phi"', "\text{1:1}"] \\
\mathcal{C}_{\mathcal{D}} \arrow[u, bend right, dashed, "\Psi'"'] \arrow[r, "\text{Th. 3.5}"'] & \mathcal{T}rip\left(\mathcal{Q}_{\mathcal{D}}\right) \arrow[r, leftrightarrow, "\simeq", "\text{Prop. 3.11}"'] & \mathcal{Q}_{\mathcal{D}} \times \mathcal{Q}_{\mathcal{D}} \arrow[u, bend right, "\Psi \times \Psi"', "\text{Th. 2.7}"]
\end{tikzcd}$$

Figure 3.1: Diagram of the construction of the map Ψ'.

Going around the cycle in the diagram, we can formally define a map

$$\begin{array}{rrcl} \Psi' : & \mathcal{C}_{\mathcal{D}} & \longrightarrow & \mathcal{B}al\Big(\mathcal{C}\ell^{o}_{L/K}\Big) \\ & [A] & \longmapsto & \Big[\Big(\Psi(Q_1), \Psi(Q_2), \left(\Psi(Q_1)\Psi(Q_2)\right)^{-1}\Big)\Big], \end{array} \tag{3.9}$$

where Q_1, Q_2 (and Q_3) are the quadratic forms arising from the cube A. This map is well-defined, because all the maps on the way are well-defined.

3.6 Composition of cubes

At this point, just one last step is remaining, and that is to prove that both $\Psi'\Phi'$ and $\Phi'\Psi'$ are identity maps. Let us start by simplifying the diagram displayed in Figure 3.1:

$$\begin{tikzcd}
\mathcal{B}al\Big(\mathcal{C}\ell^{o}_{L/K}\Big) \arrow[r, leftrightarrow] \arrow[d, bend right, "\Phi'"'] & \mathcal{T}rip\Big(\mathcal{C}\ell^{o}_{L/K}\Big) \arrow[d, bend right, "\Phi \times \Phi \times \Phi"'] \\
\mathcal{C}_{\mathcal{D}} \arrow[u, bend right, "\Psi'"'] \arrow[r, "\Theta"] & \mathcal{T}rip\left(\mathcal{Q}_{\mathcal{D}}\right) \arrow[u, bend right, "\Psi \times \Psi \times \Psi"']
\end{tikzcd}$$

Figure 3.2: Simplified diagram of the construction of the map Ψ'.

It is clear from Figure 3.1 that the map $\Psi \times \Psi \times \Psi$ (and also the map $\Phi \times \Phi \times \Phi$) provide a group isomorphism between $\mathcal{T}rip\Big(\mathcal{C}\ell^{o}_{L/K}\Big)$ and $\mathcal{T}rip\left(\mathcal{Q}_{\mathcal{D}}\right)$.

Proposition 3.12. *$\Phi'\Psi'$ is the identity map on $\mathcal{C}_{\mathcal{D}}$.*

Proof. First, note that by using the result of Lemma 3.4 and the isomorphism φ_2 from Proposition 3.6, we could have defined the map Ψ' equivalently as

$$\begin{array}{rrcl} \Psi' : & \mathcal{C}_{\mathcal{D}} & \longrightarrow & \mathcal{B}al\Big(\mathcal{C}\ell^{o}_{L/K}\Big) \\ & [A] & \longmapsto & \varphi_2\Big(\Big([\Psi(Q_1)], [\Psi(Q_2)], [\Psi(Q_3)]\Big)\Big); \end{array}$$

the situation is depicted in Figure 3.3.

$$\begin{tikzcd}
\left[\left(\frac{1}{\omega}\Psi(Q_1), \Psi(Q_2), \Psi(Q_3)\right)\right] & & & \left([\Psi(Q_1)], [\Psi(Q_2)], [\Psi(Q_3)]\right) \arrow[lll, mapsto] \\
& \mathcal{B}al\left(\mathcal{C}\ell^o_{L/K}\right) & \mathcal{T}rip\left(\mathcal{C}\ell^o_{L/K}\right) \arrow[l, "\varphi_2"'] & \\
& \mathcal{C}_{\mathcal{D}} \arrow[r, "\Theta"] \arrow[u, dashed, "\Psi'"'] & \mathcal{T}rip\left(\mathcal{Q}_{\mathcal{D}}\right) \arrow[u, "\Psi \times \Psi \times \Psi"] & \\
{[A]} \arrow[rrr, mapsto] \arrow[uuu, dashed, mapsto] & & & \left([Q_1], [Q_2], [Q_3]\right) \arrow[uuu, mapsto]
\end{tikzcd}$$

Figure 3.3: Situation in the proof of Proposition 3.12.

Let A be a representative of a class in $\mathcal{C}_{\mathcal{D}}$. By Lemma 3.3, we can assume without loss of generality that A is of the form

$$\begin{tikzcd}
& 0 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
1 \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[dd, dash] & \\
& g \arrow[rr, dash] \arrow[dl, dash] & & h \arrow[dl, dash] \\
0 \arrow[rr, dash] & & d &
\end{tikzcd} .$$

Then

$$\begin{aligned}
\Psi(Q_1) &= \left(\left[-d, \frac{-h+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(-d)\right), \\
\Psi(Q_2) &= \left(\left[-g, \frac{-h+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(-g)\right), \\
\Psi(Q_3) &= \left(\left[-f, \frac{-h+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(-f)\right),
\end{aligned}$$

and we have proved in Lemma 3.4 that

$$\Psi(Q_1)\Psi(Q_2)\Psi(Q_3) = \left(\left(\frac{-h+\sqrt{D}}{2}\right); \underline{\operatorname{sgn}}\,(-dfg)\right),$$

where $D = \operatorname{Disc}(A) = h^2 + 4dfg$. Hence, if we apply the map φ_2 to the triple $\big([\Psi(Q_1)], [\Psi(Q_2)], [\Psi(Q_3)]\big)$, we obtain $\Big[\,(\mathfrak{J}_1, \mathfrak{J}_2, \mathfrak{J}_3)\,\Big]$, where

$$\begin{aligned}
\mathfrak{J}_1 &= \left(\left[\frac{-h-\sqrt{D}}{2fg}, 1\right]; \underline{\operatorname{sgn}}\left(\frac{1}{fg}\right)\right), \\
\mathfrak{J}_2 &= \left(\left[-g, \frac{-h+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(-g)\right), \\
\mathfrak{J}_3 &= \left(\left[-f, \frac{-h+\sqrt{D}}{2}\right]; \underline{\operatorname{sgn}}\,(-f)\right).
\end{aligned}$$

ijk	Argument of the map τ	b_{ijk}
111	$\frac{-h-\sqrt{D}}{2fg}(-g)(-f) = -\frac{h+\sqrt{D}}{2} = -\frac{uw+h}{2} - u\Omega$	$-u$
112	$\frac{-h-\sqrt{D}}{2}(-g)\frac{-h+\sqrt{D}}{2} = \frac{D-h^2}{4f} = dg$	0
121	$\frac{-h-\sqrt{D}}{2}\frac{-h+\sqrt{D}}{2}(-f) = \frac{D-h^2}{4g} = df$	0
211	fg	0
122	$\frac{-h-\sqrt{D}}{2fg}\frac{-h+\sqrt{D}}{2}\frac{-h+\sqrt{D}}{2} = \frac{h^2-D}{4fg}\frac{-h+\sqrt{D}}{2} = -d\frac{-h+\sqrt{D}}{2} = d\frac{h-uw}{2} - ud\Omega$	$-ud$
212	$(-g)\frac{-h+\sqrt{D}}{2} = g\frac{h-uw}{2} - ug\Omega$	$-ug$
221	$\frac{-h+\sqrt{D}}{2}(-f) = f\frac{h-uw}{2} - uf\Omega$	$-uf$
222	$\frac{-h+\sqrt{D}}{2}\frac{-h+\sqrt{D}}{2} = \frac{D+h^2}{4} - h\frac{\sqrt{D}}{2} = \frac{h^2+2dfg-uhw}{2} - hu\Omega$	$-uh$

Table 3.1: Computation of the cube $(b_{ijk}) = \Phi'\Big(\big[\,(\mathfrak{J}_1, \mathfrak{J}_2, \mathfrak{J}_3)\,\big]\Big)$.

Denote $B = \Phi'\Big(\big[\,(\mathfrak{J}_1, \mathfrak{J}_2, \mathfrak{J}_3)\,\big]\Big)$. Using the facts that $D = u^2 D_\Omega$ for a totally positive unit $u \in \mathcal{U}_K^+$, and that $\Omega = \frac{-w+\sqrt{D_\Omega}}{2}$, we compute that

$$B = \begin{tikzcd}
& 0 \arrow[rr, dash] \arrow[dd, dash] & & -uh \arrow[dd, dash] \\
-u \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[ur, dash] \arrow[dd, dash] & \\
& -ug \arrow[rr, dash] & & -uh \\
0 \arrow[ur, dash] \arrow[rr, dash] & & -ud \arrow[ur, dash] &
\end{tikzcd}$$

(see Table 3.1 for detailed computations). Noting that $B = -uA$, we have that $[A] = [B]$, and hence $\Phi'\Psi' = \mathrm{id}_{\mathcal{C}_{\mathcal{D}}}$.

□

Proposition 3.13. $\Psi'\Phi'$ *is the identity map on* $\mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big)$.

Proof. We broadly follow the ideas of [Stange, Sec. 5.4]. Let ρ_1 be the isomorphism between $\mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big)$ and $\mathcal{T}rip\,(\mathcal{Q}_{\mathcal{D}})$ given by the map $(\Phi \times \Phi \times \Phi)\varphi_1$, where φ_1 is the map defined in Proposition 3.6, and denote by ρ_2 the map $\Theta\Phi'$ (see Figure 3.4). We will show that $\rho_1 = \rho_2$; then $\Psi'\Phi' = \mathrm{id}_{\mathcal{B}al\left(\mathcal{C}\ell^o_{L/K}\right)}$ follows, since $\Psi'\Phi' = \rho_1^{-1}\rho_2$.

Consider a balanced triple $B \in \mathcal{B}al\Big(\mathcal{C}\ell^o_{L/K}\Big)$, and let

$$B = \bigg(\Big([\alpha_1, \alpha_2]\,;\underline{\mathrm{sgn}}\,(\det M_1)\Big), \Big([\beta_1, \beta_2]\,;\underline{\mathrm{sgn}}\,(\det M_2)\Big), \Big([\gamma_1, \gamma_2]\,;\underline{\mathrm{sgn}}\,(\det M_3)\Big) \bigg).$$

Then $\rho_1(B)$ is equal to

$$\left(\left[\frac{\mathcal{N}_{L/K}\,(\alpha_1 x - \alpha_2 y)}{\det M_1} \right], \left[\frac{\mathcal{N}_{L/K}\,(\beta_1 x - \beta_2 y)}{\det M_2} \right], \left[\frac{\mathcal{N}_{L/K}\,(\gamma_1 x - \gamma_2 y)}{\det M_3} \right] \right). \qquad (3.10)$$

$$\begin{tikzcd}
\mathcal{B}al\left(\mathcal{C}\ell^o_{L/K}\right) \arrow[r, "\varphi_1"] \arrow[d, "\Phi'"'] \arrow[dr, dashed, bend left, "\rho_1"] \arrow[dr, dashed, bend right, "\rho_2"'] & \mathcal{T}rip\left(\mathcal{C}\ell^o_{L/K}\right) \arrow[d, "\Phi \times \Phi \times \Phi"] \\
\mathcal{C}_{\mathcal{D}} \arrow[r, "\Theta"'] & \mathcal{T}rip\left(\mathcal{Q}_{\mathcal{D}}\right)
\end{tikzcd}$$

Figure 3.4: Maps ρ_1 and ρ_2.

Let us compute $\rho_2(B)$. Recall that $\Phi'(B) = \left(\tau(\alpha_i\beta_j\gamma_k)\right)$ and $\tau(\alpha) = \frac{\alpha-\overline{\alpha}}{\Omega-\overline{\Omega}}$; for $\zeta \in L$, set

$$G(\zeta) = \begin{pmatrix} \tau(\alpha_1\beta_1\zeta) & \tau(\alpha_2\beta_1\zeta) \\ \tau(\alpha_1\beta_2\zeta) & \tau(\alpha_2\beta_2\zeta) \end{pmatrix}.$$

Then

$$\det G(\zeta) = -\mathcal{N}_{L/K}(\zeta) \cdot \frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\Omega - \overline{\Omega}} \cdot \frac{\overline{\beta_1}\beta_2 - \beta_1\overline{\beta_2}}{\Omega - \overline{\Omega}} = -\mathcal{N}_{L/K}(\zeta) \det M_1 \det M_2.$$

Note that $G(\gamma_1)$ is the upper face of the cube $\left(\tau(\alpha_i\beta_j\gamma_k)\right)$, and $G(\gamma_2)$ is the lower face; hence, if Q_3 denotes the third quadratic form assigned to this cube, it holds that

$$Q_3(x,y) = -\det\left(G(\gamma_1)x - G(\gamma_2)y\right).$$

Therefore,

$$Q_3(x,y) = -\det\left(G(\gamma_1 x - \gamma_2 y)\right) = \mathcal{N}_{L/K}(\gamma_1 x - \gamma_2 y) \det M_1 \det M_2. \qquad (3.11)$$

Since B is a balanced triple of ideals, there exists a totally positive unit $u \in \mathcal{U}_K^+$ such that $\det M_1 \det M_2 \det M_3 = u$. Thus, we can rewrite the expression (3.11) as

$$Q_3(x,y) = u \cdot \frac{\mathcal{N}_{L/K}(\gamma_1 x - \gamma_2 y)}{\det M_3}.$$

Similarly, we can prove that

$$Q_1(x,y) = u \cdot \frac{\mathcal{N}_{L/K}(\alpha_1 x - \alpha_2 y)}{\det M_1},$$
$$Q_2(x,y) = u \cdot \frac{\mathcal{N}_{L/K}(\beta_1 x - \beta_2 y)}{\det M_2}.$$

Thus,

$$\rho_2(B) = \left([Q_1], [Q_2], [Q_3]\right);$$

comparing with (3.10), we see that $\rho_1(B) = \rho_2(B)$. □

We can summarize our results; we need the term *fundamental element*, which we have introduced in Definition 1.3.

Theorem 3.14. *Let K be a number field of narrow class number one. Let D be a fundamental element of $\mathcal{O}_K$. Set $L = K\left(\sqrt{D}\right)$, and $\mathcal{D} = \left\{u^2 D \mid u \in \mathcal{U}_K^+\right\}$. Then we have a bijection between $\mathcal{C}_{\mathcal{D}}$ and $\mathcal{B}al\left(\mathcal{C}\ell^o_{L/K}\right)$ given by the map Φ' defined in* (3.8) *(equivalently by the map Ψ' defined in* (3.9)*).*

Proof. Let Ω be such that $\mathcal{O}_L = [1, \Omega]$; similarly as in the proof of Theorem 2.7 we can assume without loss of generality that $D = D_\Omega$. In Propositions 3.12 and 3.13, we have proved that Φ' and Ψ' are mutually inverse bijections. □

Corollary 3.15. *$\mathcal{C}_\mathcal{D}$ carries a group structure arising from multiplication of balanced triples of oriented ideals in $K(\sqrt{D})$. The identity element of this group is represented by the cube A_{id},*

$$A_{\mathrm{id}} = \begin{tikzcd} & 1 \arrow[rr, dash] \arrow[dd, dash] & & \Omega+\overline{\Omega} \arrow[dd, dash] \\ 0 \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[ur, dash] \arrow[dd, dash] & \\ & \Omega+\overline{\Omega} \arrow[rr, dash] & & \left(\Omega+\overline{\Omega}\right)^2-\Omega\overline{\Omega} \\ 1 \arrow[ur, dash] \arrow[rr, dash] & & \Omega+\overline{\Omega} \arrow[ur, dash] & \end{tikzcd} .$$

The inverse element to $\left[(a_{ijk})\right]$ is $\left[(-1)^{i+j+k}(a_{ijk})\right]$, i.e.

$$\left[\begin{tikzcd} & e \arrow[rr, dash] \arrow[dd, dash] & & f \arrow[dd, dash] \\ a \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[ur, dash] \arrow[dd, dash] & \\ & g \arrow[rr, dash] & & h \\ c \arrow[ur, dash] \arrow[rr, dash] & & d \arrow[ur, dash] & \end{tikzcd}\right]^{-1} = \left[\begin{tikzcd} & e \arrow[rr, dash] \arrow[dd, dash] & & -f \arrow[dd, dash] \\ -a \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[ur, dash] \arrow[dd, dash] & \\ & -g \arrow[rr, dash] & & h \\ c \arrow[ur, dash] \arrow[rr, dash] & & -d \arrow[ur, dash] & \end{tikzcd}\right].$$

Proof. The group structure of $\mathcal{C}_\mathcal{D}$ follows from Theorem 3.14.

A representative of the identity element in the group $\mathcal{B}al\left(\mathcal{C}\ell^o_{L/K}\right)$ is the triple $\left([1,\Omega],[1,\Omega],[1,\Omega]\right)$; its image under the map Φ' is the class represented by the cube A_{id}.

Consider a cube (a_{ijk}); by Theorem 3.14, there exists a balanced triple of ideals

$$B = \Big(\left([\alpha_1,\alpha_2]\,;\underline{\operatorname{sgn}}\,(\det M_1)\right), \left([\beta_1,\beta_2]\,;\underline{\operatorname{sgn}}\,(\det M_2)\right), \left([\gamma_1,\gamma_2]\,;\underline{\operatorname{sgn}}\,(\det M_3)\right) \Big)$$

such that $\Phi'(B) = (a_{ijk})$, i.e. $a_{ijk} = \tau(\alpha_i\beta_j\gamma_k)$, $1 \le i,j,k \le 2$. It follows from Lemmas 1.15 and 1.19 that the inverse element to B is $B^{-1} = \left(\mathfrak{I}_1,\mathfrak{I}_2,\mathfrak{I}_3\right)$, where

$$\begin{aligned} \mathfrak{I}_1 &= \left(\left[\frac{\overline{\alpha_1}}{\det M_1}, -\frac{\overline{\alpha_2}}{\det M_1}\right];\underline{\operatorname{sgn}}\,(\det M_1)\right), \\ \mathfrak{I}_2 &= \left(\left[\frac{\overline{\beta_1}}{\det M_2}, -\frac{\overline{\beta_2}}{\det M_2}\right];\underline{\operatorname{sgn}}\,(\det M_2)\right), \\ \mathfrak{I}_3 &= \left(\left[\frac{\overline{\gamma_1}}{\det M_3}, -\frac{\overline{\gamma_2}}{\det M_3}\right];\underline{\operatorname{sgn}}\,(\det M_3)\right). \end{aligned}$$

Denote $u = \det M_1 \det M_2 \det M_3$. Then

$$\Phi'\left(B^{-1}\right) = \left(\tau\left((-1)^{i+j+k+1}u^{-1}\overline{\alpha_i\beta_j\gamma_k}\right)\right) = \left((-1)^{i+j+k+1}u^{-1}\tau\left(\overline{\alpha_i\beta_j\gamma_k}\right)\right).$$

Multiplying the cube by u, we get an equivalent cube $\left((-1)^{i+j+k+1}\tau\left(\overline{\alpha_i\beta_j\gamma_k}\right)\right)$; hence, we have to compute $\tau\left(\overline{\alpha_i\beta_j\gamma_k}\right)$. If we write

$$\alpha_i\beta_j\gamma_k = c_{ijk} + a_{ijk}\Omega,$$

for some $c_{ijk} \in \mathcal{O}_K$, $1 \leq i, j, k \leq 2$, then

$$\overline{\alpha_i\beta_j\gamma_k} = c_{ijk} + a_{ijk}\overline{\Omega}.$$

Since $\Omega = \frac{-w+\sqrt{D_\Omega}}{2}$, we have that $\overline{\Omega} = -\Omega - w$; therefore,

$$\overline{\alpha_i\beta_j\gamma_k} = (c_{ijk} - a_{ijk}w) - a_{ijk}\Omega,$$

and

$$\tau\left(\overline{\alpha_i\beta_j\gamma_k}\right) = (-a_{ijk}).$$

It follows that the cube $\Phi'\left(B^{-1}\right)$ is equivalent to the cube $\left((-1)^{i+j+k}a_{ijk}\right)$. □

Together with the isomorphisms we have known before, we have proved the following corollary.

Corollary 3.16. *The groups $\mathcal{C}_\mathcal{D}$, $\mathcal{T}rip\left(\mathcal{Q}_\mathcal{D}\right)$ and $\mathcal{C}\ell^o_{L/K} \times \mathcal{C}\ell^o_{L/K}$ are isomorphic.*

We have actually proved even more; see Figure 3.5.

$$\begin{tikzcd}
\mathcal{B}al\left(\mathcal{C}\ell^o_{L/K}\right) \arrow[r, leftrightarrow, "\simeq", "\text{Prop. 3.6}"'] \arrow[d, leftrightarrow, "\simeq"', "\text{Theorem 3.14}"] & \mathcal{T}rip\left(\mathcal{C}\ell^o_{L/K}\right) \arrow[r, leftrightarrow, "\simeq", "\text{Prop. 3.7}"'] \arrow[d, leftrightarrow, "\simeq"'] & \mathcal{C}\ell^o_{L/K} \times \mathcal{C}\ell^o_{L/K} \arrow[d, leftrightarrow, "\simeq"'] \\
\mathcal{C}_\mathcal{D} \arrow[r, "\simeq", "\text{Th. 3.5}"'] & \mathcal{T}rip\left(\mathcal{Q}_\mathcal{D}\right) \arrow[r, leftrightarrow, "\simeq", "\text{Prop. 3.11}"'] & \mathcal{Q}_\mathcal{D} \times \mathcal{Q}_\mathcal{D}
\end{tikzcd}$$

Figure 3.5: Summary of the isomorphisms.

4. Class groups

In both of the correspondences, we were working with relative oriented class group, which has been defined in Section 1.5. In this final chapter, we will define yet another group, which we call ε-class group. On the first glance, this group looks similar to the relative oriented class group, but this time we will need only one number field (not an extension of number fields).

At first, let us recall the usual definitions of class groups. Consider a number field F. Let $\mathcal{I}_F$ be the set of all fractional $\mathcal{O}_F$-ideals, $\mathcal{P}_F$ the subset of all principal $\mathcal{O}_F$-ideals, and $\mathcal{P}_F^+$ the set of all principal $\mathcal{O}_F$-ideals generated by the totally positive elements of F, i.e. the ideals of the form $(\alpha) = \alpha\mathcal{O}_F$ for $\alpha \in F$ totally positive. Note that $\mathcal{I}_F$ forms a group under the multiplication of ideals, and both $\mathcal{P}_F$ and $\mathcal{P}_F^+$ are its subgroup. Then the *class group* is defined as

$$\mathcal{C}\ell_F = {}^{\mathcal{I}_F}\Big/_{\mathcal{P}_F}.$$

and the *narrow class group* is defined as

$$\mathcal{C}\ell_F^+ = {}^{\mathcal{I}_F}\Big/_{\mathcal{P}_F^+}.$$

Denote by $h(F)$ (called *class number*) and $h^+(F)$ (called *narrow class number*) the orders of the groups $\mathcal{C}\ell_F$ and $\mathcal{C}\ell_F^+$, respectively.

4.1 ε-class group

Let us denote the real embeddings of the field F by $\sigma_1, \dots, \sigma_r$.[1] Let us consider the set

$$\mathcal{I}_F^\varepsilon = \{(I; \varepsilon_1, \dots, \varepsilon_r) \mid I \in \mathcal{I}_F, \varepsilon_i \in \{\pm 1\}, i = 1, \dots, r\}$$

and call it the set of *(fractional) ε-ideals.* We can define the multiplication on this set by

$$(I; \varepsilon_1, \dots, \varepsilon_r) \cdot (J; \delta_1, \dots, \delta_r) = (IJ; \varepsilon_1\delta_1, \dots, \varepsilon_r\delta_r).$$

Then, by similar reason as in the case of the (narrow) class group, this set forms an abelian group; namely the identity element is $(\mathcal{O}_F; +1, \dots, +1)$, and the inverse element to $(I; \varepsilon_1, \dots, \varepsilon_r)$ is $(I^{-1}; \varepsilon_1, \dots, \varepsilon_r)$, because $\varepsilon_i^2 = +1$. Then the set

$$\mathcal{P}_F^\varepsilon = \{((\alpha); \operatorname{sgn}(\sigma_1(\alpha)), \dots, \operatorname{sgn}(\sigma_r(\alpha))) \mid \alpha \in F\}$$

is clearly a subgroup of $\mathcal{I}_F^\varepsilon$; we will call it the group of *principal (fractional) ε-ideals.* Now we can define the *ε-class group* $\mathcal{C}\ell_F^\varepsilon$ as the factorgroup, i.e.

$$\mathcal{C}\ell_F^\varepsilon = {}^{\mathcal{I}_F^\varepsilon}\Big/_{\mathcal{P}_F^\varepsilon}.$$

[1] In general, these σ_i's do not have anything in common with the real embeddings of our fixed field K, and we should use e.g. $\sigma_1', \dots, \sigma_{r'}'$. But as the number fields F and K will not ever appear next to each other in this thesis, we can afford to use the same notation for both of them.

Equivalently, we can define the multiplication of an ε-ideal $(I;\varepsilon_1,\dots,\varepsilon_r)$ by a nonzero element $\alpha\in F$ as

$$\alpha\cdot(I;\varepsilon_1,\dots,\varepsilon_r)=(\alpha I;\mathrm{sgn}(\sigma_1(\alpha))\varepsilon_1,\dots,\mathrm{sgn}(\sigma_r(\alpha))\varepsilon_r)\,,$$

and say that two ε-ideals $(I;\varepsilon_1,\dots,\varepsilon_r)$, $(J;\delta_1,\dots,\delta_r)$ are in the same *ε-ideal class* if $(J;\delta_1,\dots,\delta_r)=\alpha\cdot(I;\varepsilon_1,\dots,\varepsilon_r)$ holds for a nonzero element $\alpha\in F$.

From now on, we will write simply $\underline{\varepsilon}$ instead of $\varepsilon_1,\dots,\varepsilon_r$, and $\underline{\mathrm{sgn}}\,(\alpha)$ instead of $\mathrm{sgn}(\sigma_1(\alpha)),\dots,\mathrm{sgn}(\sigma_r(\alpha))$; then by $\underline{\varepsilon\delta}$ we understand componentwise multiplication, i.e. $\underline{\varepsilon\delta}$ stands for $\varepsilon_1\delta_1,\dots,\varepsilon_r\delta_r$.

Note that if there is no real embedding, then there are no signs added, and the condition of the totally real element is trivially satisfied. Thus the notion of the ε-class group and the class group (and also the narrow class group) coincide in this case.

We would like to find out if there is any relationship between the narrow class group and the ε-class group in general. It is clear that for every fractional ideal $I\in\mathcal{I}_F$, there are exactly 2^r copies of I in $\mathcal{I}_F^{\varepsilon}$ (one copy for every possible vector of signs $\underline{\varepsilon}$). But the group $\mathcal{P}_F^{\varepsilon}$ also contains much more elements than the group $\mathcal{P}_F$. It turns out that the narrow class group and the ε-class group are always isomorphic.

Theorem 4.1. *For a number field F, it holds that $\mathcal{C}\ell_F^{\varepsilon}\simeq\mathcal{C}\ell_F^{+}$.*

Proof. Consider the following group homomorphisms:

$$\begin{array}{rccc} f: & \mathcal{I}_F & \longrightarrow & \mathcal{I}_F^{\varepsilon} \\ & I & \longmapsto & (I;+1,\dots,+1) \\[1ex] f': & \mathcal{P}_F^{+} & \longrightarrow & \mathcal{P}_F^{\varepsilon} \\ & (\gamma) & \longmapsto & ((\gamma);+1,\dots,+1) \end{array}$$

Clearly both f and f' are injective, and f' is a restriction of f on $\mathcal{P}_F^{+}$. Furthermore, consider the following group homomorphism g and its restriction g':

$$\begin{array}{rccc} g: & \mathcal{I}_F^{\varepsilon} & \longrightarrow & \langle\pm1\rangle^r \\ & (I;\underline{\varepsilon}) & \longmapsto & \underline{\varepsilon} \\[1ex] g': & \mathcal{P}_F^{\varepsilon} & \longrightarrow & \langle\pm1\rangle^r \\ & \Big((\gamma)\,;\underline{\mathrm{sgn}}\,(\gamma)\Big) & \longmapsto & \underline{\mathrm{sgn}}\,(\gamma) \end{array}$$

Note that both g and g' are surjective; the surjectivity of g' is a consequence of Weak Approximation Theorem (see e.g. [Fröhlich and Taylor, 1993, II.(2.14)]). Moreover, we have

$$\begin{aligned} \mathrm{Ker}\,g &= \{(I;\underline{\varepsilon})\ \mid \varepsilon_i=+1\ \forall i=1,\dots,r\}=\mathrm{Im}\,f, \\ \mathrm{Ker}\,g' &= \Big\{\Big((\gamma)\,;\underline{\mathrm{sgn}}\,(\gamma)\Big)\ \mid\ \mathrm{sgn}\,\sigma_i(\gamma)=+1\ \forall i=1,\dots,r\Big\}=\mathrm{Im}\,f'. \end{aligned}$$

Hence, we obtain the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{I}_F \arrow[r, "f"] & \mathcal{I}_F^\varepsilon \arrow[r, "g"] & \langle \pm 1 \rangle^r \arrow[r] & 1 \\
1 \arrow[r] & \mathcal{P}_F^+ \arrow[r, "f'"] \arrow[u, hook, "i_1"] & \mathcal{P}_F^\varepsilon \arrow[r, "g'"] \arrow[u, hook, "i_2"] & \langle \pm 1 \rangle^r \arrow[r] \arrow[u, hook, "i_3=\mathrm{id}"] & 1
\end{tikzcd}$$

Note that $\operatorname{Coker} i_1 = \mathcal{C}\ell_F^+$, $\operatorname{Coker} i_2 = \mathcal{C}\ell_F^\varepsilon$, $\operatorname{Coker} i_3 = 1$, and $\operatorname{Ker} i_3 = 1$. Hence, by Snake Lemma, there is the following exact sequence:

$$1 \longrightarrow \mathcal{C}\ell_F^+ \longrightarrow \mathcal{C}\ell_F^\varepsilon \longrightarrow 1$$

This sequence gives us the required isomorphism between $\mathcal{C}\ell_F^\varepsilon$ and $\mathcal{C}\ell_F^+$. □

In the previous proof, we could also proceed in a different way. We could fix for every $i = 1, \dots, r$ an element α_i of F such that

$$\operatorname{sgn}(\sigma_j(\alpha_i)) = \begin{cases} -1, & \text{if } j = i, \\ +1, & \text{if } j \neq i, \end{cases}$$

(such an element α_i exists by Weak Approximation Theorem), and define a map $\varphi : \mathcal{C}\ell_F^\varepsilon \longrightarrow \mathcal{C}\ell_F^+$ by

$$(I; \varepsilon_1, \dots, \varepsilon_r)\, \mathcal{P}_F^\varepsilon \overset{\varphi}{\longmapsto} \left(\prod_{\varepsilon_i = -1} \alpha_i \right) I \mathcal{P}_F^+.$$

One has to check that this is a well-defined group homomorphism on the classes of ε-ideals with the inverse

$$I\mathcal{P}_F^+ \longmapsto (I; +1, \dots, +1)\mathcal{P}_F^\varepsilon.$$

This approach is helpful mainly in the cases of extensions of lower degree, such as quadratic and biquadratic number fields, where one has a canonical way how to fix the elements α_i.

Example. Let F be a quadratic number field, i.e. $F = \mathbb{Q}(\sqrt{D})$, D a nonzero square-free integer. We will examine the dependence of the ε-class group on D through the above given isomorphism φ.

If $D < 0$, then there are no real embeddings, and φ is the identity map. Thus, assume $D > 0$; then $r = 2$, and the situation is a bit more complicated. We need to find the elements α_1 and α_2. Without loss of generality, we may assume that $\sigma_1(\sqrt{D}) > 0$. Then necessarily $\sigma_2(\sqrt{D}) < 0$. Hence, $\alpha_2 := \sqrt{D}$ and $\alpha_1 := -\sqrt{D}$ are the natural choices of α_i's, and the isomorphism φ looks as follows:

$$\begin{array}{cccc}
\varphi : & \mathcal{C}\ell_F^\varepsilon & \longrightarrow & \mathcal{C}\ell_F^+ \\
& (I; +1, +1)\, \mathcal{P}_F^\varepsilon & \longmapsto & I\mathcal{P}_F^+ \\
& (I; +1, -1)\, \mathcal{P}_F^\varepsilon & \longmapsto & \left(\sqrt{D} I\right) \mathcal{P}_F^+ \\
& (I; -1, +1)\, \mathcal{P}_F^\varepsilon & \longmapsto & \left(-\sqrt{D} I\right) \mathcal{P}_F^+ \\
& (I; -1, -1)\, \mathcal{P}_F^\varepsilon & \longmapsto & (-DI)\, \mathcal{P}_F^+
\end{array}$$

Note that for a fractional $\mathcal{O}_F$-ideal I the following holds:

$$\gamma \in \mathcal{U}_F \;\Leftrightarrow\; \gamma I = I. \tag{4.1}$$

Suppose first that there exists $u \in \mathcal{U}_F$ such that $\mathcal{N}_F(u) = -1$; it is known that such a unit u exists if and only if the period of the continued fraction expansion of $\sqrt{D}$ (or of $\frac{\sqrt{D}-1}{2}$ in the case $D \equiv 1 \pmod 4$) is odd. Without loss of generality, we can assume that $\underline{\operatorname{sgn}}(u) = (+1, -1)$. We obtain by multiplying by the units u, $-u$ and -1 that all the ε-ideals $(I; +1, +1)$, $(I; +1, -1)$, $(I; -1, +1)$ and $(I; -1, -1)$ lie in the same ε-ideal class. Thus, in order to see that φ is well-defined, we would like to show that the ideals I, $\sqrt{D}I$, $-\sqrt{D}I$, $-DI$ also lie in the same narrow ideal class. But we have to be a bit careful, because to obtain the (narrow ideal) equivalence, we can only use totally positive elements. Multiplying by D gives the equivalence between the ideals I and $DI = -DI$; multiplying by $u\sqrt{D}$ (note that this element is totally positive) gives the equivalence between the ideals I and $u\sqrt{D}I = \sqrt{D}I = -\sqrt{D}I$.

Now suppose that there does not exist any element of $\mathcal{U}_F$ of the norm -1. Using (4.1), we can see that in this case $(I; +1, +1)$ and $(I; +1, -1)$ do not lie in the same oriented ideal class. Still, multiplying by -1 gives us the equivalence between $(I; +1, +1)$ and $(I; -1, -1)$, and also between $(I; +1, -1)$ and $(I; -1, +1)$. These correspond to the equivalence between the ideals I and DI (multiplying by D, which is totally positive), and between $\sqrt{D}I$ and $-\sqrt{D}I$ (this holds trivially because $-\sqrt{D}I = \sqrt{D}I$), respectively. Finally, we want to prove that the ideals I and $\sqrt{D}I$ are not equivalent. Let $\beta \in F \backslash \{0\}$ be such that $\beta I = \sqrt{D}I$. This is equivalent to $I = \frac{\sqrt{D}}{\beta} I$. We will again use (4.1): since we have supposed that there is not any element of $\mathcal{O}_F$ of the norm -1, it has to hold that $\mathcal{N}_F\left(\frac{\sqrt{D}}{\beta}\right) = +1$. As $\mathcal{N}_F\left(\sqrt{D}\right) < 0$, we obtain that $\mathcal{N}_F(\beta) < 0$, and thus β is not totally positive. Therefore, the ideals I and $\sqrt{D}I$ do not lie in the same narrow ideals class.

4.2 Relation between class group and narrow class group

Proposition 4.2. *For a number field F set $H = \left\{\underline{\operatorname{sgn}}(\mu) \mid \mu \in \mathcal{U}_F\right\}$; then*

$$\mathcal{C}\ell_F \simeq \mathcal{C}\ell_F^{\varepsilon} \Big/ \Big(\{\mathcal{O}_F\} \times {}^{\langle \pm 1 \rangle^r}/_{H}\Big).$$

Proof. Consider the following group homomorphism π and its restriction π':

$$\begin{array}{llcl} \pi: & \mathcal{I}_F^{\varepsilon} & \longrightarrow & \mathcal{I}_F \\ & (I; \underline{\varepsilon}) & \longmapsto & I \\ & & & \\ \pi': & \mathcal{P}_F^{\varepsilon} & \longrightarrow & \mathcal{P}_F \\ & \big((\gamma); \underline{\operatorname{sgn}}(\gamma)\big) & \longmapsto & (\gamma) \end{array}$$

Clearly both π and π' are surjective; therefore, we can consider the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \operatorname{Ker}\pi \arrow[r, hook] & \mathcal{I}_F^{\varepsilon} \arrow[r, "\pi"] & \mathcal{I}_F \arrow[r] & 1 \\
1 \arrow[r] & \operatorname{Ker}\pi' \arrow[r, hook] \arrow[u, hook] & \mathcal{P}_F^{\varepsilon} \arrow[r, "\pi'"] \arrow[u, hook] & \mathcal{P}_F \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

Using Snake Lemma, we obtain a short exact sequence:

$$1 \longrightarrow {}^{\operatorname{Ker}\pi}\Big/_{\operatorname{Ker}\pi'} \longrightarrow \mathcal{Cl}_F^{\varepsilon} \longrightarrow \mathcal{Cl}_F \longrightarrow 1$$

Noting that

$$\begin{aligned} \operatorname{Ker}\pi &= \{(\mathcal{O}_F; \underline{\varepsilon}) \mid \underline{\varepsilon} \in \langle \pm 1 \rangle^r\} = \{\mathcal{O}_F\} \times \langle \pm 1 \rangle^r, \\ \operatorname{Ker}\pi' &= \Big\{\big((\mu); \underline{\operatorname{sgn}}(\mu)\big) \mid \mu \in \mathcal{U}_F\Big\} = \{\mathcal{O}_F\} \times H, \end{aligned}$$

we obtain the required isomorphism. □

The result also tells us the relation between the class number and the narrow class number.

Corollary 4.3. *Let F be a number field with r real embeddings, and let $t \in \mathbb{Z}$ be such that*

$$\left| {}^{\mathcal{U}_F}\Big/_{\mathcal{U}_F^+} \right| = 2^t.$$

Then

$$h^+(F) = 2^{r-t}\, h(F).$$

In particular, if $h^+(F) = 1$, then $h(F) = 1$ and $r = t$, i.e. there exist units of all signs in F.

Proof. Let H be the same as above. Then clearly

$$H \simeq {}^{\mathcal{U}_F}\Big/_{\mathcal{U}_F^+},$$

and hence $|H| = 2^t$. Then the claim follows directly from Proposition 4.2. □

Conclusion

The thesis had two main goals. The first one has been to develop a theory of composition of binary quadratic forms, which would be analogous to the classic one (which dates back to Gauss, Dirichlet and Dedekind), but in a more general setting. The crucial question has been, what this "more general setting" should be. The second goal has been to try to use the new theory for a generalization of the composition of Bhargava cubes.

In the very beginning of the research, it was necessary to gain an insight into class group and narrow class group, their relation to binary quadratic forms and the difference between them. This difference is well-known in the case of quadratic number fields, but other cases are often omitted in literature. In Chapter 4, we have given an alternative description of narrow class group, which has easily yielded the relationship to class group in an arbitrary number field. Unfortunately, this relationship is still dependent on the index of the group of totally positive units in the group of all units, and in general it is a difficult problem to compute this index.

The first main goal has been fulfilled in Chapter 2. We have developed the theory of composition of binary quadratic forms, which is analogous to Dedekind's approach. The composition is given by a bijection between equivalence classes of quadratic forms and the relative oriented class group; the obtained results are summarized in Theorem 2.7. While Dedekind worked with rational integers as the coefficients of quadratic forms, we have considered the ring of algebraic integers of an arbitrary number field. It has emerged from the construction what the crucial condition is: the underlying number field has to be of narrow class number one. Of course, this condition is still quite restrictive, but we have seen in Sections 1.2 and 1.5 that it is necessary for the chosen approach; loosening this condition would lead to a less explicit description.

Chapter 3 has been devoted to Bhargava cubes. We have generalized the cubes to our setting: instead of cubes over rational integers, we have studied cubes with entries from the ring of algebraic integers. We have seen that three binary quadratic forms can be constructed from each such a cube. Assuming that the underlying number field is of narrow class number one, we have been able to use the theory of composition, namely the bijection between quadratic forms and relative oriented class group. That has given us two interesting results: the first one is an alternative description of composition of quadratic forms (Theorem 3.5), and the second one is a composition law on the cubes themselves (Theorem 3.14). By that we have accomplished the second goal of the thesis.

Overall we can say that all intended goals were achieved. It is worth noting that Bhargava used his cubes to define another composition laws on different polynomials; the two aforementioned results indicate that our theory might be suitable for generalization of the other composition laws as well.

Bibliography

Manjul Bhargava. Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. *Annals of Mathematics*, 159:217–250, Jan 2004. doi: 10.4007/annals.2004.159.217.

Valentin Blomer and Vítězslav Kala. On the rank of universal quadratic forms over real quadratic fields. *Doc. Math.*, to appear. URL https://arxiv.org/pdf/1705.03671.pdf.

Valentin Blomer and Vítězslav Kala. Number fields without n-ary universal quadratic forms. *Math. Proc. Cambridge Philos. Soc.*, 159(2):239–252, 2015. ISSN 0305-0041. URL https://doi.org/10.1017/S030500411500033X.

Florian Bouyer. Composition and Bhargava's Cubes. URL https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/gauss_composition.pdf.

Hubert Butts and Dennis Estes. Modules and binary quadratic forms over integral domains. *Linear Algebra and its Applications*, 1(2):153 – 180, 1968. ISSN 0024-3795. doi: https://doi.org/10.1016/0024-3795(68)90001-3. URL http://www.sciencedirect.com/science/article/pii/0024379568900013.

Wai-kiu Chan, Myung-Hwan Kim, and S. Raghavan. Ternary universal integral quadratic forms over real quadratic fields. *Japan. J. Math. (N.S.)*, 22(2):263–273, 1996. ISSN 0289-2316. URL https://doi.org/10.4099/math1924.22.263.

David A. Cox. *Primes of the form x2 + ny2: Fermat, class field theory, and complex multiplication*. Pure and applied mathematics. Wiley, 1997. ISBN 9780471190790. URL https://books.google.cz/books?id=pSMlAQAAIAAJ.

Bill Dulin and Hubert Butts. Composition of binary quadratic forms over integral domains. *Acta Arithmetica*, 20(3):223–251, 1972. URL http://eudml.org/doc/205080.

Andrew G. Earnest and Azar Khosravani. Universal positive quaternary quadratic lattices over totally real number fields. *Mathematika*, 44(2):342–347, 1997. ISSN 0025-5793. URL https://doi.org/10.1112/S0025579300012651.

Hugh M. Edgar, Richard Mollin, and B. L. Peterson. Class groups, totally positive units, and squares. 98:33–37, 09 1986.

Albrecht Fröhlich and Martin J. Taylor. *Algebraic Number Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1993. ISBN 9780521438346. URL https://books.google.cz/books?id=xaQu26m0vjAC.

Vítězslav Kala. Universal quadratic forms and elements of small norm in real quadratic fields. *Bull. Aust. Math. Soc.*, 94(1):7–14, 2016. ISSN 0004-9727. URL https://doi.org/10.1017/S0004972715001495.

Irving Kaplansky. Composition of binary quadratic forms. *Studia Mathematica*, 31(5):523–530, 1968. URL http://eudml.org/doc/217346.

Martin Kneser. Composition of binary quadratic forms. *Journal of Number Theory*, 15(3):406 – 413, 1982. ISSN 0022-314X. doi: https://doi.org/10.1016/0022-314X(82)90041-5. URL http://www.sciencedirect.com/science/article/pii/0022314X82900415.

Henry B. Mann. On integral basis. *Proc. Amer. Math. Soc.*, pages 167–172, 1958.

Michael W. Mastropietro. *Quadratic forms and relative quadratic extensions.* 2000. URL https://books.google.cz/books?id=C2Y-AQAAIAAJ.

James S. Milne. Algebraic number theory (v3.00), 2008. URL www.jmilne.org/math/.

Wladyslaw Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2004. ISBN 9783540219026. URL https://books.google.cz/books?id=Pw4F-EVIK-oC.

Evan M. O'Dorney. Rings of small rank over a Dedekind domain and their ideals. *Research in the Mathematical Sciences*, 3(1):8, Apr 2016. ISSN 2197-9847. doi: 10.1186/s40687-016-0054-0. URL https://doi.org/10.1186/s40687-016-0054-0.

Carl Ludwig Siegel. Sums of mth powers of algebraic integers. *Ann. of Math. (2)*, 46:313–339, 1945. ISSN 0003-486X. URL https://doi.org/10.2307/1969026.

Katherine E. Stange. Notes on Bhargava's composition laws. URL http://math.colorado.edu/~kstange/papers/notes-on-Bhargava.pdf.

Jacob Towber. Composition of oriented binary quadratic form-classes over commutative rings. *Advances in Mathematics*, 36(1):1 – 107, 1980. ISSN 0001-8708. doi: https://doi.org/10.1016/S0001-8708(80)80002-8. URL http://www.sciencedirect.com/science/article/pii/S0001870880800028.

Melanie M. Wood. Gauss composition over an arbitrary base. *Advances in Mathematics*, 226(2):1756–1771, 2011. ISSN 0001-8708. doi: https://doi.org/10.1016/j.aim.2010.08.018. URL http://www.sciencedirect.com/science/article/pii/S0001870810003257.

Kristýna Zemková. Composition of binary quadratic forms over number fields. Preprint, 2017. URL https://arxiv.org/pdf/1712.00741.pdf.